

# 100rel inbound

To configure the 100rel interworking parameters for inbound SIP adjacencies on signaling border elements (SBEs), use the **100rel inbound** command in the adjacency SIP configuration mode.

## 100rel inbound {strip | support}

Syntax Description	inbound	Sets the inbound SIP 100rel parameters.
	<b>strip</b>	Strips 100rel from the Supported and Require headers in the incoming INVITE request.
	<b>support</b>	Sends reliable provisional responses for all the requests that include a “Supported: 100rel” header, even when the request does not include a “Require: 100rel” header and responses are received as unreliable provisional responses.

**Command Default** 100rel interworking is disabled.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to enable the 100rel strip option for the incoming INVITE request for inbound SIP adjacency:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# 100rel inbound strip
Router(config-sbc-sbe-adj-sip)#
```

The following example shows how to enable 100rel support option to send reliable provisional responses for all the incoming SIP INVITE requests that contains “Supported:100rel” header:

```
Router(config-sbc-sbe-adj-sip)# 100rel inbound support
Router(config-sbc-sbe-adj-sip)#
```

# 100rel outbound

To configure the 100rel interworking parameters for outbound SIP adjacencies on signaling border elements (SBEs), use the **100rel outbound** command in the adjacency SIP configuration mode.

**100rel outbound {require-add | support-add}**

Syntax Description	Command	Description
	<b>outbound</b>	Sets the outbound SIP 100rel parameters.
	<b>require-add</b>	Adds 100rel Require header in the outgoing INVITE request.
	<b>support-add</b>	Adds 100rel Support header in the outgoing INVITE request.

**Command Default** 100rel interworking is disabled.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to enable 100rel Require header option in the outgoing INVITE request:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# 100rel outbound require-add
Router(config-sbc-sbe-adj-sip)#
```

The following example shows how to enable 100rel Support header option in the outgoing INVITE request:

```
Router(config-sbc-sbe-adj-sip)# 100rel outbound support-add
Router(config-sbc-sbe-adj-sip)#
```

# account (session border controller)

To define a SIP or H.323 adjacency account on an SBE, use the **account** command in the appropriate configuration mode. To remove this definition, use the **no** form of this command.

**account** *account-name*

**no account** *account-name*

<b>Syntax Description</b>	<p><i>account-name</i> Specifies the SBE account name.</p> <p>The <i>account-name</i> can have a maximum of 32 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	--

<b>Command Default</b>	No account name is associated with the adjacency.
------------------------	---

<b>Command Modes</b>	<p>Adjacency SIP configuration (config-sbc-sbe-adj-sip)</p> <p>Adjacency H.323 configuration (config-sbc-sbe-adj-h323)</p>
----------------------	--

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the H.323 adjacency h323ToIsp42 to account isp42:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 SipToIsp42
Router(config-sbc-sbe-adj-h323)# account isp42
```

The following example shows how to configure the SIP adjacency SipToIsp42 to account isp42:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# account isp42
```

# action (body)

To set the action to take on a body type in a SIP body profile for a non-SDP message body, use the **action (body)** command in SBE configuration mode. To restore the default behavior of **action nopass**, use the **no action** command.

**action** [*pass* | *nopass* | *strip* | *reject*]

**no action** [*pass* | *nopass* | *strip* | *reject*]

## Syntax Description

pass	Instructs the SBC to pass through the body type of the non-SDP message body.
nopass	Uses the handling parameter in the message to determine whether to strip the body or reject the entire message with error code 415 (Unsupported media type).
strip	Strips the body and passes the rest of the message.
reject	Rejects the entire message with an error code.

## Command Default

The command default is **action nopass**.

## Command Modes

SBE SIP Body Element configuration (config-sbc-sbe-sip-body-ele)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The **action (body)** command is used in conjunction with the **sip body-profile** *{profile\_name}* and **body** *{body\_name}* commands to complete the configuration.

After creating a body profile with the **sip body-profile** *{profile\_name}* command, you can associate the body profile at the following levels and configuration modes:

- At the SIP signaling entity level (ingress or egress), under SBE mode, using the **sip default body-profile** **[[inbound|outbound]** *{profile\_name}* command. The body profile is associated for the entire signaling instance (that is all messages, either ingress or egress, passing through the SBC).
- SIP adjacency level, under SIP adjacency mode, using the **body-profile** **[[inbound|outbound]** *{profile\_name}* command. The body profile is associated to an adjacency.
- At SIP method profile level, under method profile mode, using the **body-profile** *{profile\_name}* command. The body profile is associated to a method profile.

SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

**Examples**

The following example creates a body profile named `bodyprofile1`, associates the body profile at the SIP signaling level for all inbound calls passing through the SBC, describes the body type that is to act on messages with the "application/ISUP" content-type header, and instructs SBC to strip that particular message body and pass the rest of the message.

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-profile bodyprofile1
Router(config-sbc-sbe)# sip default body-profile inbound bodyprofile1
Router(config-sbc-sbe-sip-body)# body application/ISUP
Router(config-sbc-sbe-sip-body-ele)# action strip
Router(config-sbc-sbe-sip-body-ele)#
```

**Related Commands**

Command	Description
<code>sip default body-profile</code>	Associates a body profile at the SIP signaling level under the SBE mode.
<code>body-profile</code>	Associates a body profile to a method profile under the method profile mode.
<code>body-profile (sip adj)</code>	Associates a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
<code>sip body-profile</code>	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
<code>body</code>	Names a body type or content header type for a non-SDP message body that is part of the body profile.

# action (body editor)

To set an action to be taken on a body type in a SIP body editor for a non-SDP message body, use the **action** command in the signaling border element (SBE) SIP body element configuration mode. To remove the action, use the **no** form of this command.

**action** [*pass* | *nopass* | *strip* | *reject*]

**no action**

## Syntax Description

pass	Instructs the session border controller (SBC) to pass through the body type of the non-SDP message body.
nopass	Uses the handling parameter in the message to determine whether to strip the body or reject the entire message with the error code 415, which is unsupported media type.
strip	Strips the body and passes the rest of the message.
reject	Rejects the entire message.

## Command Default

No default behavior or values are available.

## Command Modes

SBE SIP body element configuration (config-sbc-sbe-mep-bdy-ele)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The **action (body)** command is used in conjunction with the **sip body-editor** {*editor-name*} and **body** {*word*} commands to complete the configuration.

The SBC uses a body editor that you have created and associated, to filter the non-SDP bodies from the incoming and outgoing SIP messages, based on the Content Type header field. A body editor allows a message containing a specific non-SDP body to be passed (without altering the message), stripped off the body (and pass the rest of the message), or rejected.

## Examples

The following example shows how to create a body editor named bodyeditor1, describe the body type, that is to act on the messages with the *application/ISUP* Content Type header, and instruct the SBC to strip that particular message body and pass the rest of the message:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-editor bodyeditor1
Router(config-sbc-sbe-mep-bdy)# body application/ISUP
Router(config-sbc-sbe-mep-bdy-ele)# action strip
Router(config-sbc-sbe-mep-bdy-ele)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	body	Names a body type or content header type for a non-SDP message body that is a part of a body editor.
	body-editor	Associates a body editor at a SIP adjacency level to an adjacency in the SIP adjacency mode.
	sip body-editor	Creates a body editor to filter the non-SDP bodies from the incoming and outgoing SIP messages.

# action (CAC)

To configure the action to perform after this entry in an admission control table, use the **action** command in CAC table entry configuration mode.

**action** { **cac-complete** | **next-table** *goto-table-name* }

**no action** { **cac-complete** | **next-table** *goto-table-name* }

## Syntax Description

<b>cac-complete</b>	Indicates an event matches, this CAC policy is complete.
<b>next-table</b>	Specifies the name of the next cac table.
<i>goto-table-name</i>	Table name identifying the next CAC table to process (or cac-complete, if processing should stop).

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the next table to process for the entry in the new admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# table-type limit src-account
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
```

## Related Commands

Command	Description
action (NA-)	Configures the action to perform after an entry in an admission control table.
action (RTG-SRC)	Configures the action to take if a routing entry is chosen.





# action drop-msg

To add an action of dropping the message to a SIP message profile, use the **action drop-msg** command in SIP header-profile configuration mode. To remove the method from the profile, use the **no** form of this command.

```
action drop-msg
```

```
no action drop-msg
```

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SIP header configuration (config-sbc-sbe-sip-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows action of dropping the message to a SIP message profile to the header profile Myprofile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile Myprofile
Router(config-sbc-sbe-sip-hdr)# action drop-msg
```

Related Commands	Command	Description
	<b>sip header-profile</b>	Configures a header profile.

## action (header-editor)

To configure an action that is to be taken on an element type in a header editor or parameter editor, use the **action** command in the appropriate configuration mode. To remove an action from the element type, use the **no** form of this command.

```
action { add-first-header | add-header | replace-name | replace-value } { value word }
```

```
action { as-editor | drop-msg | pass | strip }
```

```
action reject [status-code code-number]
```

```
no action
```

Syntax	Description
<b>add-first-header</b>	Adds the first occurrence of a header (no action occurs if a header already exists).
<b>add-header</b>	Adds a header irrespective of whether or not a header already exists.
<b>as-editor</b>	Default editor action (whitelist or blacklist).
<b>drop-msg</b>	Drops the message.
<b>pass</b>	Passes on the header.
<b>reject</b>	Rejects a request if this header is present, specifically for INVITE headers.
<b>replace-name</b>	Replaces the header name.
<b>replace-value</b>	Replaces the header content (value).
<b>strip</b>	Unconditionally strips the matched body, header, or parameter element.
<b>value</b>	Specifies the string used in conjunction with the action.
<i>word</i>	String used in the action. It can be upto 256 characters.
<b>status-code</b>	Specifies the SIP status code for the response.
<i>code-number</i>	SIP status-code number that can range from 300 to 699. By default, it is 488.

**Command Default** By default, the *code-number* is 488.

**Command Modes** SBE Header Editor Header configuration (config-sbc-sbe-mep-hdr-ele)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, you must remove the existing configuration first.

**Examples**

The following example shows how to set the as-editor action for the To header element type in the headerprof1 parameter editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor headerprof1
Router(config-sbc-sbe-mep-hdr)# header To
Router(config-sbc-sbe-mep-hdr-ele)# action as-editor
```

**Related Commands**

Command	Description
<b>header</b>	Configures a header element in a header editor.
<b>parameter-editor</b>	Configures a parameter element in a parameter editor.
<b>sip header-editor</b>	Configures a header editor.

## action (method-editor)

To configure an action to be taken on a method editor, use the **action** command in the signaling border element (SBE) method editor element configuration mode. To deconfigure an action, use the **no** form of this command.

```
action {as-editor | pass | reject}
```

```
no action
```

Syntax Description	as-editor	Passes the method for the whitelist method editor, and rejects for the blacklist method editor.
	pass	Passes the method.
	reject	Rejects the method.

**Command Default** The default is the **as-editor** keyword.

**Command Modes** SBE method editor element configuration (config-sbc-sbe-mep-mth-ele)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows the reject action:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-editor editor1
Router(config-sbc-sbe-mep-mth)# description mysbc editor1
Router(config-sbc-sbe-mep-mth)# blacklist
Router(config-sbc-sbe-mep-mth)# method test
Router(config-sbc-sbe-mep-mth-ele)# action reject
Router(config-sbc-sbe-mep-mth-ele)# end
```

Related Commands	Command	Description
	<b>header</b>	Configures a header element in a header editor.
	<b>parameter-editor</b>	Configures a parameter element in a parameter editor.



## action (method profile)

To configure the action to take on a method profile, use the **action** command in the SBE method profile element configuration mode. To remove the action on a method profile, use the **no** form of this command.

```
action {as-profile | pass | reject}
```

```
no action
```

Syntax Description		
	as-profile	Drops the method. This is the default
	pass	Passes the method.
	reject	Rejects the method.

**Command Default** The default is as-profile.

**Command Modes** SBE method profile element configuration (config-sbc-sbe-sip-mth-ele)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows the action to drop the method:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile profile1
Router(config-sbc-sbe-sip-mth)# description mysbc profile1
Router(config-sbc-sbe-sip-mth)# blacklist
Router(config-sbc-sbe-sip-mth)# pass-body
Router(config-sbc-sbe-sip-mth)# method test
Router(config-sbc-sbe-sip-mth-ele)# action as-profile
Router(config-sbc-sbe-sip-mth-ele)# end
```

Related Commands	Command	Description
	<b>header</b>	Configures a header element in a header profile.
	<b>parameter-profile</b>	Configures a parameter element in a parameter profile.

# action (NA-)

To configure the action of an entry in the number analysis table with entries of the table matching a source number (prefix or whole number), a dialed number (prefix or whole number) or the source adjacency or account, use the **action (NA-)** command in the Number analysis table configuration mode. To deconfigure the action, use the **no** form of this command.

**action** { **next-table** *goto-table-name* | **accept** | **reject** }

**no action**

Syntax Description	next-table	Specifies the next number analysis table to process, if the event matches this entry.
	<i>goto-table-name</i>	
	<b>accept</b>	Configures the call to be accepted if it matches the entry in the table.
	<b>reject</b>	Configures the call to be rejected if it matches the entry in the table.

**Command Default** No default behavior or values are available.

**Command Modes** Number analysis table configuration (config-sbc-sbe-rtgpolicy-natable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	This command was updated to support source number analysis.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the call to be accepted if it matches the entry in the new number analysis table MyNaTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-number-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# action accept
```

The following example shows how to configure the call to be accepted if it matches the start of the entry in the new number analysis table MyNaTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
```



```

Router(config-sbc-sbe) # call-policy-set 1
Router(config-sbc-sbe-rtgpolicy) # na-dst-prefix-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable) # entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry) # action accept

```

The following example shows how to configure the call to be accepted if it matches the source adjacency entry in the new number analysis table MyNaTable:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc) # sbe
Router(config-sbc-sbe) # call-policy-set 1
Router(config-sbc-sbe-rtgpolicy) # na-src-adjacency-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable) # entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry) # action accept

```

The following example shows how to configure the call to be accepted if it matches the source account entry in the new number analysis table MyNaTable:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc) # sbe
Router(config-sbc-sbe) # call-policy-set 1
Router(config-sbc-sbe-rtgpolicy) # na-src-account-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable) # entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry) # action accept

```

#### Related Commands

Command	Description
action (CAC)	Configures the action to perform after an entry in an admission control table.
action (RTG-SRC)	Configures the action to take if a routing entry is chosen.

# action (parameter)

To configure the action to take on an element type in a parameter, use the **action** command in the appropriate configuration mode. To remove an action from the element type, use the **no** form of this command.

**action** { **add-not-present** | **add-or-replace** | **strip** }

**no action** { **add-not-present** | **add-or-replace** | **strip** }

## Syntax Description

<b>add-not-present</b>	Adds the parameter if it is not present.
<b>add-or-replace</b>	Adds the parameter if it is not present or replace the parameter if it is present.
<b>strip</b>	Strips out the parameter if it is present.

## Command Default

The default parameter action is **strip**.

The default header action is **strip**.

## Command Modes

SBE header profile header configuration (config-sbc-sbe-sip-hdr-ele)

SBE parameter profile parameter configuration (config-sbc-sbe-sip-prm-ele)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.

## Examples

The following example shows how to set the action for parameter element type user in parameter profile paramprof1 to add-not-present:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-profile paramprof1
Router(config-sbc-sbe-sip-prm)# parameter user
Router(config-sbc-sbe-sip-prm-ele)# action add-not-present value phone
```

The following example shows how to set the action for header element type To in parameter profile headerprof1 to as-profile:

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# sip header-profile headerprof1  
Router(config-sbc-sbe-sip-hdr)# header To  
Router(config-sbc-sbe-sip-hdr-ele)# action as-profile
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>header</b>	Configures a header element in a header profile.
<b>parameter</b>	Configures a parameter element in a parameter profile.

# action (parameter editor)

To configure an action to be taken on an element type in a parameter editor, use the **action** command in the SIP Parameter Editor Element configuration mode. To remove an action from an element type, use the **no** form of this command.

**action** {**add-not-present** | **add-or-replace**} {**value**} {*word* | **private-ip-address** | **public-ip-address**}

action strip

**no action**

## Syntax Description

<b>add-not-present</b>	Adds the parameter if it is not present.
<b>add-or-replace</b>	Adds the parameter if it is not present, or replaces the parameter if it is present.
<b>value</b>	Specifies the value of the parameter to be added or replaced.
<i>word</i>	Description of the action. Length can be a maximum of 30 characters.
<b>private-ip-address</b>	Specifies the value of the parameter as the private IP address.
<b>public-ip-address</b>	Specifies the value of the parameter as the public IP address.
<b>strip</b>	Strips out the parameter if it is present.

## Command Default

By default, **strip** is used.

## Command Modes

SIP Parameter Editor Element configuration (config-sbc-sbe-mep-prm-ele)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to set the add-not-present action for the parameter element type user in the paramedit1 parameter editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-editor paramedit1
Router(config-sbc-sbe-mep-prm)# parameter user
Router(config-sbc-sbe-mep-prm-ele)# action add-not-present value phone
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>parameter</b>	Configures a parameter element in a parameter editor.
<b>sip parameter-editor</b>	Configures a parameter editor.

# action (RTG-)

To configure the action to take if a routing entry is chosen, use the **action** command in the RTG routing table configuration mode. To delete the action, use the **no** form of this command.

**action** { **next-table** *goto-table-name* | **complete** | **reject** }

**no action**

## Syntax Description

<b>next-table</b> <i>goto-table-name</i>	Specifies the next routing table to process if the event matches the entry.
<b>complete</b>	Completes the action.
<b>reject</b>	Rejects the indicated action.

## Command Default

No default behavior or values are available.

## Command Modes

RTG routing table configuration (config-sbc-sbe-rtgpolicy-rtgtable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action reject
```

The following example shows how to configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-adjacency 1471
```

```
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action reject
```

The following example shows how to configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-account-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-account 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action reject
```

The following example shows how to configure the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-round-robin-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
```

The following example configures the match-value of an entry in the new routing table MyRtgTable and if any calls match this criterion, they are rejected.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 1471
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
```

## Related Commands

Command	Description
action (NA-)	Configures the action of an entry in the number analysis table with entries of the table matching a dialed number (prefix or whole number) or the source adjacency or account.
action (CAC)	Configures the action to perform after an entry in an admission control table.

# action (SDP)

To configure an SDP policy table action, use the **action** command in sdp match table configuration mode. To return to the default, use the **no** form of this command.

**action** { **whitelist** | **blacklist** }

**no action**

## Syntax Description

whitelist	Allow the defined set of attributes and block the rest.
blacklist	Block the defined set of attributes and allow the rest. This is the default.

## Command Default

The default action is blacklist.

## Command Modes

SDP match table configuration (config-sbc-sbe-sdp-match-tbl)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows action of dropping the message to a SIP message profile to the header profile Myprofile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sdp-match-table 1
Router(config-sbc-sbe-sdp-match-tbl)# action blacklist
```

## Related Commands

Command	Description
sdp-match-table	Creates an SDP match table.
match-string	Configures an SDP attribute matching string.
sdp-policy-table	<b>Configures</b> an SDP policy table.



## action (SIP)

To configure the action to take on an element type in a header or parameter profile, use the **action** command in the appropriate configuration mode. To remove an action from the element type, use the **no** form of this command.

```
action { add-first-header | add-header | as-profile | drop-msg | pass | replace-name |
replace-value | strip }
```

```
no action { add-first-header | add-header | as-profile | drop-msg | pass | replace-name |
replace-value | strip }
```

### Syntax Description

add-first-header	Adds the first occurrence of a header (no action if a header exists).
<b>add-header</b>	Adds a header whether or not one already exists.
as-profile	Default profile action (whitelist or blacklist).
drop-msg	Drops the message.
pass	Pass on the header.
replace-name	Replace the header name.
replace-value	Replace the header content (value).
<b>strip</b>	Unconditionally strips the matched body, header, or parameter element.

### Command Default

The default body action is **strip**.

The default parameter action is **strip**.

The default header action is **strip**.

### Command Modes

SBE header profile header configuration (config-sbc-sbe-sip-hdr-ele)

SBE parameter profile parameter configuration (config-sbc-sbe-sip-prm-ele)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.

**Examples**

The following example shows how to set the action for parameter element type user in parameter profile paramprof1 to add-not-present:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-profile paramprof1
Router(config-sbc-sbe-sip-prm)# parameter user
Router(config-sbc-sbe-sip-prm-ele)# action add-not-present value phone
```

The following example shows how to set the action for header element type To in parameter profile headerprof1 to as-profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile headerprof1
Router(config-sbc-sbe-sip-hdr)# header To
Router(config-sbc-sbe-sip-hdr-ele)# action as-profile
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>header</b>	Configures a header element in a header profile.
<b>parameter-profile</b>	Configures a parameter element in a parameter profile.

# activate (billing)

To activate billing once it is configured, use the **activate** command in SBE billing configuration mode.

**activate**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, billing is not activated.

**Command Modes** SBE billing configuration (config-sbc-sbe-billing)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.

You can activate billing only after the RADIUS configuration has been activated.

**Examples** The following example shows how to activate the billing functionality after configuration is committed:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# activate
```

## Related Commands

Command	Description
<b>billing</b>	Configures billing.
ldr-check	Configures the time of day (local time) to run the Long Duration Check (LDR).
<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
method packetcable-em	Enables the packet-cable billing method.

<b>Command</b>	<b>Description</b>
packetcable-em <i>transport radius</i>	Configures a packet-cable billing instance.
show sbc sbe billing remote	Displays the local and billing configurations.

## activate (enum)

To activate ENUM client, use the **activate** command in ENUM configuration mode. To deactivate ENUM client, use the no form of this command.

**activate**

**no activate**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** ENUM configuration (config-sbc-sbe-enum)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to activate ENUM client:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# activate
```

Related Commands	Command	Description
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
	<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.

<b>Command</b>	<b>Description</b>
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe</b> <b>call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum</b> <b>entry</b>	Displays the contents of an ENUM client entry.

# activate (radius)

To activate the RADIUS client, use the **activate** command in the appropriate configuration mode. To disable this command, use the **no** form of this command.

**activate**

**no activate**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Default is the **no** form of the command.

**Command Modes** Server accounting (config-sbc-sbe-acc)  
Server authentication (config-sbc-sbe-auth)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to activate the RADIUS client.

```
Router# configure terminal
Router(config)# sbc uut105-1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting SBC1-account-1
Router(config-sbc-sbe-acc)# activate
```

Related Commands	Command	Description
	<b>retry-interval</b>	Sets the retry interval to connect to the RADIUS server.
	<b>retry-limit</b>	Sets the retry interval to the RADIUS server.
	<b>concurrent-requests</b>	Sets the maximum number of concurrent requests to the RADIUS server.

# activate (session border controller)

To start the Session Border Controller (SBC) service when all signaling border element (SBE) or data border element (DBE) address configuration have been successfully committed, use the **activate** command in the appropriate configuration mode. To deactivate the SBE service of the SBC, use the **no** form of this command.

**activate**

**no activate**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Default is the **no** form of the command.

**Command Modes** DBE configuration (config-sbc-dbe)  
SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.4	SBE support added for unified SBC.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The command is not completed even when the CLI returns; there is an asynchronous process (activation or deactivation) going on and the new instruction is not actioned until the last one completes.

**Examples** The following example shows how to activate the DBE on the service mySbc:

```
Router# configur
Router(config)# sbc mySbc dbe
Router (config-sbc-dbe)# activate
```

The following example shows how to activate the SBE on the service mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router (config-sbc)# sbe
Router (config-sbc-sbe)# activate
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>deact-mode</b>	Indicates how to implement the deactivation of an SBE.

# cac-policy-set global

To activate the global call admission control (CAC) policy set within an signaling border element (SBE) entity, use the **cac-policy-set global** command in the SBE configuration mode.

**cac-policy-set global** *policy-set-id*

<b>Syntax Description</b>	<i>policy-set-id</i> Integer identifying the policy set that should be made global. Range is from 1 to 2147483647.
---------------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was replaced by the <b>cac-policy-set global</b> command.

**Usage Guidelines** The active CAC policy set cannot be modified.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to activate policy set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# cac-policy-set global 1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cac-policy-set</b>	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
	<b>show sbc sbe cac-policy-set</b>	Lists detailed information pertaining to a CAC policy table.

# call-policy-set default

To activate a default policy set within a signaling border element (SBE) entity, use the **call-policy-set default** command in the SBE configuration mode. To deactivate a default policy set, use the **no** form of this command.

**call-policy-set default** *policy-set-id*

**no call-policy-set default**

<b>Syntax Description</b>	<i>policy-set-id</i>	Number that identifies the default call policy set. The range is from 1 to 2147483647.
---------------------------	----------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was replaced by the <b>call-policy-set default</b> command.

**Usage Guidelines**

If another policy set was previously active, it is made inactive by executing this command. The SBE is created with no active routing policy set; an active routing policy set must be explicitly configured using this command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples**

The following example shows how to set policy set 1 as the default on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# call-policy-set default 20
```

Related Commands	Command	Description
	<b>call-policy-set</b>	Creates a policy set on the session border controller (SBC).
	<b>first-inbound-na-table</b>	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
	<b>first-outbound-na-table</b>	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
	<b>show sbc sbe call-policy-set</b>	Lists the details of the policy sets configured on the SBC.
	<b>show sbc sbe call-policy-set default</b>	Lists the summary of the default policy set configured on the SBC.

# active-script-set

To activate a script set, use the **active-script-set** command in the SBE configuration mode. To change the active script set to the inactive state, use the **no** form of this command. Only one script set can be active on the SBC at any given point in time. When you use the **no** form of this command, script-based editing is temporarily disabled.

**active-script-set** *script-set-number*

**no active-script-set**

## Syntax Description

<i>script-set-number</i>	Script set number. This is the number that you set when you run the <b>script-set lua</b> command.
--------------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

At any particular point of time, only one script can be in the active state on the SBC. When you run the **active-script-set** command for a particular script set, the script set that was previously active automatically goes to the inactive state. The editors in an inactive script set are not applied to SIP messages. You can switch an inactive script set to the active state by running the **active script-set** command on it. To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **active-script-set** command is used to activate the script set with the number 10:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# script-set 10 lua
Router(config-sbc-sbe-script-set)# script mySBCScript
Router(config-sbc-sbe-scrpset-script)# load-order 2
Router(config-sbc-sbe-scrpset-script)# type wrapped edit-point both
Router(config-sbc-sbe-scrpset-script)# filename bootflash:mySBCScript.lua
Router(config-sbc-sbe-scrpset-script)# exit
Router(config-sbc-sbe-script-set)# complete
```

```
Router(config-sbc-sbe-script-set)# exit
Router(config-sbc-sbe)# active-script-set 10
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
<b>editor</b>	Specifies the order in which a particular editor must be applied.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

## address ipv4 (session border controller)

To configure the address of the RADIUS server, use the **address** command in the Server accounting configuration mode. To deconfigure the active accounting server address, use the **no** form of this command.

*address ipv4 A.B.C.D.*

*no address ipv4 A.B.C.D.*

<b>Syntax Description</b>	<i>A.B.C.D.</i>	IP address of the RADIUS server.
---------------------------	-----------------	----------------------------------

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Server accounting (config-sbc-sbe-acc-ser)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	Any number of accounting servers can be specified. Call Detail Reports are sent to the accounting server with the highest priority upon call termination.
-------------------------	---

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

<b>Examples</b>	The following command configures accounting servers castor and pollux on mySbc for Remote Authentication Dial-In User Service (RADIUS) client instance radius1:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# radius accounting radius1
(config-sbc-sbe-acc)# server castor
(config-sbc-sbe-acc-ser)# address ipv4 10.0.0.1
(config-sbc-sbe-acc-ser)# exit
(config-sbc-sbe-acc)# server pollux
(config-sbc-sbe-acc-ser)# address pollux
(config-sbc-sbe-acc-ser)# exit
```

# address (session border controller)

To configure either an IP address or a host name to act as a redundant peer, use the **address** command in adjacency Session Initiation Protocol (SIP) peer configuration mode. To deconfigure an IP address or a host name, use the **no** form of this command.

**address** *address*

**no address** *address*

## Syntax Description

<i>address</i>	The IP address or host name of a peer.
----------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP peer configuration (config-sbc-sbe-adj-sip-peer)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how the **address** command is used to configure an IP address or a host name to act as a redundant peer on a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# redundant peer 1
Router(config-sbe-adj-sip-peer)# address sbc1
```

## Related Commands

Command	Description
network	Configures either an IPv4 or IPv6 network in a redundant peer.
port	Configures a port for redundant peer.
priority	Configures a redundant peer's priority.
redundant peer	Configures an alternative signaling peer for an adjacency.





# adjacency

To configure an adjacency for an Session Border Controller (SBC) service, use the **adjacency** command in SBE configuration mode. To deconfigure the adjacency, use the **no** form of this command.

**adjacency** {**sip** | **h323**} *adjacency-name*

**no adjacency** {**sip** | **h323**} *adjacency-name*

## Syntax Description

<b>sip</b>	Enters the mode of an SBE SIP adjacency, often called adjacency sip mode, to configure a destination SIP adjacency.
<b>h323</b>	Enters the mode of an SBE H.323 adjacency, often called adjacency h323, to configure a destination H.323 adjacency.
<i>adjacency-name</i>	Specifies the name of the SBE SIP or H.323 adjacency.  The <i>adjacency-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section below shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **adjacency** command configures a SIP adjacency named sipGW, and enters into adjacency sip mode.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip sipGW
Router(config-sbc-sbe-adj-sip)#
```

The following example shows how the **adjacency** command configures an H.323 adjacency named H323ToIsp42, and enters into adjacency h323 mode.

```
Router# configure terminal
Router(config)# sbc mySbc
```

```
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 H323ToIsp42
Router(config-sbc-sbe-adj-h323)#
```

# adjacency h248

To configure an H.248 Border Access Controller (BAC) access adjacency and core adjacency, use the **adjacency h248** command in the H248 BAC configuration mode. To unconfigure an H.248 BAC access adjacency and core adjacency, use the **no** form of this command.

```
adjacency h248 {access access-adjacency name}
```

```
adjacency h248 {core core-adjacency name}
```

```
no adjacency h248 {access access-adjacency name} | {core core-adjacency name}
```

## Syntax Description

<b>h248</b>	Specifies an adjacency for an H.248 BAC.
<b>access</b>	Specifies an access adjacency.
<i>access-adjacency name</i>	Name of the access adjacency.  The <i>access-adjacency name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
<b>core</b>	Specifies a core adjacency.
<i>core-adjacency name</i>	Name of the core adjacency.  The <i>core-adjacency name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

## Command Default

None

## Command Modes

H248 BAC configuration (config-h248-bac)

## Command History

Release	Modification
Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

When you configure an access adjacency, the **adjacency h248** command enters the access adjacency submenu.

When you configure a core adjacency, the **adjacency h248** command enters the core adjacency submenu.

## Examples

The following example shows how the **adjacency h248** command is used to configure an H.248 BAC access adjacency:

```
Router# configure terminal  
Router(config)# sbc h248 bac  
Router(config-h248-bac)# adjacency h248 access iad_80_123
```

The following example shows how the **adjacency h248** command is used to configure an H.248 BAC core adjacency:

```
Router# configure terminal  
Router(config)# sbc h248 bac  
Router(config-h248-bac)# adjacency h248 core core_spec2
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>core-adj</b>	Binds an H.248 BAC core djacency with its corresponding H.248 BAC access adjacency.

# adjacency timeout

To configure the adjacency retry timeout interval, use the **adjacency timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**adjacency timeout** *value*

**no adjacency timeout** *value*

<b>Syntax Description</b>	<i>value</i>	Specifies the timeout period in milliseconds. Valid values are from 10000 to 30000. The default value is 30 seconds.
---------------------------	--------------	--

<b>Command Default</b>	The default value is 30 seconds.
------------------------	----------------------------------

<b>Command Modes</b>	Adjacency H.323 configuration (config-sbc-sbe-adj-h323) H.323 configuration (config-sbc-sbe-h323)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>adjacency timeout</b> command configures adjacency retry timeout in adjacency H.323 configuration mode:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# adjacency timeout 10000
```

The following example shows how the **adjacency timeout** command configures adjacency retry timeout in H.323 configuration mode.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# adjacency timeout 10000
```

# admin-domain

To configure an administrative domain, use the **admin-domain** command in the Signaling border element (SBE) configuration mode. To deconfigure an administrative domain, use the **no** form of this command.

**admin-domain** *name*

**no admin-domain** *name*

## Syntax Description

<i>name</i>	The name of an administrative domain.  The <i>name</i> field can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration mode (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

The command enables the user to enter into the administrative domain mode. The policy set that is to be used for an administrative domain is defined in the administrative domain mode. A user can specify only one CAC policy set to be used for the administrative domain. A user can also define separate call policy sets for inbound number analysis, routing policy, and outbound number analysis. If the policies are not specified, the default call policy set is used.

The policy sets must be in a complete state before they can be assigned to an administrative domain. A default call policy set must be configured before the administrative domain mode can be entered.

## Examples

The following example shows how to configure an administrative domain in the SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set default 25 priority 1
Router(config-sbc-sbe)# admin-domain ADMINDOMAIN
Router(config-sbc-sbe-ad)# description This is the description of the admin-domain 1
```

```

Router(config-sbc-sbe-ad) # call-policy-set inbound-na 2 priority 1
Router(config-sbc-sbe-ad) # call-policy-set outbound-na 3 priority 1
Router(config-sbc-sbe-ad) # call-policy-set rtg 2 priority 1
Router(config-sbc-sbe-ad) # cac-policy-set 2
Router(config-sbc-sbe-ad) # exit

```

**Related Commands**

Command	Description
cac-policy-set (admin-domain)	Configures the call admission control (CAC) policy set for an administrative domain.
call-policy-set (admin-domain)	Configures the inbound and outbound number analysis and routing policy set for an administrative domain.
show sbc sbe admin-domain	Lists the administrative domains on the Session Border Controller (SBC) and per adjacency.



## admin-domain (adjacency)

To associate an administrative domain to an adjacency, use the **admin-domain** command in the Session Initiation Protocol (SIP) adjacency and an H.323 adjacency configuration mode. To remove the association of an administrative domain from an adjacency, use the **no** form of this command.

**admin-domain** *name*

**no admin-domain** *name*

### Syntax Description

<i>name</i>	Specifies the name of an administrative domain.  The <i>name</i> field can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------	---

### Command Default

No default behavior or values are available.

### Command Modes

SIP adjacency mode (config-sbc-sbe-adj-sip)  
H.323 adjacency mode (config-sbc-sbe-adj-h323)

### Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

In the SIP and H.323 adjacency modes, the user can configure up to two optional administrative domains on an adjacency. A separate **admin-domain** command is configured for every administrative domain. An administrative domain can be configured for both the SIP adjacency and the H323 adjacency. However, the H.323 adjacency must be unattached in order to be able to add, delete, or modify the administrative domain.

### Examples

The following example shows how to assign the administrative domain to a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# admin-domain ADMINDOMAIN
Router(config-sbc-sbe-adj-sip)#
```

Related Commands	Command	Description
	cac-policy-set (admin-domain)	Configures the call admission control (CAC) policy set for an administrative domain.
	call-policy-set (admin-domain)	Configures the inbound and outbound number analysis and routing policy set for an administrative domain.
	show sbc sbe admin-domain	Lists the administrative domains on the Session Border Controller (SBC) and per adjacency.

# alias (session border controller)

To configure the endpoint alias of an H.323 adjacency, use the **alias** command in adjacency H.323 configuration mode. To remove this configuration, use the **no** form of this command.

**alias** *alias-name*

**no alias**

<b>Syntax Description</b>	<p><i>alias-name</i> Specifies the alias of the H.323 adjacency endpoint.</p> <p>The <i>alias-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency H.323 configuration (config-sbc-sbe-adj-h323)
----------------------	---

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the H.323 adjacency h323ToIsp42 endpoint alias to end1:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# alias end1
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>attach-controller</b></td> <td>Configures a DBE to attach to a controller.</td> </tr> </tbody> </table>	Command	Description	<b>attach-controller</b>	Configures a DBE to attach to a controller.
Command	Description				
<b>attach-controller</b>	Configures a DBE to attach to a controller.				

# allow diff-med-sig-vpn

To allow media and signaling to use different VPN IDs in a call leg, use the **allow diff-med-sig-vpn** command in the session border controller (SBC) configuration mode. To allow media and signaling to use the same VPN ID in a call leg, use the **no** form of this command.

**allow diff-med-sig-vpn**

**no allow diff-med-sig-vpn**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default values are available.

**Command Modes** SBC configuration (config-sbc)

Command History	Release	Modification
	Cisco IOS XE Release 3.5.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Ensure that the SBC is deactivated before running the **allow diff-med-sig-vpn** command.

If the SBC is active and you run the **allow diff-med-sig-vpn** command, the system issues a warning message, asking you to first deactivate the SBC. You can reactivate the SBC using the **activate** command.

Use the **show run** command to display the output of the **allow diff-med-sig-vpn** command.

**Examples** The following example shows how the **allow diff-med-sig-vpn** command allows media and signaling to use different VPN IDs in a call leg:

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# no activate
Router(config-sbc)# allow diff-med-sig-vpn
Router(config-sbc)# activate
Router(config-sbc)# exit
```

# allow private info

To configure an H.323 adjacency to allow private information on messages sent out by the adjacency, use the **allow private info** command in the adjacencyH.323 configuration mode. To disallow private information on messages sent out by the adjacency, use the **no** form of this command.

**allow private info**

**no allow private info**

## Syntax Description

This command has no arguments or keywords.

## Command Default

By default, the H.323 adjacency does not send private information.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Please note that if you configure the H.323 adjacency to allow private information, then it will allow private information on messages even if the CAC policy is configured to apply privacy service or the user requests privacy service.

## Examples

The following example shows how the **allow private info** command is used to configure an H.323 adjacency to allow private information on messages sent by the adjacency.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323ToIsp422
Router(config-sbc-sbe-adj-h323)# allow private info
```

## Related Commands

Command	Description
<b>privacy restrict outbound</b>	Configures an H.323 adjacency to apply privacy restriction on outbound messages if the user requests it.

# associate dspfarm profile

To associate the session border controller (SBC) with a digital signal processor (DSP) farm profile, use the **associate dspfarm profile** command in the SBC and SBC-DBE configuration modes. To remove the association with a DSP farm profile, use the **no** form of this command.

**associate dspfarm profile** {*profile-number* | **all**}

**no associate dspfarm profile** {*profile-number* | **all**}

## Syntax Description

<i>profile-number</i>	The DSP farm profile number the SBC is to associate with.
<b>all</b>	The SBC picks one of the DSP farm profiles associated with the SBC for its transcoding session.

## Command Default

No default behavior or values.

## Command Modes

SBC and SBC-DBE configuration (config-sbc-dbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to associate the SBC with a DSP farm profile using the **associate dspfarm profile** command in the SBC-DBE mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC dbe
Router(config-sbc-dbe)# associate dspfarm profile 1
```

# attach-controllers (session border controller)

To configure a DBE to attach to an H.248 controller, use the **attach-controllers** command in VDBE configuration mode. To detach the DBE from its controller, use the **no** form of this command.

**attach-controllers**

**no attach-controllers**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The default is that no controllers are attached.

**Command Modes** VDBE configuration mode (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** The attachment and detachment of the DBE from its controller does not always complete immediately. To view the current attachment status, use the **show sbc dbe controllers** command.

**Examples** In a configuration where the DBE has been created and controllers have been configured, the following example shows how to attach the DBE to a controller in VDBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# attach-controllers
```

Related Commands	Command	Description
	vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.
	show sbc dbe controllers	Lists the media gateway controllers configured on each vDBE and its controller address.

# attach (H.248 BAC)

To set the Border Access Controller (BAC) adjacency state to Attached, use the **attach** command in the H248 BAC adjacency configuration mode. To set the BAC adjacency state to Detached, use the **no** form of this command.

**attach**

**no attach**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** H248 BAC adjacency configuration (config-h248-bac-adj)

Command History	Release	Modification
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **attach** command is used to set the BAC adjacency state:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# attach
```



## attach (Rf billing)

To attach an origin realm or an origin host to a Rf billing on an Element (SBE), use the **attach** command in the SBC SBE billing Rf configuration mode. To detach an origin realm or an origin host to a Rf billing on an SBE, use the **no** form of this command.

**attach**

**no attach**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None.

**Command Modes** SBC SBE billing Rf configuration (config-sbc-sbe-billing-rf)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to attach the an origin realm to an Rf billing on an SBE:

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# rf 0
Router(config-sbc-sbe-billing-rf)# origin-realm mySBC
Router(config-sbc-sbe-billing-rf)# attach
```

## attach (session border controller)

To attach an adjacency to an account on an SBE, use the **attach** command in the appropriate configuration mode. To detach the adjacency from an account on an SBE, use the **no** form of this command.

**attach**

**no attach** *force* [*abort* | *normal*]

### Syntax Description

<i>force</i>	Executes a forced detach.
<i>abort</i>	Tears down calls without signaling an end.
<i>normal</i>	Tears down calls gracefully.

### Command Default

Default is the **no** form of the command.

### Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
Adjacency SIP configuration (config-sbc-sbe-adj-sip)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

You can only modify adjacencies when the adjacency is detached. Before modifying an adjacency, you can detach the adjacency first with the **no attach** command. The adjacency stays in the going down state when a call is active or when the ping enable feature is running. During this state, existing calls are not torn down and new calls are not accepted. The adjacency does not go to detached state until all calls have ended. An adjacency cannot be attached until the adjacency is in detached state.

If you wish to override the option to wait till active calls on the adjacency end, the adjacency can be detached immediately using the following commands:

- **no attach force abort**—Executes a forced detach, tearing down calls without signaling their end.
- **no attach force normal**—Executes a forced detach, tearing down calls gracefully.

To check the state of the adjacency, you can use the **show sbc sbe adjacencies** command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples**

The following example shows how to attach the H.323 adjacency to h323ToIsp42:

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42  
Router(config-sbc-sbe-adj-h323)# attach
```

# audit (H.248 BAC)

To force the Border Access Controller (BAC) to send an audit to an H.248 terminal device, ignoring the audit initiated by the H.248 terminal device, use the **audit force** command in the H248 BAC adjacency configuration mode. To auto audit (default), which means the BAC will not send an audit to an H.248 terminal device if the audit initiated by the H.248 terminal device is received within the audit interval, use the **no** form of this command.

To change the audit interval in the BAC, use the **audit interval** command in the H248 BAC adjacency configuration mode. To return to the default value, use the **no** form of this command.

**audit force**

**audit interval** *idle time*

**no audit** {*force* | *interval idle time*}

Syntax Description	force	interval	idle time
	Forces the H.248 BAC to send an audit to the terminal devices. Default is auto audit.	Specifies the audit interval.	Audit time interval, in seconds. The range is from 0 to 3600. The default value is 60.

**Command Default** The default is the **no** form of the command.

**Command Modes** H248 BAC adjacency configuration (config-h248-bac-adj)

Command History	Release	Modification
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command can be configured only in the access adjacency submode and not in the core adjacency submode.

**Examples** The following example shows how the **audit force** command forces the BAC to send an audit to the H.248 terminal devices:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# audit force
```

The following example shows how the **audit interval** command is used to change the audit interval in the BAC:

```
Router# configure terminal  
Router(config)# sbc h248 bac  
Router(config-h248-bac)# adjacency h248 access iad_80_123  
Router(config-h248-bac-adj)# audit interval 300
```

# authentication mode (session border controller)

To configure the authentication mode for a SIP adjacency, use the **authentication mode** command in the adjacency SIP configuration mode. To deconfigure the authentication mode, use the **no** form of this command.

**authentication mode {local | remote}**

**no authentication mode {local | remote}**

## Syntax Description

<b>local</b>	Configures the SIP adjacency for local authentication.
<b>remote</b>	Configures the SIP adjacency for remote authentication.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **authentication mode** command is used to configure the SIP adjacency for local authentication:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# authentication mode local
```

## Related Commands

Command	Description
<b>authentication nonce timeout</b>	Configures the authentication nonce timeout for a SIP adjacency.

# authentication (session border controller)

To configure the H.323 adjacency authentication, use the **authentication** command in the adjacency H.323 configuration mode. To deconfigure the H.323 adjacency authentication mode, use the **no** form of this command.

**authentication** *auth-type*

**no authentication**

<b>Syntax Description</b>	<b>auth-type</b> The authentication type; currently this can only be <b>endpoint</b> .
---------------------------	--

<b>Command Default</b>	Default is the <b>no</b> form of the command.
------------------------	---

<b>Command Modes</b>	Adjacency H.323 configuration (config-sbc-sbe-adj-h323)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	<p>This command causes the SBC to authenticate itself with a Gatekeeper. The gatekeeper is responsible for performing the endpoint authentication.</p> <p>To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.</p>
-------------------------	--

<b>Examples</b>	The following command sets H.323 adjacency "h323ToIsp42" to use endpoint authentication.
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# isp42 adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# authentication endpoint
Router(config-sbc-sbe-adj-h323)# exit
```

# bandwidth-fields mandatory

To set the bandwidth description of Session Description Protocol (SDP) as mandatory, use the **bandwidth-fields mandatory** command in Virtual Data Border Element (VDBE) configuration mode. To set the bandwidth description as optional, use the **no** form of this command.

**bandwidth-fields mandatory**

**no bandwidth-fields**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The default behaviour is that the bandwidth description of SDP is optional.

**Command Modes** VDBE configuration (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in a user group that is associated with a task group that includes the proper task IDs. To use this command, you must be in the correct configuration mode and submenu. The Examples section that follows shows the hierarchy of the modes and submodes required to run the command.

**Examples** The following example shows how to set the bandwidth description of the SDP as mandatory in the VDBE configuration mode:

```
Router# configure terminal
Router# sbc sbc dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# bandwidth-fields mandatory
```

Related Commands	Command	Description
	<b>vdbe</b>	Enters VDBE configuration mode.



# bandwidth (session border controller)

To configure the maximum and minimum bandwidth limits for media calls, use the **bandwidth** command in codec definition mode. To return the bandwidth to the default value, use the no form of this command.

**bandwidth** *bandwidth-value* [ **min** *bandwidth-value* ]

**no bandwidth** *bandwidth-value* [ **min** *bandwidth-value* ]

Syntax Description		
<i>bandwidth</i>		Specifies the maximum bandwidth in bits per second (bps) for media calls. Decimal points are allowed.
<b>min</b> <i>bandwidth-value</i>		(Optional) Specifies the minimum bandwidth in bits per second (bps) for media calls. Decimal points are allowed.

**Command Default** The default minimum bandwidth is 128 kbps.

**Command Modes** Codec definition mode (config-sbc-sbe-codec-def)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

This command configures the bandwidth for the analog-to-digital codec (enCOder/DECOder) hardware. The codec name must be one of the system codecs that SBC can recognize. To see a list of the system codecs, use the **show sbc sbc sbe codecs** command.

The minimum bandwidth setting is for use with the **media police degrade** command. It specifies the minimum acceptable bandwidth for the video codec. If the available bandwidth is smaller than the configured **min bandwidth-value**, the call is rejected under the degrade policy. The minimum bandwidth setting applies only to the unidirectional bandwidth of the media stream, and does not include the packet overhead.

The **bandwidth min** command specifies the unidirectional, minimum bandwidth limit bandwidth and does not include packet overhead.

**Examples** The following example shows how to configure the maximum bandwidth limit to 400,000 bps for media calls:

```
Router# configure terminal
Router(config)# sbc mySBC
```

```

Router(config-sbc)# sbc
Router(config-sbc-sbc)# codec system H263 id 34
Router(config-sbc-sbc-codec-def)# bandwidth 400000

```

The following example shows how to configure the minimum bandwidth limit to 328,000 bps, specifically for video type media calls:

```

Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbc
Router (config-sbc-sbc)# codec custom h263-c id 96
Router (config-sbc-sbc-codec-def)# type variable
Router (config-sbc-sbc-codec-def)# media video
Router (config-sbc-sbc-codec-def)# bandwidth min 328000

```

#### Related Commands

Command	Description
<b>bandwidth</b>	Configures the maximum and minimum bandwidth limits for media calls.
<b>caller-bandwidth-field</b>	Configures SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the caller.
<b>callee-bandwidth-field</b>	Configures the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the callee
<b>max-bandwidth-per-scope</b>	Configures the maximum limit for the bandwidth in bps, Kbps, Mbps or Gbps for an entry in an admission control table.

# batch-size

To configure the batching or grouping of RADIUS messages sent to a RADIUS server, use the **batch** command in the packetcable-em configuration mode. To disable the batch, use the **no** form of this command.

**batch-size** *number*

**no batch-size**

## Syntax Description

*number* Specifies the batch size in bytes. The range is 0 through 4096.

## Command Default

0

## Command Modes

Packet-cable em configuration (config-sbc-sbe-billing-packetcable-em)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

A value of 0 indicates no batching. A platform may choose to set a non-zero default value (this may increase performance.)

## Examples

The following example shows how to configure the maximum size of a batch of CDRs:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
(config-sbc-sbe-billing)# packetcable-em 4 transport radius test
(config-sbc-sbe-billing-packetcable-em)# batch-size 256
```

## Related Commands

Command	Description
<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
<b>attach</b>	activate the billing for a RADIUS client
<b>batch-size</b>	Configures the batching or grouping of RADIUS messages sent to a RADIUS server.
<b>batch-time</b>	Configures the maximum number of milliseconds for which any record is held in the batch before the batch is sent
<b>deact-mode</b>	Configures the deactivate mode for the billing method.

<b>Command</b>	<b>Description</b>
ldr-check	Configures the time of day (local time) to run the Long Duration Check (LDR).
<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
<b>local-address ipv4 (packet-cable)</b>	Configures the local address of the packet-cable billing instance.
method packetcable-em	Enables the packet-cable billing method.
packetcable-em <i>transport radius</i>	Configures a packet-cable billing instance.
show sbc sbe billing remote	Displays the local and billing configurations.

# batch-time

To configure the maximum number of milliseconds for which any record is held before the batch is sent, use the **batch-time** command in the packetcable-em configuration mode. To disable the waiting period, use the **no** form of this command.

**batch-time** *number*

**no batch-time**

<b>Syntax Description</b>	<i>number</i> Specifies the batch time in milliseconds. The range is 1 through 3600000.
---------------------------	---

<b>Command Default</b>	1000 milliseconds
------------------------	-------------------

<b>Command Modes</b>	Packet-cable em configuration (config-sbc-sbe-billing-packetcable-em)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the maximum number of milliseconds for which any record is held before the batch is sent:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
(config-sbc-sbe-billing)# packetcable-em 4 transport radius test
(config-sbc-sbe-billing-packetcable-em)# batch-size 256
(config-sbc-sbe-billing-packetcable-em)# batch-time 22
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>activate (radius)</b>
	attach	activate the billing for a RADIUS client
	batch-size	Configures the batching or grouping of RADIUS messages sent to a RADIUS server.
	batch-time	Configures the maximum number of milliseconds for which any record is held in the batch before the batch is sent
	deact-mode	Configures the deactivate mode for the billing method.

<b>Command</b>	<b>Description</b>
ldr-check	Configures the time of day (local time) to run the Long Duration Check (LDR).
<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
<b>local-address ipv4 (packet-cable)</b>	Configures the local address of the packet-cable billing instance.
method packetcable-em	Enables the packet-cable billing method.
packetcable-em <i>transport radius</i>	Configures a packet-cable billing instance.
<b>show sbc sbe billing remote</b>	Displays the local and billing configurations.

# bgp additional-paths select

To have the system calculate a second BGP bestpath, use the **bgp additional-paths select** command in address family configuration mode. To remove this mechanism for calculating a second bestpath, use the **no** form of the command.

**bgp additional-paths select { best-external [backup] | backup }**

**no bgp additional-paths select**

Syntax Description	best-external	(Optional) Calculates a second bestpath from among those received from external neighbors. Configure this keyword on a PE or RR. This keyword enables the BGP Best External feature on an RR.
	backup	(Optional) Calculates a second bestpath as a backup path.

**Command Default** This command is disabled by default.

**Command Modes** Address family configuration (config-router-af)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines** The BGP Diverse Path feature can be enabled on a route reflector to calculate a bestpath and an additional path per address family.

Computation of a diverse path per address family is triggered by any of the following commands:

- **bgp additional-paths install**
- **bgp additional-paths select**
- **maximum-paths ebgp**
- **maximum-paths ibgp**

The **bgp additional-paths install** command will install the type of path that is specified in the **bgp additional-paths select** command. Either the **best-external** keyword or the **backup** keyword is required; both keywords can be specified. If both keywords (**best-external** and **backup**) are specified, the system will install a backup path.

**Examples** In the following example, the system computes a second best path from among those received from external neighbors:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
```

```

neighbor 10.1.1.1 activate
maximum-paths ibgp 4
bgp bestpath igp-metric ignore
bgp additional-paths select best-external
bgp additional-paths install
neighbor 10.1.1.1 advertise diverse-path backup

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>bgp additional-paths install</b>	Enables BGP to calculate a backup path for a given address and to install it into the RIB and CEF.
<b>bgp bestpath igp-metric ignore</b>	Specifies that the system ignore the IGP metric during best path selection.
<b>maximum-paths ebgp</b>	Configures multipath load sharing for eBGP and iBGP routes.
<b>maximum-paths ibgp</b>	Controls the maximum number of parallel iBGP routes that can be installed in a routing table.



# bgp bestpath igp-metric ignore

To have the system ignore the Interior Gateway Protocol (IGP) metric during BGP best path selection, use the **bgp bestpath igp-metric ignore** command in address family configuration mode. To remove the instruction to ignore the IGP metric, use the **no** form of this command.

**bgp bestpath igp-metric ignore**

**no bgp bestpath igp-metric ignore**

**Syntax Description** This command has no arguments or keywords.

**Command Default** This command is disabled by default.

**Command Modes** Address family configuration (config-router-af)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines** The IGP metric is a configurable metric for EIGRP, IS-IS, or OSPF that is related to distance. The **bgp bestpath igp-metric ignore** command can be used independently, or in conjunction with the BGP Diverse Path feature. This command does not enable the BGP Diverse Path feature.

Similarly, enabling the BGP Diverse Path feature does not necessarily require that the IGP metric be ignored. If you enable the BGP Diverse Path feature and the RR and its shadow RR are not co-located, this command must be configured on the RR, shadow RR, and PE routers.

This command is supported in the following address families:

- ipv4 unicast
- vpnv4 unicast
- ipv6 unicast
- vpnv6 unicast
- ipv4+label
- ipv6+label



**Note** This command is not supported per VRF; if you use it per VRF, it is at your own risk.

This command applies per VRF as follows (which is consistent with the BGP PIC/Best External feature):

- When configured under address-family vpnv4 or vpnv6, it applies to all VRFs, but it will be nvgened only under vpnv4/vpnv6 global.

- When configured under a particular VRF, it applies only to that VRF and will be nvgened only for that VRF.
- When configured under vpv4 or vpv6 global, this command can be disabled for a particular VRF by specifying **no bgp bestpath igp-metric ignore**. The **no** form will be nvgened under that VRF, while under vpv4 or vpv6 **bgp bestpath igp-metric ignore** is nvgened and the command applies to all other VRFs.

**Examples**

In the following example, the IGP metric is ignored during calculation of the BGP best path:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select backup
 bgp additional-paths install
 neighbor 10.1.1.1 advertise diverse-path backup
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>bgp additional-paths select</b>	Specifies that the system compute a second BGP bestpath.

# bgp consistency-checker

To enable the BGP Consistency Checker feature, use the **bgp consistency-checker** command in router configuration mode. To disable the BGP Consistency Checker feature, use the **no** form of this command.

```
bgp consistency-checker {error-message | auto-repair} [interval minutes]
```

```
no bgp consistency-checker
```

Syntax Description	Parameter	Description
	<b>error-message</b>	Specifies that when an inconsistency is found, the system will only generate a syslog message.
	<b>auto-repair</b>	Specifies that when an inconsistency is found, the system will generate a syslog message and take action based on the type of inconsistency found.
	<b>interval</b> <i>minutes</i>	(Optional) Specifies the interval at which the BGP consistency checker process occurs. <ul style="list-style-type: none"> <li>The range is 5 to 1440 minutes. The default is 1440 minutes (one day).</li> </ul>

**Command Default** No BGP consistency check is performed.

**Command Modes** Router configuration (config-router)

Command History	Release	Modification
	15.1(2)S	This command was introduced.
	Cisco IOS XE 3.3S	This command was integrated into Cisco IOS XE 3.3S.

**Usage Guidelines** A BGP route inconsistency with a peer occurs when an update or a withdraw is not sent to a peer, and black-hole routing can result. The BGP consistency checker feature is a low-priority process created to address this issue. This feature performs nexthop-label, RIB-out, and aggregation consistency checks. When BGP consistency checker is enabled, it is performed for all address families. Once the process identifies such an inconsistency:

- If the **error-message** keyword is specified, the system will report the inconsistency with a syslog message, and will also perform forceful aggregation reevaluation in the case of an aggregation inconsistency.
- If the **auto-repair** keyword is specified, the system will report the inconsistency with a syslog message and also take appropriate action, such as a route refresh request or an aggregation reevaluation, depending on the type of inconsistency.

**Examples** In the following example, BGP consistency checker is enabled. If a BGP route inconsistency is found, the system will send a syslog message and take appropriate action.

```
Router(config)# router bgp 65000
Router(config-router)# bgp consistency-checker auto-repair
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip bgp vpnv4 all inconsistency next-hop-label</b>	Displays routes that have next-hop-label inconsistency found by BGP consistency checker.

# bgp refresh max-eor-time

To cause the router to generate a Route-Refresh End-of-RIB (EOR) message if it was not able to generate one due to route flapping, use the **bgp refresh max-eor-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

**bgp refresh max-eor-time** *seconds*

**no bgp refresh max-eor-time**

<b>Syntax Description</b>	<i>seconds</i>	<p>Number of seconds after which, if the router was unable to generate a Route-Refresh EOR message due to route flapping, the router generates a Route-Refresh EOR message.</p> <ul style="list-style-type: none"> <li>Valid values are from 600 to 3600, or 0.</li> <li>The default is 0, meaning the command is disabled.</li> </ul>
---------------------------	----------------	--

<b>Command Default</b>	0 seconds
------------------------	-----------

<b>Command Modes</b>	Router configuration (config-router)
----------------------	--------------------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 3.4S</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 3.4S	This command was introduced.
Release	Modification				
Cisco IOS XE Release 3.4S	This command was introduced.				

<b>Usage Guidelines</b>	<p>The BGP Enhanced Route Refresh feature is enabled by default. The <b>bgp refresh max-eor-time</b> command is not needed under normal circumstances. You might configure the <b>bgp refresh max-eor-time</b> command in the event of continuous route flapping, when the router is unable to generate a Route-Refresh EOR message, in which case a Route-Refresh EOR is generated after the timer expires.</p>
-------------------------	--

<b>Examples</b>	<p>In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.</p>
-----------------	--

```
router bgp 65000
  bgp refresh stalepath-time 800
  bgp refresh max-eor-time 800
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>bgp refresh stalepath-time</b></td> <td>Causes the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message.</td> </tr> </tbody> </table>	Command	Description	<b>bgp refresh stalepath-time</b>	Causes the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message.
Command	Description				
<b>bgp refresh stalepath-time</b>	Causes the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message.				

# bgp refresh stalepath-time

To cause the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message, use the **bgp refresh stalepath-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

**bgp refresh stalepath-time** *seconds*

**no bgp refresh stalepath-time**

<b>Syntax Description</b>	<i>seconds</i>	<p>Number of seconds the router waits to receive a Route-Refresh End-of-RIB (EOR) message, and then removes the stale paths from BGP table if the router hasn't received an EOR message.</p> <ul style="list-style-type: none"> <li>• Valid values are 600 to 3600, or 0.</li> <li>• The default is 0, meaning the command is disabled.</li> </ul>
---------------------------	----------------	--

**Command Default** 0 seconds

**Command Modes** Router configuration (config-router)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines** The BGP Enhanced Route Refresh feature is enabled by default. The **bgp refresh stalepath-time** command is not needed under normal circumstances. You might configure the **bgp refresh stalepath-time** command in the event of continuous route flapping, when the router does not receive a Route-Refresh EOR after an Adj-RIB-Out, in which case the router removes the stale routes from the BGP table after the timer expires. The stale path timer is started when the router receives a Route-Refresh SOR.

**Examples** In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.

```
router bgp 65000
  bgp refresh stalepath-time 800
  bgp refresh max-eor-time 800
```

**Related Commands**

Command	Description
<b>bgp refresh max-eor-time</b>	Causes the router to generate a Route-Refresh EOR message if it was not able to generate one due to route churn.

# billing

To configure billing, use the **billing** command in SBE configuration mode. Use the **no** form of this command to remove all the billing configuration.

**billing**

**no billing**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

There is only one billing per SBC.

**Examples** The following example shows how to enter the billing mode for mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)#
```

Related Commands	Command	Description
	<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
	<b>ldr-check</b>	Configures the time of day (local time) to run the Long Duration Check (LDR).
	<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
	<b>method packetcable-em</b>	Enables the packet-cable billing method.



<b>Command</b>	<b>Description</b>
packetcable-em <i>transport radius</i>	Configures a packet-cable billing instance.
show sbc sbe billing remote	Displays the local and billing configurations.

# billing (CAC)

To configure billing, use the **billing** command in the CAC table entry configuration mode. To unconfigure the billing configuration, use the **no** form of this command.

**billing** {filter {disable | enable} | methods {packetcable-em | xml}}

**no billing** {filter | methods {packetcable-em | xml}}

## Syntax Description

<b>filter</b>	Specifies whether the billing filter scheme is enabled or disabled.
<b>disable</b>	Disables the billing filter.
<b>enable</b>	Enables the billing filter.
<b>methods</b>	Specifies the billing methods that are allowed for calls relating to different adjacencies.
<b>packetcable-em</b>	Configures the PacketCable billing method for billing.
<b>xml</b>	Configures the XML billing method for billing.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

There is only one billing per SBC.

## Examples

The following example shows how to enter the billing mode for mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# billing filter enable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# billing methods xml
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	cac-policy-set	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
	<b>cac-table</b>	Configures admission control tables.
	<b>table-type</b>	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

# blacklist

To enter the mode for configuring the event limits of a given source, use the **blacklist** command in the SBE configuration mode. To return the event limits to the default values, use the **no** form of this command.

**[no] blacklist [critical] global** [address-default | {**ipv4** {*addr*} | **ipv6** {*addr*}}] [**tcp** {*tcp-port*} | **udp** {*udp-port*} | default-port-limit] ]

**[no] blacklist [critical] vpn** {*vpn-name*} [**address-default** [**address-family** {**ipv4** | **ipv6**}] | **address-family** {**ipv4** | **ipv6**} | **ipv4** *addr* [**tcp** {*tcp-port*} | **udp** {*udp-port*} | **default-port-limit**] | **ipv6** *addr* [**tcp** {*tcp-port*} | **udp** {*udp-port*} | **default-port-limit**] ]

## Syntax Description

<b>global</b>	(Required) Allows blacklisting limits or critical blacklisting limits to be configured for the global VPN. Sets limits for total traffic from global VPN.  This keyword is required when the command is used on the global VPN. Either global or vpn name must be specified for the blacklist.
<b>critical</b>	Configures critical blacklisting limits for the global VPN or a specific VPN.
<b>vpn {<i>vpn_name</i>}</b>	(Required) Enters the mode for configuring the event limits or critical event limits for the given VPN. Sets limits for total traffic from the named VPN.  <i>vpn_name</i> is the VPN name. Either global or vpn name must be specified for the blacklist.
<b>address-default</b>	(Optional) Enters the mode for configuring the default event limits for the source addresses in the given VPN. Sets default traffic limits to apply to each IP address within the global VPN, except where overridden by the <b>ipv4</b> or <b>ipv6</b> command option.
<b>address-family</b>	(Optional) Enters the mode for configuring the default event limits for the IPv4 or IPv6 address family in the given VPN.
<b>ipv4 <i>addr</i></b>	(Optional) Enters the mode for configuring the default event limits for the IPv4 address in the given VPN. Sets traffic limits for total traffic from this IP address within the global VPN.  <i>addr</i> is the IPv4 address.
<b>ipv6 <i>addr</i></b>	(Optional) Enters the mode for configuring the default event limits for the IPv6 address in the given VPN. Sets traffic limits for total traffic from this IP address within the global VPN.  <i>addr</i> is the IPv6 address.
<b>tcp <i>tcp-port</i></b>	(Optional) Sets traffic limit for traffic from this IP address and TCP port within the global VPN.
<b>udp <i>udp-port</i></b>	(Optional) Sets traffic limit for traffic from this IP address and UDP port within the global VPN.
<b>default-port-limit</b>	(Optional) Sets traffic limits to apply to each port within the IP address in the global VPN, except where overridden by either the <b>tcp</b> or <b>udp</b> command option.

## Command Default

No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.4.2	The <b>critical</b> keyword and options were added.
	Cisco IOS XE Release 2.6	The <b>ipv6</b> keyword was added.
	Cisco IOS XE Release 3.1S	The <b>ipv6</b> keyword was added under <b>address-family</b> . The <b>ipv6 addr</b> and options were also added.

**Usage Guidelines** For IPv4, either “global” or “vpn\_name” must be specified for the blacklist. However, if a vpn\_name is entered, a VPN token is required.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **vpn** keyword and the VPN token of 800 are used to enter the mode for configuring the event limits for the VPN test:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist vpn 800
Router(config-sbc-sbe-blacklist)#
```

The following example shows how to enter the mode for configuring the default event limits for all addresses:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global address-default
```

The following example shows how to enter the mode for configuring blacklisting to apply to all addresses:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist)#
```

The following example shows how to enter the mode for applying blacklisting options to a single IPv4 IP address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global ipv4 1.1.1.1
Router(config-sbc-sbe-blacklist)#
```

The following example shows how to enter the mode for applying blacklisting options to a single IPv6 IP address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global ipv6 2001::10:0:0:1
Router(config-sbc-sbe-blacklist)#
```

The following example shows how to enter the mode for applying blacklisting options to an IPv6 address family in a VPN:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist vpn Mgmt-intf address-family ipv6
Router(config-sbc-sbe-blacklist)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
address-default	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
clear sbc sbe blacklist	Clears the blacklist for the specified SBC service.
global	Enters the mode for configuring blacklisting to apply to all addresses.
ipv4 (blacklist)	Enters the mode for applying blacklisting options to a single IPv4 IP address.
ipv6 (blacklist)	Enters the mode for applying blacklisting options to a single IPv6 IP address.
vpn	Enter the mode for configuring the event limits for a given VPN.
<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source.
show sbc sbe blacklist configured-limits	Lists the explicitly configured limits, showing only the sources configured.
<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.
tcp	Enters the mode for configuring blacklisting for TCP protocol only.
<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
<b>trigger-period</b>	Defines the period over which events are considered.
default-port-limit	Enters a mode for configuring the default even limits for the ports of a given address.
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
udp	Enters the mode for configuring blacklisting for UDP protocol only.
<b>vpn</b>	Enters the mode for configuring the event limits for a given VPN.

# blacklist (profile)

To set a profile to be blacklisted, use the **blacklist** command in the appropriate profile configuration mode. To remove blacklist from this profile, use the **no** form of this command.

**blacklist**

**no blacklist**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes**

- SIP Method Profile configuration (config-sbc-sbe-mep-mth)
- SIP Option Profile configuration (config-sbc-sbe-mep-opt)
- SIP Header Profile configuration (config-sbc-sbe-mep-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to blacklist an option profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-profile option1
Router(config-sbc-sbe-mep-opt)# blacklist
```

The following example shows how to blacklist a method profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile Method1
Router(config-sbc-sbe-mep-mth)# blacklist
```

The following example shows how to blacklist a header profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile header1
Router(config-sbc-sbe-mep-hdr)# blacklist
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip header-profile</b>	Configures a header profile.
<b>sip method-profile</b>	Configures a method profile.
<b>sip option-profile</b>	Configures an option profile.



## blacklist (sip-opt)

To set profile to be blacklisted, use the **blacklist** command in SIP option mode. Use the **no** form of this command to remove blacklist from this profile.

**blacklist**

**no blacklist**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The global default is used.

**Command Modes** SIP option (sip-opt)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command:

**Examples** The following example shows how to add an option to the profile.

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-profile optpr1
Router(config-sbc-sbe-sip-opt)# blacklist
```

# blended-codec-list

To add a blended codec list, use the **blended-codec-list** command in SBC SBE CAC policy CAC table entry configuration mode. To remove a blended codec list, use the **no** form of this command.

**blended-codec-list** *blended-codec-list*

**no blended-codec-list** *blended-codec-list*

<b>Syntax Description</b>	<i>blended-codec-list</i>	Case-sensitive, unique name for a blended codec list. The maximum length is 63 characters.
---------------------------	---------------------------	--

<b>Defaults</b>	No blended codec list exists.
-----------------	-------------------------------

<b>Command Modes</b>	SBC SBE CAC policy CAC table entry configuration mode (config-sbc-sbe-cacpolicy-cactable-entry)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.11S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to configure a blended codec list:

```
Router> enable
Router# configure terminal
Router(config)# sbc 123
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table test
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table test
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# blended-codec-list codec-a
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>blended-transcode</b>	Enables the Blended Transcoding feature.

# blended-transcode

To enable the Blended Transcoding feature, use the **blended-transcode** command in the SBC SBE CAC policy CAC table entry configuration mode. To disable the Blended Transcode feature, use the **no** form of this command.

**blended-transcode**

**no blended-transcode**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The Blended Transcode feature is disabled.

**Command Modes** SBC SBE CAC policy CAC table entry configuration mode (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.11S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to enable the Blended Transcode feature:

```
Router> enable
Router# configure terminal
Router(config)# sbc 123
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table test
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table test
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# blended-transcode
```

Related Commands	Command	Description
	<b>blended-codec-list</b>	Configures a blended codec list.

# body-editor

To associate a body editor to a SIP adjacency to cause the body editor to act on the incoming and outgoing SIP messages, use the **body-editor** command in the Adjacency SIP configuration mode. To remove a body editor, use the **no** form of this command.

**body-editor** [*inbound* | *outbound*] {*editor-name*}

**no body-editor** [*inbound* | *outbound*] {*editor-name*}

## Syntax Description

inbound	Associates a body editor to act on the inbound messages on a SIP adjacency. <b>Note</b> When the message is passed, the body editor should be applied in the inbound and outbound directions on the respective adjacencies on which the message is routed.
outbound	Associates a body editor to act on the outbound messages on a SIP adjacency. <b>Note</b> When the message is passed, the body editor should be applied in the inbound and outbound directions on the respective adjacencies on which the message is routed.
<i>editor-name</i>	Text string that describes a body editor name. The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to associate two body editors, inbound editor2 and outbound editor1, at a SIP adjacency level for the adj-1 adjacency:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
```

```
Router(config-sbc-sbe)# adjacency sip adj-1
Router(config-sbc-sbe-adj-sip)# body-editor inbound editor2
Router(config-sbc-sbe-adj-sip)# body-editor outbound editor1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
action	Sets the action to be taken on a body type in a SIP body editor for a non-SDP message body.
sip body-editor	Configures a body editor.

## body-editor (method)

To add a body editor to act on a method, use the **body-editor** command in the signaling border element (SBE) SIP method element configuration mode. To remove a body editor, use the **no** form of this command.

**body-editor** *editor-name*

**no body-editor**

### Syntax Description

<i>editor-name</i>	Specifies the name of the body editor.  The following guidelines apply:  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
--------------------	--

### Command Default

No default behavior or values are available.

### Command Modes

SBE SIP method element configuration (config-sbc-sbe-mep-mth-ele)

### Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

### Examples

The following example shows how the **body-editor** command adds a body editor to act on a method:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# sip method-editor MethodEditor1
Router(config-sbc-sbe-mep-mth)# method Method2
Router(config-sbc-sbe-mep-mth-ele)# body-editor bodyEditor1
```

### Related Commands

Command	Description
sip body-editor	Configures a body editor.
sip method-editor	Configures a method editor.



# body-profile

To associate a body profile to a method profile to cause the body profile to act on incoming and outgoing SIP messages, use the **body-profile** command in SBE method profile element configuration mode. To remove the body profile, use the **no body-profile** command.

**body-profile** {*profile\_name*}

**no body-profile** {*profile\_name*}

## Syntax Description

<i>profile_name</i>	Text string that describes a body profile name. The following guidelines apply: The <i>profile_name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE method profile element configuration mode (config-sbc-sbe-sip-mth-ele)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

After creating a body profile with the **sip body-profile** {*profile\_name*} command, you can associate the body profile at the following additional levels and configuration modes:

- At the SIP signaling entity level (ingress or egress), under SBE mode, using the **sip default body-profile** [[**inbound/outbound**] {*profile\_name*}] command. The body profile is associated for the entire signaling instance (that is all messages, either ingress or egress, passing through the SBC).
- SIP adjacency level, under SIP adjacency mode, using the **body-profile** [[**inbound/outbound**] {*profile\_name*}] command. The body profile is associated to an adjacency.

SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

## Examples

The following example describes how to associate body profile, bodyprofile1, to a method profile:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
```



```

Router(config-sbc-sbe)# sip method-profile profile1
Router(config-sbc-sbe-sip-mth)# description mysbc profile1
Router(config-sbc-sbe-sip-mth)# method test
Router(config-sbc-sbe-sip-mth-ele)# body-profile bodyprofile1
Router(config-sbc-sbe-sip-mth-ele)#

```

Related Commands	Command	Description
	sip default body-profile	Associates a body profile at the SIP signaling level under the SBE mode.
	body-profile (sip adj)	Associates a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
	sip body-profile	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
	body	Names the body type or content header type for a non-SDP message body that is part of the body profile.
	action	Sets the action to be taken on a body type in a SIP body profile for a non-SDP message body
	sip method-profile	Configures a method profile in the mode of an SBE entity

## body-profile (sip adj)

To associate a body profile to a SIP adjacency to cause the body profile to act on incoming and outgoing SIP messages, use the **body-profile (sip adj)** command in adjacency SIP configuration mode. To remove the body profile, use the **no body-profile (sip adj)** command.

**body-profile** [*inbound* | *outbound*] {*profile\_name*}

**no body-profile** [*inbound* | *outbound*] {*profile\_name*}

### Syntax Description

<i>inbound</i>	Associates the body profile to act on inbound messages on the SIP adjacency.  <b>Note</b> When the message is ‘passed,’ the body profile should be applied both in the inbound and outbound direction on the respective adjacencies on which the message is routed.
<i>outbound</i>	Associates the body profile to act on outbound messages on the SIP adjacency.  <b>Note</b> When the message is ‘passed,’ the body profile should be applied both in the inbound and outbound direction on the respective adjacencies on which the message is routed.
<i>profile_name</i>	The <i>profile_name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

### Command Default

No default behavior or values are available.

### Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

### Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

After creating a body profile with the **sip body-profile** {*profile\_name*} command, you can associate the body profile at the following additional levels and configuration modes:

- At the SIP signaling entity level (ingress or egress), under SBE mode, using the **sip default body-profile** [[*inbound*|*outbound*] {*profile\_name*}] command. The body profile is associated for the entire signaling instance (that is all messages, either ingress or egress, passing through the SBC).
- At SIP method profile level, under method profile mode, using the **body-profile** {*profile\_name*} command. The body profile is associated to a method profile.

SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

### Examples

The following example describes how to associate two body profiles, inbound profile2 and outbound profile1, at the SIP adjacency level for adjacency adj-1:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj-1
Router((config-sbc-sbe-adj-sip))# body-profile inbound profile2
Router((config-sbc-sbe-adj-sip))# body-profile outbound profile1
```

### Related Commands

Command	Description
sip default body-profile	Associates a body profile at the SIP signaling level under the SBE mode.
body-profile	Associates a body profile to a method profile under the method profile mode.
sip body-profile	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
body	Names the body type or content header type for a non-SDP message body that is part of the body profile.
action	Sets the action to be taken on a body type in a SIP body profile for a non-SDP message body

# body

To name the body type or content header type for a non-SDP message body that is part of the body profile, use the **body** command in SBE SIP Body configuration mode. To remove the body type or content header type, use the **no body** command.

**body** {*WORD*}

**no body** {*WORD*}

## Syntax Description

WORD	Specifies the body type or content header type. This is a string of maximum 64 characters.  The body name must be in the form of <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive. For more information, see Usage Guidelines.
------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE SIP Body configuration (config-sbc-sbe-sip-body)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command describes the body type or content header type for SBC to act on messages with the specified body type or content header type.

The **body** command is used in conjunction with the **sip body-profile** command that is used to create the body profile.

The body name must be in the form of <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive.

Asterisk (\*) is used to match *all* non-SDP body types. Note that \* is also interpreted as a string by the CLI, and is just a token used to indicate wild-card match.

The following Content-Type descriptions are not allowed: application/sdp and multipart/mixed

Only one body element with such a wildcard can co-exist with other bodies per body profile. The wildcard body is applied if there is no other matching body in that profile. The body name is matched using regular 'string compare.' Note that there is no provision to match body names using any regular expression matching techniques.

**Examples**

The following example does the following: creates a body profile named `bodyprofile1`; describes the body type, that is to act on messages with Content-Type header “application/ISUP”; and instructs SBC to strip that particular message body and pass the rest of the message:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-profile bodyprofile1
Router(config-sbc-sbe-sip-body)# body application/ISUP
Router(config-sbc-sbe-sip-body-ele)# action strip
Router(config-sbc-sbe-sip-body-ele)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<code>sip default body-profile</code>	Associates a body profile at the SIP signaling level under the SBE mode.
<code>body-profile</code>	Associates a body profile to a method profile under the method profile mode.
<code>body-profile (sip adj)</code>	Associates a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
<code>sip body-profile</code>	Creates a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
<code>action</code>	Sets the action to be taken on a body type in a SIP body profile for a non-SDP message body.

# body (editor)

To name a body type or content header type for a non-SDP message body that is a part of the body editor, use the **body** command in the signaling border element (SBE) session initiation protocol (SIP) body configuration mode. To remove a body type or content header type, use the **no** form of this command.

**body** *word*

**no body** *word*

## Syntax Description

<i>word</i>	The <i>word</i> field can have a maximum of 64 characters which can include the underscore character (_) and alphanumeric characters.
	<b>Note</b> Except for the underscore character, do not use any special character to specify field names.
	The body name must be in the form <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive.

## Command Default

No default behavior or values are available.

## Command Modes

SIP Body Editor configuration (config-sbc-sbe-mep-bdy)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command describes the body type or content header type for the SBC to act on messages of the specified body type or content header type.

The **body** command is used in conjunction with the **sip body-editor** command that is used to create the body editor.

The body name must be in the form <media-type>/<media-sub-type>, for example, application/ISUP. The body name field is case-insensitive.

Asterisk (\*) is used to match *all* the non-SDP body types. Note that \* is also interpreted as a string by the CLI, and is a token used to indicate wildcard match.

---

**Examples**

The following example shows how to create a body editor named bodyeditor1 and describe the body type as application/ISUP:

```
Router(config)# sbc mySBC  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# sip body-editor bodyeditor1  
Router(config-sbc-sbe-mep-bdy)# body application/ISUP
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip body-editor</b>	Creates a body editor to filter the non-SDP message bodies from the incoming and outgoing SIP messages.

---

## branch bandwidth-field

To configure the SBC such that it converts a specific bandwidth line format into another bandwidth line format in the outbound Session Description Protocol (SDP) sent to a caller or a callee, use the **branch bandwidth-field** command in the CAC table entry configuration mode. To unconfigure the conversion of the bandwidth line format, use the **no** form of this command.

**branch bandwidth-field** {as-to-tias | tias-to-as}

**no branch bandwidth-field** {as-to-tias | tias-to-as}

### Syntax Description

<b>as-to-tias</b>	Configures the SBC to convert the b=AS line format into the b=TIAS line format for a specific SDP media descriptor in an outbound offer. Here, AS refers to Application Specific maximum. Similarly, TIAS refers to Transport Independent Application Specific maximum.
<b>tias-to-as</b>	Configures the SBC to convert the b=TIAS line format into the b=AS line format for a given SDP media descriptor in an outbound offer.

### Command Default

The default is that the format of bandwidth lines is not converted.

### Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

### Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

The SBC applies the outgoing bandwidth line format that you configure. If the offerer-side adjacency is configured to apply a specific style of bandwidth line format in the SDP, this command causes the SBC to convert the answer to the specified format before it is sent back to the offerer. If there are multiple bandwidth lines, only the first line is converted into the specified bandwidth line and the remaining lines are ignored.



#### Note

As mentioned earlier, the default is that the bandwidth line is not converted from one format to another. However, if the callee is configured to convert the bandwidth, and the message is converted, the response that is sent back to the caller is converted back even if this command is not configured for the caller.



**Examples**

The following example shows how to configure the SBC such that it converts an AS bandwidth line format into a TIAS bandwidth line format in the outbound SDP sent to a caller or a callee:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch bandwidth-field as-to-tias
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee-bandwidth-field</b>	Configures the SBC such that it converts a specific bandwidth line format into another bandwidth line format in an outbound SDP sent to a callee.
<b>caller-bandwidth-field</b>	Configures the SBC such that it converts a specific bandwidth line format into another bandwidth line format in an outbound SDP sent to a caller.

# branch codec

To configure the codec options for a caller or a callee, use the **branch codec** command in the CAC table entry configuration mode. To unconfigure the codec options, use the **no** form of this command.

**branch codec** {**convert** | **profile** *profile-name*}

**no caller codec** {**convert** | **profile**}

## Syntax Description

<b>convert</b>	Enables the codec variant conversion.
<b>profile</b> <i>profile-name</i>	Specifies the codec variant profile name.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character ( <code>_</code> ) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

## Command Default

By default, codec variant conversion is disabled, and no codec variant profile is specified.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the codec options for a caller using the **branch codec** command:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch codec convert
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch codec profile profile-1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee codec</b>	Configures the codec options for a callee.
<b>caller codec</b>	Configures the codec options for a caller.

# branch codec-list

To specify the codecs that the caller or the callee of a call can use, use the **branch codec-list** command in the CAC table entry configuration mode. To delete a codec list, use the **no** form of this command.

**branch codec-list** *list-name*

**no branch codec-list** *list-name*

## Syntax Description

<i>list-name</i>	Name of the codec list.  The <i>list-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to enter a mode to create the test codec list:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch codec-list test
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee-codec-list</b>	Specifies the codecs that the callee of a call can use.
<b>caller-codec-list</b>	Specifies the codecs that the caller of a call can use.

# branch hold-setting

To specify the caller hold settings or the callee hold settings, use the **branch hold-setting** command in the CAC table entry configuration mode. To remove the caller hold settings or the callee hold settings, use the **no** form of this command.

**branch hold-setting** { **hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard** }

**no branch hold-setting** { **hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard** }

## Syntax Description

<b>hold-c0</b>	Branch supports and requires c=0.0.0.0.
<b>hold-c0-inactive</b>	Branch supports and requires c=0.0.0.0 and a=inactive.
<b>hold-c0-sendonly</b>	Branch supports and requires c=0.0.0.0 and a=sendonly.
<b>hold-sendonly</b>	Branch supports and requires a=sendonly.
<b>standard</b>	Branch supports and requires c=0.0.0.0 and an a= line.

## Command Default

The default setting is **standard**.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to use the **branch hold-setting** command:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value fairchild
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch hold-setting hold-sendonly
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee-hold-setting</b>	Specifies the callee hold settings.
<b>caller-hold-setting</b>	Specifies the caller hold settings.

# branch inband-dtmf-mode

To configure the dual-tone multifrequency (DTMF) in-band mode for the caller side or the callee side, use the **branch inband-dtmf-mode** command in the CAC table entry configuration mode. To unconfigure the DTMF in-band mode, use the **no** form of this command.

**branch inband-dtmf-mode {always | inherit | maybe | never }**

**no branch inband-dtmf-mode**

## Syntax Description

<b>always</b>	Specifies that the in-band DTMF tones are always used by the endpoint.
<b>inherit</b>	Specifies that the in-band DTMF mode for the endpoint is not affected by the CAC entry.
<b>maybe</b>	Specifies that the in-band DTMF tones are used by the endpoint unless signaling indicates that an alternative format is in use for the DTMF.
<b>never</b>	Specifies that the endpoint never uses the in-band DTMF mode.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the DTMF in-band mode for the caller side using the **caller inband-dtmf-mode** command in the CAC table entry configuration mode so that the endpoint never uses the inband DTMF mode:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table InbandDTMF
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch inband-dtmf-mode never
```



Related Commands	Command	Description
	callee inband-dtmf-mode	Configures the DTMF in-band mode for the callee side.
	caller inband-dtmf-mode	Configures the DTMF in-band mode for the caller side.

# branch inbound-policy

To configure a caller inbound SDP policy table or a callee inbound SDP policy table, use the **branch inbound-policy** command in the CAC table entry configuration mode. To unconfigure an inbound SDP policy table, use the **no** form of this command.

**branch inbound-policy** *sdp-policy-table-name*

**no branch inbound-policy** *sdp-policy-table-name*

## Syntax Description

*sdp-policy-table-name*

Name of the SDP policy table.

The *sdp-policy-table-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

**Note** Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

### Release

### Modification

Cisco IOS XE Release 3.5S

This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to use the **branch inbound-policy** command to configure an inbound SDP policy table:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch inbound-policy test
```

## Related Commands

<b>Command</b>	<b>Description</b>
<b>callee-outbound-policy</b>	Configures a callee outbound SDP policy table.
<b>caller-outbound-policy</b>	Configures a caller outbound SDP policy table.

# branch media bypass

To enable or disable the Multiple SBC Media Bypass feature on the caller side or the callee side, use the **branch media bypass** command in the CAC table entry configuration mode. To unconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

**branch media bypass {enable | disable}**

**no branch media bypass**

## Syntax Description

<b>enable</b>	Enables the Multiple SBC Media Bypass feature on the caller side or the callee side.
<b>disable</b>	Disables the Multiple SBC Media Bypass feature on the caller side or the callee side.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to use the **branch media bypass** command to enable the Multiple SBC Media Bypass feature:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media bypass enable
```

## Related Commands

Command	Description
<b>codec</b>	Adds a codec to a codec list.
<b>codec-list</b>	Creates a codec list.

<b>Command</b>	<b>Description</b>
<b>codec-list description</b>	Provides a description of a codec list.
<b>show sbc sbe codec-list</b>	Displays information about codec lists.

# branch media-caps

To configure a codec list used to announce media capabilities on behalf of a SIP caller or SIP callee in a SIP-to-H.323 or H.323-to-SIP interworking call, use the **branch media-caps** command in the CAC table entry configuration mode. To unconfigure the codec list, use the **no** form of this command.

**branch media-caps** *media-caps-list-name*

**no branch media-caps** *media-caps-list-name*

## Syntax Description

<i>media-caps-list-name</i>	Name of media capabilities list.  The <i>media-caps-list-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command configures a codec list and assigns the list to a CAC table. After a codec list is assigned, it must not be deleted before it is removed from the CAC table. A codec list must exist before it can be assigned to an entry in a CAC table.

## Examples

The following example shows how to configure the caller-media-caps-list codec list and assign the list to the cac-tbl-1 CAC table in entry 1:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list caller-media-caps-list
Router(config-sbc-sbe-codec-list)# codec t38
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table cac-tbl-1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-caps media-caps-list
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee-media-caps</b>	Configures a codec list that is used to announce media capabilities on behalf of a SIP callee in a SIP-to-H.323 or H.323-to-SIP interworking call.
<b>caller-media-caps</b>	Configures a codec list that is used to announce media capabilities on behalf of a SIP caller in a SIP-to-H.323 or H.323-to-SIP interworking call.

## branch media-description disabled

To configure how the SBC handles disabled media descriptions for a caller or a callee, use the **branch media-description disabled** command in the CAC table entry configuration mode. To unconfigure how the SBC handles disabled media descriptions for a caller or a callee, use the **no** form of this command.

```
branch media-description disabled {strip {answer | offer {all | new}} | {pad offer}}
```

```
no branch media-description disabled {strip {answer | offer {all | new}} | {pad offer}}
```

### Syntax Description

<b>strip</b>	Strips the disabled media description lines.
<b>pad</b>	Pads with dummy disabled media description lines.
<b>answer</b>	Strips the disabled media description lines from answers.
<b>offer</b>	Strips the disabled media description lines from offers when this keyword is used with the <b>strip</b> keyword. Pads offers with dummy disabled media description lines when used with <b>pad</b> .
<b>all</b>	Strips all the disabled media descriptions from offers.
<b>new</b>	Strips new disabled media descriptions from offers.

### Command Default

By default, the **pad** setting is configured.

### Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

### Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to configure the removal of disabled media streams from new forwarded offers:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-description disabled strip offer new
```

The following example shows how to configure the removal of disabled media streams from forwarded offers, regardless of whether it is known to the recipient of the offer:



```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-description disabled strip offer all

```

The following example shows how to configure the removal of disabled media streams from forwarded answers:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-description disabled strip answer

```

The following example shows how to configure the SBC so that it does not pad forwarded offers with disabled media streams:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# no branch media-description disabled pad offer

```

#### Related Commands

Command	Description
<b>callee media-description disabled</b>	Configures how the SBC handles disabled media descriptions for a callee.
<b>caller media-description disabled</b>	Configures how the SBC handles disabled media descriptions for a caller.

## branch media-type

To configure the media address type settings for a caller or a callee, use the **branch media-type** command in the CAC table entry configuration mode. To unconfigure the media address type settings for a caller, use the **no** form of this command.

**branch media-type {ipv4 | ipv6 | inherit | both}**

**no branch media-type {ipv4 | ipv6 | inherit | both}**

### Syntax Description

<b>ipv4</b>	Specifies that only IPv4 media addresses are supported.
<b>ipv6</b>	Specifies that only IPv6 media addresses are supported.
<b>inherit</b>	Specifies that the supported media IP address type from earlier CAC policy entries must be inherited. This is the default setting.
<b>both</b>	Specifies that both IPv4 and IPv6 media addresses are supported.

### Command Default

The default is that the supported media IP address type from earlier CAC policy entries must be inherited.

### Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

### Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to use the **branch media-type** command to specify that only IPv4 media addresses are supported:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch media-type ipv4
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee media-type</b>	Configures the media address type settings for a callee.
<b>caller media-type</b>	Configures the media address type settings for a caller.

# branch outbound-policy

To configure an outbound Session Description Protocol (SDP) policy table for a caller or a callee, use the **branch outbound-policy** command in the CAC table entry configuration mode. To unconfigure an outbound SDP policy table, use the **no** form of this command.

**branch outbound-policy** *table-name*

**no branch outbound-policy** *table-name*

## Syntax Description

<i>table-name</i>	Name of the SDP policy table.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure an outbound SDP policy table for a caller:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch outbound-policy test
```

## Related Commands

<b>Command</b>	<b>Description</b>
<b>callee-inbound-policy</b>	Configures a callee inbound SDP policy table.
<b>caller-inbound-policy</b>	Configures a caller inbound SDP policy table.

# branch port-range-tag

To configure the port range tag for a caller or a callee that is used when selecting a media address and port, use the **branch port-range-tag** command in the CAC table entry configuration mode. To unconfigure the port range tag, use the **no** form of this command.

**branch port-range-tag** { *adjacency-name* | **none** | **string** *tag-string* }

**no branch port-range-tag**

## Syntax Description

<i>adjacency-name</i>	Source adjacency name that is used as a port range tag.
<b>none</b>	Prompts the SBC to not use a port range tag for calls matching the CAC entry, and removes any previously found strings.
<b>string</b> <i>tag-string</i>	Specifies the explicit port range tag string.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to use the **branch port-range-tag** command to configure a port range tag:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch port-range-tag adj1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee port-range-tag</b>	Configures the port range tag for a callee.
<b>caller port-range-tag</b>	Configures the port range tag for a caller.

# branch privacy edit-privacy-request

To edit and update privacy indications provided by a user, use the **branch privacy edit-privacy-request** command in the CAC table configuration mode. To remove the indications, use the **no** form of this command.

```
branch privacy edit-privacy-request {pass | strip | insert | replace | sip {strip {all | critical | header | id | none | session | token word | user} | insert {critical | header | id | none | session | token word | user}}}
```

```
no branch privacy edit-privacy-request {pass | strip | insert | replace | sip {strip {all | critical | header | id | none | session | token word | user} | insert {critical | header | id | none | session | token word | user}}}
```

## Syntax Description

<b>insert</b>	Inserts privacy restrictions, depending on the type of message: <ul style="list-style-type: none"> <li>• SIP message—Inserts Privacy:header;session;user;id;critical if the header is not already present.</li> <li>• H323 message—Changes the presentation indicator from Allowed to Restricted.</li> </ul>
<b>pass</b>	Passes on the privacy header or presentation indicators.
<b>replace</b>	Replaces privacy restrictions, depending on the type of message: <ul style="list-style-type: none"> <li>• SIP message—Replaces Privacy:header;session;user;id;critical except when none has been requested.</li> <li>• H323 message—Sets the presentation indicator to Restricted.</li> </ul>
<b>strip</b>	Removes all the privacy restrictions, depending on the type of message: <ul style="list-style-type: none"> <li>• SIP message—Removes the Privacy header.</li> <li>• H323 message—Sets the presentation indicator to Allowed.</li> </ul>
<b>sip</b>	Specifies the following SIP settings. These settings allow greater control and override all generic actions: <ul style="list-style-type: none"> <li>• <b>insert</b>—Inserts privacy tokens into the Privacy header.</li> <li>• <b>strip</b>—Removes privacy tokens from the Privacy header.</li> </ul>
<b>critical</b>	Specifies the call must be discontinued if privacy cannot be achieved in the Privacy header.
<b>header</b>	Obscures all the header information that is related to the user, from the Privacy header.
<b>id</b>	Adds or removes the ID headers from the Privacy header.
<b>none</b>	Specifies that privacy must not be applied to the call.
<b>session</b>	Specifies the media privacy for the session in the Privacy header. No media bypass is performed.
<b>token</b>	Specifies the nonstandard user-defined privacy token in the Privacy header.
<i>word</i>	User-defined privacy token.
<b>user</b>	Removes all nonessential header information that is related to the user, from the Privacy header.



**Command Default** The default setting is **pass**.

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure an entry to remove all the privacy restrictions from the SIP and H323 adjacencies in the MyCacTable admission control table:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch-privacy edit-privacy-request strip
```

Related Commands	Command	Description
	<b>callee-privacy edit-privacy-request</b>	Edits and updates privacy indications provided by a user, from the callee side.
	<b>caller-privacy edit-privacy-request</b>	Edits and updates privacy indications provided by a user, from the caller side.

# branch privacy privacy-service

To apply privacy settings according to RFC3323, RFC3325, and the H.323 presentation restriction settings in the admission control table, use the **branch privacy privacy-service** command in the CAC table configuration mode. To unconfigure the privacy settings, use the **no** form of this command.

```
branch privacy privacy-service {adj-trust-boundary | always | never}
```

```
no branch privacy privacy-service
```

## Syntax Description

<b>adj-trust-boundary</b>	Specifies the adjacency privacy trust level to determine whether the privacy service is required.
<b>always</b>	Specifies that the privacy service must be provided indefinitely if requested by the user.
<b>never</b>	Specifies that the privacy service must not be provided even if requested by the user.

## Command Default

The default privacy setting value is **adj-trust-boundary**.

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure an entry to provide privacy service indefinitely in the MyCacTable admission control table:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch privacy privacy-service always
```

## Related Commands

<b>Command</b>	<b>Description</b>
<b>callee privacy privacy-service</b>	Applies privacy settings according to RFC3323, RFC3325, and H.323 presentation restriction settings, on the callee side.
<b>caller privacy privacy-service</b>	Applies privacy settings according to RFC3323, RFC3325, and H.323 presentation restriction settings, on the caller side.

# branch ptime

To configure the packetization time on the caller side or the callee side, use the **branch ptime** command in the CAC table configuration mode. To unconfigure the packetization time setting, use the **no** form of this command.

**branch ptime** *packetization-time*

**no branch ptime** *packetization-time*

## Syntax Description

<i>packetization-time</i>	Packetization time, in milliseconds. The range is from 0 to 100. The default is 0.
---------------------------	--

## Command Default

The default packetization time is 0 milliseconds. This value indicates that transrating must not be performed.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the packetization time to 30 milliseconds by using the **branch ptime** command:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch ptime 30
```

## Related Commands

Command	Description
<b>callee ptime</b>	Configures the packetization time on the callee side.
<b>caller ptime</b>	Configures the packetization time on the caller side.



# branch secure-media

To apply the granular-level Secure Media feature on the caller side or the callee side, use the **branch secure-media** command in the CAC table entry configuration mode. To remove the granular-level Secure Media feature, use the **no** form of this command.

**branch secure-media**

**no branch secure-media**

## Syntax Description

This command has no arguments or keywords.

## Command Default

By default, the granular-level (Unsigned) Secure Media feature is disabled.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

We recommend that you use the granular-level Secure Media feature instead of enabling Secure Media globally. The granular-level feature enables you to specify the calls and adjacencies at the location where you want to use secure media.

## Examples

The following example shows an Unsigned Secure Media configuration where the two SIP adjacencies for both legs of the call are configured for security trusted-unencrypted, and both the caller and the callee sides are configured for secure media in a CAC table entry:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# adjacency sip server
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table testSecure
Router(config-sbc-sbe-cacpolicy)# cac-table testSecure
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch secure-media
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```

```
Router(config-sbc-sbe-cacpolicy)# exit  
Router(config-sbc-sbe)# cac-policy-set global 1  
Router(config-sbc-sbe)# end
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee secure-media</b>	Configures the granular-level Secure Media feature on the callee side.
<b>caller secure-media</b>	Configures the granular-level Secure Media feature on the caller side.

# branch sig-qos-profile

To configure the Quality of Service (QoS) profile to be used for signaling packets sent to the original caller or callee, use the **branch sig-qos-profile** command in the CAC table entry configuration mode. To unconfigure the QoS profile, use the **no** form of this command.

**caller-sig-qos-profile** *profile-name*

**no caller-sig-qos-profile** *profile-name*

## Syntax Description

<i>profile-name</i>	Name of the QoS profile. The <i>default</i> string is reserved.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character ( <code>_</code> ) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command can be run only at the per-call scope. The CAC policy will not be activated if this command is configured in any other scope.

Packet marking will not be applied until the CAC decision process is run. This means that some initial signaling packets sent to the caller, for example, the SIP 100 provisional response, will not receive any particular Differentiated Services Codepoint (DSCP) marking.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command shows how to configure calls from the acme account to use the voice QoS profile enterprise for signaling packets sent from the SBC to the original caller or callee:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-account
```



```

Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch-sig-qos-profile enterprise

```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee-sig-qos-profile</b>	Configures the QoS profile to be used for the signaling packets sent to the original callee.
<b>caller-sig-qos-profile</b>	Configures the QoS profile to be used for the signaling packets sent to the original caller.

# branch tel-event payload type

To configure the payload type to be used for the caller or the callee in H.323-SIP interworking calls, use the **branch tel-event payload-type** command in the CAC entry configuration mode. To unconfigure the payload type setting, use the **no** form of this command.

**branch tel-event payload type** *payload-type*

**no branch tel-event payload type**

## Syntax Description

*payload-type* See RFC 2833 for detailed information about the values of *payload-type*. The range is from 96 to 127. The default is 101.

## Command Default

No default behavior or values are available.

## Command Modes

CAC entry configuration (config-sbc-cac-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The **branch tel-event payload type** command enables support for dual tone multifrequency (DTMF) H.323-SIP interworking. The telephone-event payload type configured by this command is used by the SBC only in situations where the payload type information is not provided by the other side in an H.323-SIP interworking call.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to use the **branch tel-event payload-type** command to set the payload type to 101:

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-cac-pol)# cac-table CAC-POLICY-TBL1
Router(config-sbc-cac-entry)# branch tel-event payload-type 101
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee tel-event payload-type</b>	Configures the payload type to be used for the callee in H.323-SIP interworking calls.
<b>caller tel-event payload-type</b>	Configures the payload type to be used for the caller in H.323-SIP interworking calls.

# branch video-qos-profile

To configure the QoS profile to be used for the media packets sent to the original caller or original callee, use the **branch video-qos-profile** command in the CAC table configuration mode. To remove this configuration, use the **no** form of this command.

**branch video-qos-profile** *profile-name*

**no branch video-qos-profile** *profile-name*

## Syntax Description

<i>profile-name</i>	Name of the QoS profile.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  Except for the underscore character, do not use any special character to specify field names.
---------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command. The **branch video-qos-profile** command can be executed only in the per-call scope. The CAC policy is not activated if this command is configured in any other scope.

## Examples

The following example shows how to configure calls from the acme account to use the video QoS profile enterprise for the packets sent from the SBC to the original caller:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch video-qos-profile enterprise
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee-video-qos-profile</b>	Configures the QoS profile to be used for the media packets sent to the original callee.
<b>caller-video-qos-profile</b>	Configures the QoS profile to be used for the packets sent to the original caller.

# branch voice-qos-profile

To configure the QoS profile to be used for the media packets sent to the original caller or the original callee, use the **branch voice-qos-profile** command in the CAC table configuration mode. To unconfigure the QoS profile, use the **no** form of this command.

**branch voice-qos-profile** *profile-name*

**no branch voice-qos-profile**

## Syntax Description

*profile-name* Name of the QoS profile.

The *profile-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command. This command can be run only in the per-call scope. The CAC policy is not activated if this command is configured in any other scope.

## Examples

The following example shows how to configure the calls from the acme account to use the voice QoS profile enterprise for the packets sent from the SBC:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# branch voice-qos-profile enterprise
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>calle-voice-qos-profile</b>	Configures the QoS profile to be used for the media packets sent to the original callee.
<b>caller-voice-qos-profile</b>	Configures the QoS profile to be used for the media packets sent to the original caller.

# cac-policy-set

To create a new call admission control (CAC) policy set, copy an existing complete policy set, swap the references of a complete policy set to another policy set, or set the averaging period for rate calculations in a CAC policy set, use the **cac-policy-set** command in the Signaling border element (SBE) configuration mode. To remove a policy set or deconfigure the averaging period, use the **no** form of this command.

```
cac-policy-set {policy-set-id | copy {source policy-set-id destination policy-set-id} | swap {source
policy-set-id destination policy-set-id} | averaging-period {avg-number avg-period}
```

```
no cac-policy-set {policy-set-id | averaging-period {avg-number}}
```

## Syntax Description

<i>policy-set-id</i>	An integer chosen by a user to identify the policy set. The range is from 1 to 2147483647.
<b>copy</b>	Copies an existing policy set.
<b>swap</b>	Swaps the existing references of a complete policy set to another policy set.
<b>source</b>	Specifies the existing complete call policy set.
<b>destination</b>	Specifies the destination of the call policy set.
<b>averaging-period</b>	Specifies the averaging period for rate calculations.
<i>avg-number</i>	The averaging period number. It can be 1 or 2.
<i>avg-period</i>	The averaging period used by the CAC in rate calculations, in seconds. It can range from 1 to 3600 seconds. By default, 60 seconds is configured.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The copy-and-swap function was added to this command. The averaging period could also be configured for a CAC policy set.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Changes are not permitted to the configuration of a global policy set. Also, a policy set cannot be removed if it is a global policy set.



## Examples

The following command creates a policy set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# exit
```

The following example shows how to copy an existing complete CAC policy set and swap its references to the new policy set:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set copy source 12 destination 22
Router(config-sbc-sbe)# cac-policy-set 22
Router(config-sbc-sbe-cacpolicy)# no complete
Router(config-sbc-sbe-cacpolicy)# cac-table TAB1
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# $max-call-rate-per-scope 100
Router(config-sbc-sbe)# cac-policy-set 22
Router(config-sbc-sbe-cacpolicy)# complete
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# cac-policy-set swap source 12 destination 22

Router(config-sbc-sbe-cacpolicy)# cac-policy-set global 22
Router(config-sbc-sbe)# end
```

The following example shows how to set the averaging period for rate calculations in a CAC policy set:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 100
Router(config-sbc-sbe)# cac-policy-set averaging-period 2 175
```

## Related Commands

Command	Description
cac-policy-set global	Activates the global CAC policy set within an SBE entity.
show sbc sbe	Lists detailed information pertaining to a CAC policy table.
cac-policy-set	

## cac-policy-set (admin-domain)

To configure the call admission control (CAC) policy set for an administrative domain, use the **cac-policy-set** command in the **Administrative domain** configuration mode. To **remove a policy set from the administrative domain**, use the **no** form of this command.

```
cac-policy-set policy-set-id
```

```
no cac-policy-set
```

### Syntax Description

<i>policy-set-id</i>	The integer, ranging from 1 to 2147483647, that identifies a complete policy set.
----------------------	---

### Command Default

By default, no CAC policy set is configured.

### Command Modes

Administrative domain configuration (config-sbc-sbe-ad)

### Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

A user can specify only one CAC policy set for an administrative domain.

### Examples

The following example shows how to configure the CAC policy set for the administrative domain ADMIN1 using the **call-policy-set** command in **an administrative domain** configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# admin-domain ADMIN1
Router(config-sbc-sbe-ad)# cac-policy-set 2
```

### Related Commands

Command	Description
admin-domain	Configures an administrative domain.
call-policy-set (admin-domain)	Configures the inbound and outbound number analysis and routing policy set for an administrative domain.
show sbc sbe admin-domain	Lists the administrative domains on the Session Border Controller (SBC) and per adjacency.



# cac-policy-set global

To activate the global call admission control (CAC) policy set within an signaling border element (SBE) entity, use the **cac-policy-set global** command in the SBE configuration mode.

**cac-policy-set global** *policy-set-id*

<b>Syntax Description</b>	<i>policy-set-id</i> Integer identifying the policy set that should be made global. Range is from 1 to 2147483647.
---------------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The <b>cac-policy-set global</b> command was renamed as <b>cac-policy-set global</b> .

**Usage Guidelines** The active CAC policy set cannot be modified.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to activate policy set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# cac-policy-set global 1
```

<b>Command</b>	<b>Description</b>
cac-policy-set	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
show sbc sbe cac-policy-set	Lists detailed information pertaining to a CAC policy table.

# cac-table

To create or configure an admission control table, use the **cac-table** command in CAC-policy-set configuration mode. To **delete the admission control table**, use the **no** form of this command.

**cac-table** *table-name*

**no cac-table** *table-name*

<b>Syntax Description</b>	<i>table-name</i>	Specifies the admission control table.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------------	-------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** CAC-policy-set configuration (config-sbc-sbe-cacpolicy)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to create the admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)#
```

Related Commands	Command	Description
	<b>first-cac-table</b>	Configures the name of the first policy table to process when performing the admission control stage of policy.
	<b>first-cac-scope</b>	Configure the scope at which to begin defining limits when performing the admission control stage of policy.

# cache-lifetime

To configure the lifetime of any DNS entry, use the **cache-lifetime** command in the DNS configuration mode. To disable the lifetime, use the **no** form of this command.

**cache-lifetime** *0-1879048*

**no cache-lifetime**

<b>Syntax Description</b>	<i>0-1879048</i> Specifies the lifetime of any DNS entry in seconds.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	DNS configuration (config-sbc-sbe-dns)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the lifetime of any DNS entry,:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip dns
Router(config-sbe-dns)# cache-lifetime 444
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		cache-limit
	sip dns	Enter the SIP DNS configuration mode.

# cache-limit

To configure the maximum number of entries that are permitted in the DNS cache, use the **cache-limit** command in the DNS configuration mode. To set the limit to 100, use the **no** form of this command.

```
cache-limit 0-4294967295
```

```
no cache-lifetime
```

<b>Syntax Description</b>	<i>0-4294967295</i> Specifies the maximum number of DNS entries.
---------------------------	--

<b>Command Default</b>	100
------------------------	-----

<b>Command Modes</b>	DNS configuration (config-sbc-sbe-dns)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure limits on DNS entries:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip dns
Router(config-sbe-dns)# cache-limit 14
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	cache-lifetime	Configures the lifetime of any DNS entry.
sip dns	Enters the SIP DNS configuration mode.	

# cache (session border controller)

To enable caching and configure call detail record caching parameters on a local disk, use the **cache** command in the SBE Billing configuration mode. To disable caching and local cache parameters, use the **no** form of this command.

```
cache [path {WORD}] | alarm [critical VAL] [major VAL] [minor VAL] | max-size {0-4194303}
```

```
no cache [path {WORD}] | alarm [critical VAL] [major VAL] [minor VAL] | max-size {0-4194303}
```

Syntax Description		
<b>path</b>	(Required to enable caching)	Specifies the local CDR cache file path location.
<b>WORD</b>	(Required to enable caching)	Specifies the local drive name, up to a maximum of 255 characters.
<b>alarm</b>	(Optional)	Specifies the cache file alarm thresholds.
<b>critical VAL</b>	(Optional)	Specifies a critical alarm threshold.
<b>major VAL</b>	(Optional)	Specifies a major alarm threshold.
<b>minor VAL</b>	(Optional)	Specifies a minor alarm threshold.
<b>max-size</b>	(Optional)	Specifies the maximum size of the local call detail record (CDR) cache file in kilobytes.
<b>0-4194303</b>	(Optional)	This is the maximum size of the local CDR cache file, from zero to 4194303 kilobytes.  The default is zero. The <b>cache max-size 0</b> command results in no limit on how big the cache can be.

**Command Default** The default size of the local CDR cache file is zero.

**Command Modes** SBE Billing configuration (config-sbc-sbe-billing)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** The Cisco ASR 1000 Series Routers have a local disk where records and event messages can be stored on a local cache. Local cache support is a significant advantage because call detail records and event messages (EMs) are not lost when a billing server is unavailable.

Use the **cache** command configures parameters for storing call detail records and EMs on local disk as part of Cisco Unified Border Element (SP Edition)'s integrated billing system in the unified model.

The **cache path** command enables caching and the **no cache path** command disables caching. You can use the other optional keywords to specify alarm thresholds and how large the cache size is in kilobytes.



**Examples**

The following example configures billing and enables caching of call detailed records and EMs on the designated hard disk:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address aaa ipv4 10.1.1.1
Router(config-sbc-sbe)# radius accounting ACCT-CLIENT-GROUP-1
Router(config-sbc-sbe-acc)# activate
Router(config-sbc-sbe-acc)# server ACCT-SERVER-1
Router(config-sbc-sbe-acc-ser)# address ipv4 20.1.1.1
Router(config-sbc-sbe-acc-ser)# key cisco
Router(config-sbc-sbe-acc)# activate
Router(config-sbc-sbe-acc)# exit
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# ldr-check 22 30
Router(config-sbc-sbe-billing)# local-address ipv4 10.20.1.1
Router(config-sbc-sbe-billing)# method packetcable-em
Router(config-sbc-sbe-billing)# cache path harddisk:
Router(config-sbc-sbe-billing)# packetcable-em 3 transport radius test
Router(config-sbc-sbe-billing-packetcable-em)# batch-size 256
Router(config-sbc-sbe-billing-packetcable-em)# batch-time 22
Router(config-sbc-sbe-billing-packetcable-em)# local-address ipv4 10.1.1.1
Router(config-sbc-sbe-billing-packetcable-em)# attach
Router(config-sbc-sbe-billing-packetcable-em)# exit
Router(config-sbc-sbe-billing)# activate
```

The following configuration example shows that the cache file alarm thresholds and maximum size of the local CDR cache file are configured:

```
cache path disk2:
cache alarm minor 100 major 200 critical 300
cache max-size 1234567
```

The following configuration example shows that caching is enabled on the hard disk:

```
sbc asr
sbe
! - Local radius IP address
control address aaa ipv4 10.1.1.1

! - First radius accounting client group
radius accounting ACCT-CLIENT-GROUP-1
! - First radius server
server ACCT-SERVER-1
address ipv4 20.1.1.1
key cisco
activate

! - Billing manager.
billing
local-address ipv4 10.1.1.1
method packetcable-em
cache path harddisk:
! - First billing method.
packetcable-em 0 transport radius ACCT-CLIENT-GROUP-1
local-address ipv4 10.1.1.1
attach
activate
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
	<b>billing</b>	Configures billing.
	<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
	<b>packetcable-em</b> <i>method-index</i> <b>transport</b> <b>radius</b> <i>RADIUS-client-name</i>	Configures a packet-cable billing instance.
	<b>method</b> <b>packetcable-em</b>	Enables the packet-cable billing method.
	<b>show sbc sbe billing</b> <b>remote</b>	Displays the local and billing configurations.

# cac-policy-set global

To activate the global call admission control (CAC) policy set within an signaling border element (SBE) entity, use the **cac-policy-set global** command in the SBE configuration mode. To deactivate the global CAC policy, use the **no** form of the command.

**cac-policy-set global** *policy-set-id*

**no cac-policy-set global**

<b>Syntax Description</b>	<i>policy-set-id</i> Integer identifying the policy set that should be made global. Range is from 1 to 2147483647.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It replaces the <b>cac-policy-set global</b> command.

<b>Usage Guidelines</b>	<p>From Release 3.5S onward, an active CAC policy set can be modified.</p> <p>To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.</p>
-------------------------	--

<b>Examples</b>	The following example shows how to activate policy set 1 on mySbc:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# cac-policy-set global 1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cac-policy-set</b>	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
	<b>show sbc sbe cac-policy-set</b>	Lists detailed information pertaining to a CAC policy table.

## cac-scope

To allow you to choose the scope in which CAC limits are to be applied within each entry in a policy set table, use the **cac-scope** command in the CAC table entry configuration mode. To unconfigure the scope, use the **no** form of this command.

**cac-scope** *{list of scope options}*

**no cac-scope** *{list of scope options}*

### Syntax Description

*list of scope options* The scope options are as follows:

- **account**—Events that are from the same account.
- **adjacency**—Events that are from the same adjacency.
- **adj-group**—Events that are from members of the same adjacency group.
- **call**—Scope limits are per single call.
- **category**—Events under the same category.
- **dst-account**—Events that are sent to the same account.
- **dst-adj-group**—Events that are sent to the same adjacency group.
- **dst-adjacency**—Events that are sent to the same adjacency.
- **dst-number**—Events that have the same destination.
- **global**—Scope limits are global.
- **src-account**—Events that are from the same account.
- **src-adj-group**—Events that are from the same adjacency group.
- **src-adjacency**—Events that are from the same adjacency.
- **src-number**—Events that have the same source number.
- **sub-category**—Limits specified at this scope are applicable to all the events sent to or received from members of the same subscriber category.
- **sub-category-pfx prefix-len**—Limits specified in this scope are applicable to all the events sent to or received from members having the same subscriber category prefix.



**Note** *prefix-len* is included as part of the **cac-scope** command, for example, the command is as follows:  
**cac-scope sub-category-pfx prefix-len**

- **subscriber**—The limits specified in this scope apply to all the events sent to or received from individual subscribers (a device that is registered with a Registrar server).

### Command Default

The default setting is **global**.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	The <b>sub-category</b> , <b>sub-category-pfx</b> , and <b>subscriber</b> scope options were added.
	Cisco IOS XE Release 3.5S	The <b>account</b> and <b>adjacency</b> scope options were added.

**Usage Guidelines** The **cac-scope** command allows you to choose a scope in which CAC limits are to be applied within each entry. This command is available only to the entries defined within a Policy Set table type. You can define more than one **cac-scope** command within an entry.

Use the **table-type** command to configure a Policy Set table type.

Some CAC scopes can be combined to create compound scopes. The **global** scope and **call** scope cannot be combined.

When policy-set is defined as the table type for a CAC table, you must define cac-scope and cac-scope-prefix-len within the entry, for example:

```
cac-scope sub-category-pfx prefix-len
```

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the call event at which limits are applied in the TAB1 CAC policy-set table:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table TAB1
Router(config-sbc-sbe-cacpolicy)# cac-table TAB1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-num-calls 20
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# complete
```

Related Commands	Command	Description
	<b>cac-table</b>	Configures a Call Admission Control (CAC) table.
	<b>table-type</b>	Configures a CAC table type that enables the priority of the call to be used as a criterion in the CAC policy.

# calc-moscqe

To specify the percentage of calls that must be used to calculate the MOS-CQE score, use the **calc-moscqe** command in the adjacency H.323 configuration mode or adjacency SIP configuration mode. To remove this configuration, use the **no** form of this command.

**calc-moscqe** *call-percentage*

**no calc-moscqe**

## Syntax Description

<i>call-percentage</i>	Percentage of calls. The range is from 0 to 1000. For example, if you enter 205 as the value of <i>call-percentage</i> , the SBC uses 20.5 percent of the calls for measuring local jitter.
------------------------	---

## Command Default

By default, the value of *call-percentage* is 0.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **calc-moscqe** command is used to specify that 20.5 percent of the calls must be used to calculate the MOS-CQE score:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 adj1
Router(config-sbc-sbe-adj-h323)# calc-moscqe 205
```

## Related Commands

Command	Description
current15minutes	Specifies that QoS statistics must be calculated for 15-minute intervals.
current5minutes	Specifies that QoS statistics must be calculated for 5-minute intervals.
currentday	Specifies that statistics must be calculated for 24-hour intervals.
currenthour	Specifies that QoS statistics must be calculated for 60-minute intervals.

<b>Command</b>	<b>Description</b>
currentindefinite	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
g107 bpl	Sets a value for the Packet-Loss Robustness (Bpl) factor.
g107 ie	Sets a value for the Equipment Impairment (Ie) factor.
g107a-factor	Sets a value for the Advantage (A) factor.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
show sbc sbe adjacencies	Displays details of the adjacencies configured on the SBE.
show sbc sbe call-stats	Displays the statistics pertaining to all the calls on a the SBE.
snmp-server enable traps sbc	Enables SBC notification types.
statistics	Specifies the QoS statistic for which alert levels must be set.

# call-policy-set

To create a new policy set, copy an existing complete policy set, or swap the references of a complete policy set to another policy set, use the **call-policy-set** command in the Signaling border element (SBE) configuration mode. To **delete a policy set**, use the **no** form of this command.

```
call-policy-set {policy-set-id | copy {source policy-set-id destination policy-set-id} | swap {source
policy-set-id destination policy-set-id}}
```

```
no call-policy-set policy-set-id
```

## Syntax Description

<i>policy-set-id</i>	The integer, ranging from 1 to 2147483647, for a call policy set.
<b>copy</b>	Copies an existing policy set.
<b>swap</b>	Swaps the existing references of a complete policy set to another policy set.
<b>source</b>	Specifies the existing complete call policy set.
<b>destination</b>	Specifies the destination of the call policy set.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The copy-and-swap function was added to this command.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to create policy set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)#
```

The following example shows how to copy an existing complete policy set and swap its references to a new policy set:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```



```

Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set copy source 2 destination 20
Router(config-sbc-sbe)# call-policy-set 20
Router(config-sbc-sbe-rtgpolicy)# no complete
Router(config-sbc-sbe-rtgpolicy)# first-inbound-na-table InTable
Router(config-sbc-sbe-rtgpolicy)# first-outbound-na-table OutTable
Router(config-sbc-sbe-rtgpolicy)# complete
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)# call-policy-set swap source 2 destination 20

```

**Related Commands**

<b>Command</b>	<b>Description</b>
call-policy-set	Creates a new policy set on the session border controller (SBC).
call-policy set default	Configures a default policy set on the SBE entity.
first-call-routing-table	Configures the name of the first policy table to be processed when performing the routing stage of a policy for new call events.
first-inbound-na-table	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
first-outbound-na-table	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
show sbc sbe call-policy-set	Lists the details of the policy sets configured on the SBC.
show sbc sbe call-policy-set default	Lists the summary of the default policy set configured on the SBC.

## call-policy-set (admin-domain)

To configure the inbound and outbound number analysis and routing policy set for an administrative domain, use the **call-policy-set** command in the **Administrative domain** configuration mode. To **remove a policy set from an administrative domain**, use the **no** form of this command.

```
call-policy-set { inbound-na policy-set-id | outbound-na policy-set-id | rtg policy-set-id } [priority priority-id]
```

```
no call-policy-set { inbound-na | outbound-na | rtg }
```

### Syntax Description

<b>inbound-na</b>	Specifies a completed inbound number analysis policy.
<b>outbound-na</b>	Specifies a completed outbound number analysis policy.
<b>rtg</b>	Specifies a completed routing policy.
<i>policy-set-id</i>	The integer, ranging from 1 to 2147483647, that identifies a complete policy set.
<b>priority</b>	Specifies the administrative domain priority
<i>priority-id</i>	The priority value, ranging from 1 to 10, with 10 indicating the highest priority. By default, 10 is the priority value given to a policy set.

### Command Default

If the policy sets are not configured, an administrative domain uses the values defined within the default call policy set.

### Command Modes

Administrative domain configuration (config-sbc-sbe-ad)

### Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

### Examples

The following example shows how to configure an inbound and outbound number analysis and routing policy set for the administrative domain ADMIN1, and allocate priority to the policy sets using the **call-policy-set** command in the **Administrative domain** configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# admin-domain ADMIN1
Router(config-sbc-sbe-ad)# call-policy-set inbound-na 2 priority 10
Router(config-sbc-sbe-ad)# call-policy-set outbound-na 3 priority 10
Router(config-sbc-sbe-ad)# call-policy-set rtg 1 priority 10
```

**Related Commands**

<b>Command</b>	<b>Description</b>
admin-domain	Configures an administrative domain.
cac-policy-set (admin-domain)	Configures the CAC policy set for an administrative domain.
show sbc sbe admin-domain	Lists the administrative domains on the SBC and per adjacency.

# call-policy-set default

To activate a default policy set within an signaling border element (SBE) entity, use the **call-policy-set default** command in the **SBE** configuration mode. To deactivate a default policy set, use the **no** form of this command.

**call-policy-set default** *policy-set-id* [**priority** *priority-value*]

**no call-policy-set default**

## Syntax Description

<i>policy-set-id</i>	The integer, ranging from 1 to 2147483647, that identifies a default call policy set.
<b>priority</b>	Specifies the priority for the administrative domains that are not configured.
<i>priority-id</i>	The priority value, ranging from 1 to 10, with 10 indicating the highest priority. By default, 6 is the priority value given to the policy set.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The <b>call-policy-set default</b> command was renamed as <b>call-policy-set default</b> . The <b>priority</b> keyword and its value were also added.

## Usage Guidelines

If another policy set was previously active, it is made inactive by executing this command. The SBE is created with no active routing policy set; an active routing policy set must be explicitly configured using this command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to set policy set 1 as the default on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# call-policy-set default 1 priority 9
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	call-policy-set	Creates a new policy set on the session border controller (SBC).
	first-inbound-na-table	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
	first-outbound-na-table	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
	show sbc sbe call-policy-set	Lists the details of the policy sets configured on the SBC.
	show sbc sbe call-policy-set default	Lists the summary of the default policy set configured on the SBC.

# callee-bandwidth-field

To configure the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the callee, use the **callee-bandwidth-field** command in CAC table entry configuration mode. To remove the specific style of bandwidth line format, use the **no callee-bandwidth-field** command.

**callee-bandwidth-field** [*as-to-tias* | *tias-to-as*]

**no callee-bandwidth-field** [*as-to-tias* | *tias-to-as*]

Syntax Description		
<i>as-to-tias</i>	This option causes the SBC to convert a b=AS line format into a b=TIAS line format, for a given SDP bandwidth modifier in an outbound offer.	AS = Application Specific Maximum TIAS = Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.
<i>tias-to-as</i>	This option causes the SBC to convert a b=TIAS line format into a b=AS line format, for a given SDP bandwidth modifier in an outbound offer.	AS = Application Specific Maximum TIAS = Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.

**Command Default** The default is that the bandwidth line is not translated from one format to another.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** The SBC follows whichever outgoing bandwidth line format is configured. If the outgoing adjacency is configured to prefer a specific style of bandwidth line, then the preferred format is used, and any b=AS or b=TIAS lines are translated to that format.

If the answerer-side adjacency is configured to prefer a specific style of bandwidth line format in the SDP, this command causes the SBC to convert the offer to the specified format before being sent to the answerer. If there are multiple bandwidth lines, only the first is converted into the specified bandwidth line and the rest are ignored.



**Note**

The default is that the bandwidth line is not translated from one format to another. However, if the callee is configured to convert the bandwidth, and the message is converted, then the response back to the caller is converted back even if the caller-bandwidth-field option is not provisioned.

**Examples**

The following example shows the SBC is configured to convert an AS bandwidth line format into a TIAS bandwidth line format in an outbound SDP sent to the callee:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-bandwidth-field as-to-tias
```

**Related Commands**

Command	Description
<b>caller-bandwidth-field</b> [ <i>as-to-tias</i>   <i>tias-to-as</i> ]	Configures the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the caller.

# callee-codec-list

To list the codecs which the callee leg of a call is allowed to use, use the **callee-codec-list** command in the CAC table entry configuration mode. To delete a codec list, use the **no** form of this command.

**callee-codec-list** *list-name*

**no callee-codec-list** *list-name*

## Syntax Description

<i>list-name</i>	Specifies the name of the codec list.  The <i>list-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to enter a mode to create a codec list using the name test:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-codec-list test
```



# callee-hold-setting

To configure the callee hold settings that are supported, use the **callee-hold-setting** command in CAC table entry configuration mode. To deconfigure the callee hold settings, use the **no** form of this command.

*callee-hold-setting {hold-c0 | hold-c0-inactive | hold-c0-sendonly | hold-sendonly | standard}*

*no callee-hold-setting {hold-c0 | hold-c0-inactive | hold-c0-sendonly | hold-sendonly | standard}*

Syntax Description	
hold-c0	Callee supported; requires c=I 0.0.0.0.
hold-c0-inactive	Callee supported; requires c=I 0.0.0.0 or a=inactive.
hold-c0-sendonly	Callee supported; requires c=0.0.0.0 or a=sendonly
hold-sendonly	Callee supported; requires a=sendonly.
standard	Callee supported; requires c=0.0.0.0 and either a=forward-direction capability.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the callee hold settings:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value fairchild
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-hold-setting hold-sendonly
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

**Related Commands**

<b>Command</b>	<b>Description</b>
callee-inbound-policy	Configures a callee inbound SDP policy table.
<b>callee-outbound-policy</b>	Configures a callee outbound SDP policy table.

# callee-inbound-policy

To configure a callee inbound SDP policy table, use the *callee-inbound-policy* command in CAC table entry configuration mode. To, use the **no** form of this command.

*callee-inbound-policy* *WORD*

**no** *callee-inbound-policy* *WORD*

<b>Syntax Description</b>	<i>WORD</i>	Specifies the name of the SDP policy table. The maximum size is 30 characters.
<b>Command Default</b>	No default behavior or values are available.	
<b>Command Modes</b>	CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.	
<b>Examples</b>	The following example shows how to create the admission control table MyCacTable: <pre>Router# configure terminal Router(config)# sbc mySbc Router(config-sbc)# sbe Router(config-sbc-sbe)# cac-policy-set 1 Router(config-sbc-sbe-cacpolicy)# first-cac-scope global Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account Router(config-sbc-sbe-cacpolicy-cactable)# entry 1 Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-inbound-policy test</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	callee-hold-setting	Configures the callee hold settings that are supported.
	callee-outbound-policy	Configures a callee outbound SDP policy table.

# callee-media-caps

To configure a codec list used to announce media capabilities on behalf of a SIP callee in a SIP to H.323 or H.323 to SIP interworking call, use the **callee-media-caps** command in CAC table entry configuration mode. To remove the codec list, use the **no callee-media-caps** command.

**callee-media-caps** *{code-list-name}*

**no callee-media-caps** *{code-list-name}*

## Syntax Description

<i>code-list-name</i>	This is a string text of a maximum length of 30 characters. Describes the extra codecs that a SIP callee can announce to the H.323 side.
-----------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.5.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command configures a codec list and assigns the list to a CAC table.

Once a codec list has been assigned, it may not be deleted until it is removed from the CAC table entry. A codec list must exist before it can be assigned to an entry in a CAC table.

For a description of “H.323 TCS Codecs,” see the “Codec Handling” chapter in the [Cisco Unified Border Element \(SP Edition\) Configuration Guide: Unified Model](#).

## Examples

The following example configures a codec list called “callee-media-caps-list” and assigns that list to the CAC table “cac-tbl-1” in entry 1 to announce that T.38 was added as a callee SIP media capabilities.

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list callee-media-caps-list
Router(config-sbc-sbe-codec-list)# codec t38
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table cac-tbl-1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-media-caps callee-media-caps-list
```

Related Commands	Command	Description
	caller-media-caps	Configures a codec list used to announce media capabilities on behalf of a SIP caller in a SIP to H.323 or H.323 to SIP interworking call.
	tcs-extra-caps-list	Configures a codec list used to announce media capabilities on behalf of both the SIP caller and callee in a SIP to H.323 or H.323 to SIP interworking call.

# callee-outbound-policy

To configure a callee outbound SDP policy table, use the **callee-outbound-policy** command in CAC table entry configuration mode. To, use the **no** form of this command.

*callee-outbound-policy WORD*

*no callee-outbound-policy WORD*

<b>Syntax Description</b>	<i>WORD</i>	Specifies the name of the SDP policy table. The maximum size is 30 characters.
---------------------------	-------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to create the admission control table MyCacTable:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-inbound-policy test
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>callee-hold-setting</b>	Configures the callee hold settings that are supported.
	<b>callee-inbound-policy</b>	Configures a callee inbound SDP policy table.

# callee-privacy edit-privacy-request

To edit and update privacy indications provided by the user, use the **callee-privacy edit-privacy-request** command in CAC table configuration mode. To remove the indications, use the **no** form of this command.

```
callee-privacy edit-privacy-request {pass | strip | insert | replace | sip {strip {all | critical | header | id | none | session | token word | user} | insert {critical | header | id | none | session | token word | user}}}
```

```
no callee-privacy edit-privacy-request {pass | strip | insert | replace | sip {strip {all | critical | header | id | none | session | token word | user} | insert {critical | header | id | none | session | token word | user}}}
```

Syntax Description	
<b>insert</b>	Inserts privacy restrictions: <ul style="list-style-type: none"> <li>• SIP—Inserts Privacy:header;session;user;id;critical, if the header is not present already</li> <li>• H323—Sets presentation indicator from allowed to restricted.</li> </ul>
<b>pass</b>	Passes on the privacy header or presentation indicators.
<b>replace</b>	Replaces privacy restrictions: <ul style="list-style-type: none"> <li>• SIP—Replaces the Privacy:header;session;user;id;critical, except when none has been requested.</li> <li>• H323—Sets presentation indicator to restricted.</li> </ul>
<b>strip</b>	Removes all privacy restrictions: <ul style="list-style-type: none"> <li>• SIP—Removes Privacy header.</li> <li>• H323—Set presentation indicator to allowed.</li> </ul>
<b>sip</b>	Specifies the following SIP settings that allows greater control and overrides all generic actions: <ul style="list-style-type: none"> <li>• <b>insert</b>—Inserts Privacy tokens into the Privacy header.</li> <li>• <b>strip</b>—Removes privacy tokens from the Privacy header.</li> </ul>
<b>critical</b>	Specifies the call to discontinue if privacy cannot be achieved in the SIP Privacy header.
<b>header</b>	Obscures all header information that is related to the user from the SIP Privacy header.
<b>id</b>	Adds or removes the ID headers from the SIP Privacy header.
<b>none</b>	Privacy is not applied to call.
<b>session</b>	Specifies the media privacy for the session in the SIP Privacy header. No media bypass is performed.
<b>token</b>	Specifies the non standard user defined privacy token in the SIP Privacy header.
<i>word</i>	Specifies the user defined privacy token.
<b>user</b>	Removes all non-essential header information that is related to the user from the SIP Privacy header.

**Command Default** *The privacy request editing is set to Pass.*

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified from <b>callee-privacy</b> to <b>callee-privacy edit-privacy-request</b> . The <b>callee-privacy limited-privacy-service</b> command has been removed.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the entry to remove all privacy restrictions from SIP and H323 adjacencies in the new admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-privacy edit-privacy-request strip
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands	Command	Description
	<b>cac-table</b>	Configures admission control tables.
	<b>callee-privacy privacy-service</b>	Applies privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings.
	<b>table-type</b>	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.



# callee-privacy privacy-service

To apply privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings in the given entry in the admission control table, use the **callee-privacy privacy-service** command in CAC table configuration mode. To remove the privacy settings, use the **no** form of this command.

**callee-privacy privacy-service {adj-trust-boundary | always | never}**

**no callee-privacy privacy-service**

Syntax Description	
<b>adj-trust-boundary</b>	Specifies the adjacency privacy trust level to determine if the privacy service is required.
<b>always</b>	Provides privacy service always, if requested by the user.
<b>never</b>	Never provides privacy service even if requested by the user.

**Command Default** The privacy setting value is set to adj-trust-boundary.

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified from <b>callee-privacy</b> to <b>callee-privacy privacy-service</b> . The <b>callee-privacy limited-privacy-service</b> command has been removed.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the entry to provide privacy service always as requested by the user in the new admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-privacy privacy-service always
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands	Command	Description
	<b>cac-table</b>	Configures admission control tables.
	callee-privacy edit-privacy-request	Edits and updates privacy indications provided by the user
	<b>table-type</b>	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

# callee-sig-qos-profile

To configure the QoS profile to be used for signaling packets sent to the original callee, use the **callee-sig-qos-profile** command in the CAC table entry configuration mode. To **deconfigure the QoS profile**, use the **no** form of this command.

**callee-sig-qos-profile** *profile-name*

**no callee-sig-qos-profile** *profile-name*

## Syntax Description

<i>profile-name</i>	Specifies the name of the QoS profile. The string “default” is reserved. The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **callee-sig-qos-profile** command is used to configure the QoS profile named enterprise to be used for signaling packets sent to the original callee:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-sig-qos-profile enterprise
```

## callee tel-event payload type

To configure the payload type to be used for the callee in H.323-SIP interworking calls, use the **callee tel-event payload-type** command in the CAC entry configuration mode. To unconfigure the payload type setting, use the **no** form of this command.

**callee tel-event payload type** *payload-type*

**no callee tel-event payload type**

### Syntax Description

<i>payload-type</i>	See RFC 2833 for detailed information about the values of <i>payload-type</i> . The range is from 96 to 127. The default is 101.
---------------------	--

### Command Default

No default behavior or values are available.

### Command Modes

CAC entry configuration (config-sbc-cac-entry)

### Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers in a release earlier than Release 3.1S.

### Usage Guidelines

The **callee tel-event payload type** command enables support for dual tone multifrequency (DTMF) H.323-SIP interworking. The telephone-event payload type configured by this command is used by the SBC only in situations where the payload type information is not provided by the other side in an H.323-SIP interworking call.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to use the **callee tel-event payload-type** command to set the payload type to 101:

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-cac-pol)# cac-table CAC-POLICY-TBL1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee tel-event payload-type 101
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>branch tel-event payload-type</b>	Configures the payload type to be used for the callee or the caller in H.323-SIP interworking calls.
<b>caller tel-event payload-type</b>	Configures the payload type to be used for the caller in H.323-SIP interworking calls.

# callee-video-qos-profile

To configure the QoS profile to use for media packets sent to the original callee, use the **callee-video-qos-profile** command in CAC table entry configuration mode. To return to the default behavior, use the **no** form of this command.

**callee-video-qos-profile** *profile-name*

**no callee-video-qos-profile**

## Syntax Description

<i>profile-name</i>	Name of the QoS profile.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

The **callee-video-qos-profile** can be executed only at the per-call scope. CAC policy does not activate if configured at any other scope.

## Examples

The following example shows how to configure calls from the acme account to use the video QoS profile enterprise for packets sent from the SBC to the original callee:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme  
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-video-qos-profile enterprise  
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit  
Router(config-sbc-sbe-cacpolicy-cactable)# exit  
Router(config-sbc-sbe-cacpolicy)# exit
```

# callee-voice-qos-profile

To configure the QoS profile to use for media packets sent to the original callee, use the **callee-voice-qos-profile** command in CAC table entry configuration mode. To return to the default behavior, use the **no** form of this command.

**callee-voice-qos-profile** *profile-name*

**no callee-voice-qos-profile**

## Syntax Description

<i>profile-name</i>	Name of the QoS profile.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

This command can be executed only at the per-call scope. CAC policy does not activate if this command is configured at any other scope.

## Examples

The following example shows how to configure calls from the acme account to use the voice QoS profile enterprise for packets sent from the SBC to the original callee.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
```



```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee-voice-qos-profile enterprise  
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit  
Router(config-sbc-sbe-cacpolicy-cactable)# exit  
Router(config-sbc-sbe-cacpolicy)# exit
```

# callee codec

To configure the codec options for a callee, use the **callee codec** command in the CAC table entry configuration mode. To deconfigure the codec options, use the **no** form of this command.

**callee codec {convert | profile *profile-name*}**

**no callee codec {convert | profile}**

## Syntax Description

<b>convert</b>	Enables or disables the codec variant conversion.
<b>profile</b>	Specifies or removes the codec variant profile.
<i>profile-name</i>	The codec variant profile name.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

## Command Default

By default, codec variant conversion is disabled, and no codec variant profile is specified.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the codec options for a callee using the **callee codec** command in the CAC table entry mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee codec convert
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee codec profile profile-1
```



# callee inband-dtmf-mode

To configure the dual tone multifrequency (DTMF) in-band mode for the callee side, use the **callee inband-dtmf-mode** command in the CAC table entry configuration mode. To deconfigure the DTMF in-band mode for the callee side, use the **no** form of this command.

**callee inband-dtmf-mode** { **always** | **inherit** | **maybe** | **never** }

**no callee inband-dtmf-mode**

## Syntax Description

<b>always</b>	Specifies that the in-band DTMF tones are always used by the endpoint.
<b>inherit</b>	Specifies that the in-band DTMF mode for the endpoint is not affected by the CAC entry.
<b>maybe</b>	Specifies that the in-band DTMF tones are used by the endpoint unless signaling indicates that an alternative format is in use for the DTMF.
<b>never</b>	Specifies that the endpoint never uses in-band DTMF.

## Command Default

No default behavior or values.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the DTMF in-band mode for the callee side using the **callee inband-dtmf-mode** command in the CAC table entry configuration mode so that the in-band DTMF tones are always in use by the endpoint:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table InbandDTMF
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee inband-dtmf-mode always
```

Related Commands	Command	Description
	caller inband-dtmf-mode	Configures the DTMF in-band mode for the caller side

# callee media-description disabled

To configure how Cisco Unified Border Element (SP Edition) handles disabled media descriptions for a callee, use the **callee media-description disabled** command in the CAC table entry configuration mode.

```
callee media-description disabled {strip {answer | offer {all | new}} | {pad offer}}
```

```
no callee media-description disabled {strip {answer | offer {all | new}} | {pad offer}}
```

## Syntax Description

strip	Strips disabled media description lines.
pad	Pads with dummy disabled media description lines.
answer	Strips disabled media description lines from answers.
offer	Strips disabled media description lines from offers when used with strip. Pad offers with dummy disabled media description lines when used with pad.
all	Strips all disabled media descriptions from offers.
new	Strips new disabled media descriptions from offers.

## Command Default

Pad and do-not-strip are the default behaviors.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to remove disabled media streams in forwarded offers which are new:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-description disabled strip offer new
```

The following example shows how to remove all disabled media streams from forwarded offers, whether known to the recipient of the offer or not.

```
Router# configure terminal
Router(config)# sbc mySbc
```

```
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-description disabled strip
offer all
```

The following example shows how to remove all disabled media streams from forwarded answers.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-description disabled strip
answer
```

The following example shows how to stop SBC from padding forwarded offers with disabled media streams.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# no callee media-description disabled pad
offer
```

# callee media-type

To configure the media address type settings for a callee on the Cisco Unified Border Element (SP Edition), use the **callee media-type** command in the CAC table entry configuration mode. Use the **no** form of this command to disable the media address type settings for a callee.

**callee media-type {ipv4 | ipv6 | inherit | both}**

**no callee media-type {ipv4 | ipv6 | inherit | both}**

## Syntax Description

ipv4	Only IPv4 media addresses are supported.
ipv6	Only IPv6 media addresses are supported.
inherit	Inherit the supported media IP address type from earlier CAC policy entries (default).
both	Both IPv4 and IPv6 media addresses are supported.

## Command Default

The default behavior is inherit.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to remove disabled media streams in forwarded offers which are new:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media-type ipv4
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```



# callee media bypass

To enable or disable the Multiple SBC Media Bypass feature on the callee side, use the **callee media bypass** command in the CAC table entry configuration mode. To deconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

```
callee media bypass {enable | disable}
```

```
no callee media bypass
```

Syntax Description	enable	Enables the Multiple SBC Media Bypass feature on the callee side.
	disable	Disables the Multiple SBC Media Bypass feature on the callee side.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to enable the Multiple SBC Media Bypass feature on the callee side:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee media bypass enable
```

Related Commands	Command	Description
	<b>cac-table</b>	Configures admission control tables.
	caller media bypass	Enables or disables the Multiple SBC Media Bypass feature on the caller side.
	<b>table-type</b>	Configures a CAC table type to enable the priority of the call to be used as a criterion in the CAC policy.



# callee port-range-tag

To configure the port range tag for a callee that is used when selecting a media address and port, use the **callee port-range-tag** command in the CAC table entry configuration mode. To deconfigure the port range tag, use the **no** form of this command.

```
callee port-range-tag {adj-name | none | string tag-string}
```

```
no callee port-range-tag
```

## Syntax Description

<i>adj-name</i>	Uses the destination adjacency name as a port-range tag.
<b>none</b>	Prompts the SBC to not use a port range tag for calls matching the CAC entry, and removes any previously found strings.
<i>string tag-string</i>	Specifies the explicit port range tag string.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure a port-range tag:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match SIPIMSAccess
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee port-range-tag string
GenericCorePortRange
```

## Related Commands

Command	Description
<b>media-address-pool</b>	Adds an IPv4 and IPv6 address to the set of addresses that can be used by the DBE as a local media address.

# callee ptime

To configure the packetization time on the callee side, use the **callee ptime** command in the CAC table configuration mode. To deconfigure the packetization time on the callee side, use the **no** form of this command.

```
callee ptime 0-100
```

```
no callee ptime 0-100
```

## Syntax Description

*0-100* The packetization time in milliseconds (ms).

## Command Default

By default, 0 ms is configured. This means that no transrating occurs.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the packetization time on the callee side using the **callee ptime** command in the CAC table configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee ptime 30
```

## Related Commands

Command	Description
<b>caller ptime</b>	Configures the packetization time on the caller side.

# callee secure-media

To configure granular-level Secure Media on the callee side, use the **callee secure-media** command in CAC table entry configuration mode. To remove granular-level Secure Media, use the **no callee secure-media** command.

**callee secure-media**

**no callee secure-media**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Granular-level (Unsigned) Secure Media is disabled by default.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Restriction—Both caller and callee sides of the call need to be configured. If only one leg of the call has granular secure media configured, then the call will fail.

We recommend you use unsigned (also called granular-level) Secure Media configuration because, instead of turning on Secure Media globally, you can specify the calls and adjacencies where you want to use Secure Media.

## Examples

The following example shows an Unsigned Secure Media configuration where the two SIP adjacencies for both legs of the call are configured for “security trusted-unencrypted” and both the caller and callee sides are configured for Secure Media in a CAC table entry:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# adjacency sip server
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table testSecure
Router(config-sbc-sbe-cacpolicy)# cac-table testSecure
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller secure-media
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee secure-media
```

```

Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# cac-policy-set global 1
Router(config-sbc-sbe)# end

```

The following configuration example shows how to configure Unsignaled Secure Media where an adjacency is *untrusted* by using the **transport srtp allowed** command on the untrusted adjacency in a CAC policy table:

```

...
cac-policy-set 2
  first-cac-table 1
  cac-table 1
    table-type limit all
    entry 1
      match-value call-update
      transport srtp allowed
      caller secure-media
      callee secure-media
      action cac-complete
      exit
    complete
  exit
cac-policy-set global 2

```

The following configuration example shows that SIP adjacencies ‘client’ and ‘server’ are configured as “security trusted-unencrypted” and that CAC table entry 1 is configured for Secure Media on both the caller and callee sides:

```

...
cac-policy-set 2
  first-cac-table 1
  cac-table 1
    table-type policy-set
    entry 1
      action cac-complete
      caller secure-media
      callee secure-media
    complete
cac-policy-set global 2

adjacency sip client
  nat force-off
  security trusted-unencrypted
  signaling-address ipv4 10.10.100.110
  signaling-port 9060
  remote-address ipv4 10.10.100.10 255.255.255.255
  signaling-peer 10.10.100.10
  signaling-peer-port 9060
  attach

adjacency sip server
  nat force-off
  security trusted-unencrypted
  signaling-address ipv4 10.10.100.110
  signaling-port 9070
  remote-address ipv4 10.10.100.10 255.255.255.255
  signaling-peer 10.10.100.10
  signaling-peer-port 9070
  attach

```

**Related Commands**

<b>Command</b>	<b>Description</b>
caller secure-media	Configures granular-level Secure Media on the caller side.
security	Configures transport-level security (TLS) on a SIP adjacency.

# caller-bandwidth-field

To configure the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the caller, use the **caller-bandwidth-field** command in CAC table entry configuration mode. To remove the specific style of bandwidth line format, use the **no caller-bandwidth-field** command.

**caller-bandwidth-field** [*as-to-tias* | *tias-to-as*]

**no caller-bandwidth-field** [*as-to-tias* | *tias-to-as*]

## Syntax Description

<i>as-to-tias</i>	Configures the SBC to convert a b=AS line format into a b=TIAS line format, for a given SDP media descriptor in an outbound offer.  AS —Application Specific Maximum  TIAS—Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.
<i>tias-to-as</i>	Configures the SBC to convert a b=TIAS line format into a b=AS line format, for a given SDP media descriptor in an outbound offer.  AS—Application Specific Maximum  TIAS—Transport Independent Application Specific Maximum has an integer bit-rate value in bits per second.

## Command Default

The default is that the bandwidth line is not translated from one format to another.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The SBC follows whichever outgoing bandwidth line format is configured. If the outgoing adjacency is configured to prefer a specific style of bandwidth line, then the preferred format is used, and any b=AS or b=TIAS lines are translated to that format.

If the offerer-side adjacency is configured to prefer a specific style of bandwidth line format in the SDP, this command causes the SBC to convert the answer to the specified format before being sent back to the offerer. If there are multiple bandwidth lines, only the first is converted into the specified bandwidth line and the rest are ignored.



### Note

The default is that the bandwidth line is not translated from one format to another. However, if the callee is configured to convert the bandwidth, and the message is converted, then the response back to the caller is converted back even if the caller-bandwidth-field option is not provisioned.



**Examples**

The following example shows the SBC is configured to convert an AS bandwidth line format into a TIAS bandwidth line format in an outbound SDP sent to the caller:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-bandwidth-field as-to-tias
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee-bandwidth-field</b>	Configures the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the callee.

# caller-codec-list

To list the codecs which the caller leg of a call is allowed to use, use the **caller-codec-list** command in the CAC table entry configuration mode. To delete a codec list, use the **no** form of this command.

**caller-codec-list** *list-name*

**no caller-codec-list** *list-name*

## Syntax Description

<i>list-name</i>	Specifies the name of the codec list.  The <i>list-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to enter a mode to create a codec list using the name test:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-codec-list test
```

# caller-hold-setting

To configure the caller hold settings that are supported, use the **caller-hold-setting** command in CAC table entry configuration mode. To cancel caller hold settings, use the **no** form of this command.

**caller-hold-setting** { **hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard** }

**no caller-hold-setting** { **hold-c0** | **hold-c0-inactive** | **hold-c0-sendonly** | **hold-sendonly** | **standard** }

Syntax Description		
hold-c0	Specifies callee supported; requires c=I 0.0.0.0.	
hold-c0-inactive	Specifies callee supported; requires c=I 0.0.0.0 or a=inactive.	
hold-c0-sendonly	Specifies callee supported; requires c=0.0.0.0 or a=sendonly	
hold-sendonly	Specifies callee supported; requires a=sendonly.	
standard	Specifies callee supported; requires c=0.0.0.0 and either a=forward-direction capability.	

**Command Default** *The default is standard.*

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the caller hold settings:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value fairchild
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-hold-setting hold-sendonly
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

**Related Commands**

<b>Command</b>	<b>Description</b>
caller-outbound-policy	Configures a caller outbound SDP policy table.
<b>caller-inbound-policy</b>	Configures a caller inbound SDP policy table.

# caller-inbound-policy

To configure a caller inbound SDP policy table, use the **caller-inbound-policy** command in CAC table entry configuration mode. To deconfigure a caller inbound SDP policy table, use the **no** form of this command.

**caller-inbound-policy** *WORD*

**no caller-inbound-policy** *WORD*

<b>Syntax Description</b>	<i>WORD</i> Specifies the name of the SDP policy table. The maximum size is 30 characters.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure a caller inbound SDP policy table:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-inbound-policy test
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	caller-hold-setting	Configures the caller hold settings.
	<b>caller-outbound-policy</b>	Configure a caller outbound SDP policy table.
	codec	Adds a codec to a codec list.
	caller-codec-list	Lists the codecs which the caller of a call can use.

# caller-media-caps

To configure a codec list used to announce media capabilities on behalf of a SIP caller in a SIP to H.323 or H.323 to SIP interworking call, use the **caller-media-caps** command in CAC table entry configuration mode. To remove the codec list, use the **no caller-media-caps** command.

**caller-media-caps** *{code-list-name}*

**no caller-media-caps** *{code-list-name}*

## Syntax Description

<i>code-list-name</i>	This is a string text of a maximum length of 30 characters. Describes the extra codecs that a SIP caller can announce to the H.323 side.
-----------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.5.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command configures a codec list and assigns the list to a CAC table.

Once a codec list has been assigned, it may not be deleted until it is removed from the CAC table entry. A codec list must exist before it can be assigned to an entry in a CAC table.

For a description of “H.323 TCS Codecs,” see the “Codec Handling” chapter in the [Cisco Unified Border Element \(SP Edition\) Configuration Guide: Unified Model](#).

## Examples

The following example configures a codec list called “caller-media-caps-list” and assigns that list to the CAC table “cac-tbl-1” in entry 1 to announce that T.38 is added as a caller SIP media capabilities:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list caller-media-caps-list
Router(config-sbc-sbe-codec-list)# codec t38
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table cac-tbl-1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-media-caps caller-media-caps-list
```

Related Commands	Command	Description
	callee-media-caps	Configures a codec list used to announce media capabilities on behalf of a SIP callee in a SIP to H.323 or H.323 to SIP interworking call.
	tcs-extra-caps-list	Configures a codec list used to announce media capabilities on behalf of both the SIP caller and callee in a SIP to H.323 or H.323 to SIP interworking call.

# caller-outbound-policy

To configure a caller outbound SDP policy table, use the **caller-outbound-policy** command in CAC table entry configuration mode. To deconfigure a caller outbound SDP policy table, use the **no** form of this command.

**caller-outbound-policy** *table\_name*

**no caller-outbound-policy** *table\_name*

<b>Syntax Description</b>	<i>WORD</i> Specifies the name of the SDP policy table. The maximum size is 30 characters.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

**Examples** The following example shows how to configure a caller outbound SDP Limit table:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope global
Router(config-sbc-sbe-cacpolicy)# first-cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy)# cac-table callhold-dst-settings
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-account
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-outbound-policy test
```

<b>Command</b>	<b>Description</b>
caller-hold-setting	Configures the caller hold settings.
caller-inbound-policy	Configures a caller inbound SDP policy table.



# caller-privacy edit-privacy-request

To edit and update privacy indications provided by the user, use the **caller-privacy edit-privacy-request** command in CAC table configuration mode. To remove the indications, use the **no** form of this command.

```
caller-privacy edit-privacy-request {pass | strip | insert | replace | sip {strip {all | critical | header | id | none | session | token word | user} | insert {critical | header | id | none | session | token word | user}}}
```

```
no caller-privacy edit-privacy-request {pass | strip | insert | replace | sip {strip {all | critical | header | id | none | session | token word | user} | insert {critical | header | id | none | session | token word | user}}}
```

Syntax Description	
<b>insert</b>	Inserts privacy restrictions: <ul style="list-style-type: none"> <li>• SIP—Inserts Privacy:header;session;user;id;critical, if the header is not present already</li> <li>• H323—Sets presentation indicator from allowed to restricted.</li> </ul>
<b>pass</b>	Passes on the privacy header or presentation indicators.
<b>replace</b>	Replaces privacy restrictions: <ul style="list-style-type: none"> <li>• SIP—Replaces the Privacy:header;session;user;id;critical, except when none has been requested.</li> <li>• H323—Sets presentation indicator to restricted.</li> </ul>
<b>strip</b>	Removes all privacy restrictions: <ul style="list-style-type: none"> <li>• SIP—Removes Privacy header.</li> <li>• H323—Set presentation indicator to allowed.</li> </ul>
<b>sip</b>	Specifies the following SIP settings that allows greater control and overrides all generic actions: <ul style="list-style-type: none"> <li>• <b>insert</b>—Inserts Privacy tokens into the Privacy header.</li> <li>• <b>strip</b>—Removes privacy tokens from the Privacy header.</li> </ul>
<b>critical</b>	Specifies the call to discontinue if privacy cannot be achieved in the SIP Privacy header.
<b>header</b>	Obscures all header information that is related to the user from the SIP Privacy header.
<b>id</b>	Adds or removes the ID headers from the SIP Privacy header.
<b>none</b>	Privacy is not applied to call.
<b>session</b>	Specifies the media privacy for the session in the SIP Privacy header. No media bypass is performed.
<b>token</b>	Specifies the non standard user defined privacy token in the SIP Privacy header.
<i>word</i>	Specifies the user defined privacy token.
<b>user</b>	Removes all non-essential header information that is related to the user from the SIP Privacy header.

**Command Default** *The privacy request editing is set to Pass.*

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified from <b>caller-privacy</b> to <b>caller-privacy edit-privacy-request</b> . The <b>caller-privacy limited-privacy-service</b> command has been removed.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the entry to remove all privacy restrictions from SIP and H323 adjacencies in the new admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-privacy edit-privacy-request strip
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Command	Description
<b>cac-table</b>	Configures admission control tables.
<b>caller-privacy privacy-service</b>	Applies privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings.
<b>table-type</b>	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

# caller-privacy privacy-service

To apply privacy settings according to RFC3323, RFC3325, and/or setting of H.323 presentation restriction settings in the given entry in the admission control table, use the **caller-privacy privacy-service** command in CAC table configuration mode. To remove the privacy settings, use the **no** form of this command.

**caller-privacy privacy-service** { **adj-trust-boundary** | **always** | **never** }

**no caller-privacy privacy-service**

Syntax Description	
<b>adj-trust-boundary</b>	Specifies the adjacency privacy trust level to determine if the privacy service is required.
<b>always</b>	Provides privacy service always, if requested by the user.
<b>never</b>	Never provides privacy service even if requested by the user.

**Command Default** The privacy setting value is set to adj-trust-boundary.

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified from <b>caller-privacy</b> to <b>caller-privacy privacy-service</b> . The <b>caller-privacy limited-privacy-service</b> command has been removed.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the entry to provide privacy service always as requested by the user in the new admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-privacy privacy-service always
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands	Command	Description
	<b>cac-table</b>	Configures admission control tables.
	caller-privacy edit-privacy-request	Edits and updates privacy indications provided by the user
	<b>table-type</b>	Configures a CAC table type that enables the priority of the call to be used as a criterion in CAC policy.

# caller-sig-qos-profile

To **configure** the QoS profile to use for signaling packets sent to the original caller, use the **caller-sig-qos-profile** command in the CAC table entry configuration mode. To **deconfigure the QoS profile**, use the **no** form of this command.

**caller-sig-qos-profile** *profile-name*

**no caller-sig-qos-profile** *profile-name*

## Syntax Description

<i>profile-name</i>	Specifies the name of the QoS profile. The string “default” is reserved. The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command can only be executed at the per-call scope. CAC policy will not activate if this command is configured at any other scope.

Packet marking will not be applied until the CAC decision process is run. This means that some initial signaling packets sent to the caller (for example, the SIP 100 provisional response) will not receive any particular DSCP marking.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

---

**Examples**

The following command configures calls from the acme account to use the voice QoS profile enterprise for signaling packets sent from the SBC to the original caller:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-sig-qos-profile enterprise
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

## caller tel-event payload type

To configure the payload type to be used for the caller in H.323-SIP interworking calls, use the **caller tel-event payload-type** command in the CAC entry configuration mode. To unconfigure the payload type setting, use the **no** form of this command.

**caller tel-event payload type** *payload-type*

**no caller tel-event payload type**

<b>Syntax Description</b>	<i>payload-type</i>	See RFC 2833 for detailed information about the values of <i>payload-type</i> . The range is from 96 to 127. The default is 101.
---------------------------	---------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC entry configuration (config-sbc-cac-entry)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers in a release earlier than Release 3.1S.

<b>Usage Guidelines</b>	The <b>caller tel-event payload type</b> command enables support for dual tone multifrequency (DTMF) H.323-SIP interworking. The telephone-event payload type configured by this command is used by the SBC only in situations where the payload type information is not provided by the other side in an H.323-SIP interworking call.
-------------------------	--

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

<b>Examples</b>	The following example shows how to use the <b>caller tel-event payload-type</b> command to set the payload type to 101:
-----------------	---

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-cac-pol)# cac-table CAC-POLICY-TBL1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller tel-event payload-type 101
```

Related Commands	Command	Description
	<b>branch tel-event payload-type</b>	Configures the payload type to be used for the callee or the caller in H.323-SIP interworking calls.
	<b>callee tel-event payload-type</b>	Configures the payload type to be used for the callee in H.323-SIP interworking calls.



# caller-video-qos-profile

To configure the QoS profile to use for media packets sent to the original caller, use the **caller-video-qos-profile** command in CAC table configuration mode. To remove this configuration, use the **no** form of this command.

**caller-video-qos-profile** *profile-name*

**no caller-video-qos-profile** *profile-name*

## Syntax Description

<i>profile-name</i>	Specifies the Qos profile.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  Except for the underscore character, do not use any special character to specify field names.
---------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

The **caller-video-qos-profile** command can be executed only at the per-call scope. CAC policy does not activate if this command is configured at any other scope.

## Examples

The following example shows how to configure calls from the acme account to use the video QoS profile enterprise for packets sent from the SBC to the original caller:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme  
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-video-qos-profile enterprise  
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit  
Router(config-sbc-sbe-cacpolicy-cactable)# exit  
Router(config-sbc-sbe-cacpolicy)# exit
```

# caller-voice-qos-profile

To configure the QoS profile to use for media packets sent to the original caller, use the **caller-voice-qos-profile** command in CAC table configuration mode. To remove this configuration, use the **no** form of this command.

**caller-voice-qos-profile** *profile-name*

**no caller-voice-qos-profile**

## Syntax Description

*profile-name* Specifies the QoS profile.

The *profile-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

**Note** Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

This command can be executed only at the per-call scope. CAC policy does not activate if this command is configured at any other scope.

## Examples

The following example shows how to configure calls from the acme account to use the voice QoS profile enterprise for packets sent from the SBC to the original caller:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-account
Router(config-sbc-sbe-cacpolicy-cactable)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match-value acme  
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller-voice-qos-profile enterprise  
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit  
Router(config-sbc-sbe-cacpolicy-cactable)# exit  
Router(config-sbc-sbe-cacpolicy)# exit
```

# caller codec

To configure the codec options for a caller, use the **caller codec** command in the CAC table entry configuration mode. To deconfigure the codec options, use the **no** form of this command.

```
caller codec {convert | profile profile-name}
```

```
no caller codec {convert | profile}
```

Syntax Description	convert	Enables or disables the codec variant conversion.
	<b>profile</b>	Specifies or removes the codec variant profile.
	<i>profile-name</i>	The codec variant profile name.

**Command Default** By default, codec variant conversion is disabled, and no codec variant profile is specified.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to configure the codec options for a caller using the **caller codec** command in the CAC table entry mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller codec convert
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller codec profile profile-1
```

# caller inband-dtmf-mode

To configure the dual tone multifrequency (DTMF) in-band mode for the caller side, use the **caller inband-dtmf-mode** command in the CAC table entry configuration mode. To deconfigure the DTMF in-band mode for the caller side, use the **no** form of this command.

**caller inband-dtmf-mode** { **always** | **inherit** | **maybe** | **never** }

**no caller inband-dtmf-mode**

## Syntax Description

<b>always</b>	Specifies that the in-band DTMF tones are always used by the endpoint.
<b>inherit</b>	Specifies that the in-band DTMF mode for the endpoint is not affected by the CAC entry.
<b>maybe</b>	Specifies that the in-band DTMF tones are used by the endpoint unless signaling indicates that an alternative format is in use for the DTMF.
<b>never</b>	Specifies that the endpoint never uses in-band DTMF mode.

## Command Default

No default behavior or values.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the DTMF in-band mode for the caller side using the **caller inband-dtmf-mode** command in the CAC table entry configuration mode so that the endpoint never uses in-band DTMF mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table InbandDTMF
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller inband-dtmf-mode never
```

Related Commands	Command	Description
	callee inband-dtmf-mode	Configures the DTMF in-band mode for the callee side.

# caller media-description disabled

To configure how Cisco Unified Border Element (SP Edition) handles disabled media descriptions for a caller, use the **caller media-description disabled** command in the CAC table entry configuration mode.

**caller media-description disabled {strip {answer | offer {all | new}} | {pad offer}}**

**no caller media-description disabled {strip {answer | offer {all | new}} | {pad offer}}**

## Syntax Description

strip	Strips disabled media description lines.
pad	Pads with dummy disabled media description lines.
answer	Strips disabled media description lines from answers.
offer	Strips disabled media description lines from offers when used with strip. Pad offers with dummy disabled media description lines when used with pad.
all	Strips all disabled media descriptions from offers.
new	Strips new disabled media descriptions from offers.

## Command Default

Pad and do-not-strip are the default behaviors.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to remove disabled media streams in forwarded offers which are new:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-description disabled strip
offer new
```

The following example shows how to remove all disabled media streams from forwarded offers, whether known to the recipient of the offer or not.

```
Router# configure terminal
Router(config)# sbc mySbc
```



```
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-description disabled strip
offer all
```

The following example shows how to remove all disabled media streams from forwarded answers.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-description disabled strip
answer
```

The following example shows how to stop SBC from padding forwarded offers with disabled media streams.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# no caller media-description disabled pad
offer
```

# caller media-type

To configure the media address type settings for a caller on the Cisco Unified Border Element (SP Edition), use the **caller media-type** command in the CAC table entry configuration mode. Use the **no** form of this command to disable the media address type settings for a caller.

```
caller media-type {ipv4 | ipv6 | inherit | both}
```

```
no caller media-type {ipv4 | ipv6 | inherit | both}
```

## Syntax Description

ipv4	Only IPv4 media addresses are supported.
ipv6	Only IPv6 media addresses are supported.
inherit	Inherit the supported media IP address type from earlier CAC policy entries (default).
both	Both IPv4 and IPv6 media addresses are supported.

## Command Default

Inherit is the default behavior.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to remove disabled media streams in forwarded offers which are new:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table mytable
Router(config-sbc-sbe-cacpolicy)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media-type ipv4
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

# caller media bypass

To enable or disable the Multiple SBC Media Bypass feature on the caller side, use the **caller media bypass** command in the CAC table entry configuration mode. To deconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

**caller media bypass {enable | disable}**

**no caller media bypass**

Syntax Description	enable	Enables the Multiple SBC Media Bypass feature on the caller side.
	disable	Disables the Multiple SBC Media Bypass feature on the caller side.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to enable the Multiple SBC Media Bypass feature on the caller side:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller media bypass enable
```

Related Commands	Command	Description
	cac-table	Configures the admission control tables.
	callee media bypass	Enables or disables the Multiple SBC Media Bypass feature on the callee side.
	table-type	Configures a CAC table type to enable the priority of the call to be used as a criterion in the CAC policy.



# caller port-range-tag

To configure the port range tag for a caller that is used when selecting a media address and port, use the **caller port-range-tag** command in the CAC table entry configuration mode. To deconfigure the port range tag, use the **no** form of this command.

```
caller port-range-tag {adj-name | none | string tag-string}
```

```
no caller port-range-tag
```

Syntax Description		
	<i>adj-name</i>	Uses the source adjacency name as a port-range tag.
	<b>none</b>	Prompts the SBC to not use a port range tag for calls matching the CAC entry, and removes any previously found strings.
	string <i>tag-string</i>	Specifies the explicit port range tag string.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to configure a port-range tag:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# match SIPIMSAccess
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller port-range-tag adj-name
```

Related Commands	Command	Description
	<b>media-address-pool</b>	Adds an IPv4 and IPv6 address to the set of addresses that can be used by the DBE as a local media address.



# caller ptime

To configure the packetization time on the caller side, use the **caller ptime** command in the CAC table configuration mode. To deconfigure the packetization time on the caller side, use the **no** form of this command.

```
caller ptime 0-100
```

```
no caller ptime 0-100
```

<b>Syntax Description</b>	<i>0-100</i>	The packetization time in milliseconds (ms).
---------------------------	--------------	--

<b>Command Default</b>	By default, 0 ms is configured. This means that no transrating occurs.
------------------------	--

<b>Command Modes</b>	CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.
-------------------------	---

<b>Examples</b>	The following example shows how to configure the packetization time on the caller side using the <b>caller ptime</b> command in the CAC table configuration mode:
-----------------	---

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# first-cac-table Transrate
Router(config-sbc-sbe-cacpolicy)# cac-table Transrate
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller ptime 30
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	callee ptime	Configures the packetization time on the callee side.





# caller secure-media

To configure granular-level Secure Media on the caller side, use the **caller secure-media** command in CAC table entry configuration mode. To remove granular-level Secure Media, use the **no caller secure-media** command.

**caller secure-media**

**no caller secure-media**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Granular-level (Unsignaled) Secure Media is disabled by default.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Restriction—Both caller and callee sides of the call need to be configured. If only one leg of the call has granular secure media configured, then the call will fail.

We recommend you use Unsignaled (also called granular-level) Secure Media configuration because, instead of turning on Secure Media globally, you can specify the calls and adjacencies where you want to use Secure Media.

**Examples** The following example shows an Unsignaled Secure Media configuration where the two SIP adjacencies for both legs of the call are configured for “security trusted-unencrypted” and both the caller and callee sides are configured for Secure Media in a CAC table entry:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# adjacency sip server
Router(config-sbc-sbe-adj-sip)# security trusted-unencrypted
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table testSecure
Router(config-sbc-sbe-cacpolicy)# cac-table testSecure
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# caller secure-media
Router(config-sbc-sbe-cacpolicy-cactable-entry)# callee secure-media
```

```

Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy)# exit
Router(config-sbc-sbe)# cac-policy-set global 1
Router(config-sbc-sbe)# end

```

The following configuration example shows how to configure Unsignaled Secure Media where an adjacency is *untrusted* by using the **transport srtp allowed** command on the untrusted adjacency in a CAC policy table:

```

...
cac-policy-set 2
  first-cac-table 1
  cac-table 1
    table-type limit all
    entry 1
      match-value call-update
      transport srtp allowed
      caller secure-media
      callee secure-media
      action cac-complete
      exit
    complete
  exit
cac-policy-set global 2

```

The following configuration example shows that SIP adjacencies ‘client’ and ‘server’ are configured as “security trusted-unencrypted” and that CAC table entry 1 is configured for Secure Media on both the caller and callee sides:

```

...
cac-policy-set 2
  first-cac-table 1
  cac-table 1
    table-type policy-set
    entry 1
      action cac-complete
      caller secure-media
      callee secure-media
    complete
cac-policy-set global 2

adjacency sip client
  nat force-off
  security trusted-unencrypted
  signaling-address ipv4 10.10.100.110
  signaling-port 9060
  remote-address ipv4 10.10.100.10 255.255.255.255
  signaling-peer 10.10.100.10
  signaling-peer-port 9060
  attach

adjacency sip server
  nat force-off
  security trusted-unencrypted
  signaling-address ipv4 10.10.100.110
  signaling-port 9070
  remote-address ipv4 10.10.100.10 255.255.255.255
  signaling-peer 10.10.100.10
  signaling-peer-port 9070
  attach

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>callee secure-media</b>	Configures granular-level Secure Media on the callee side.
<b>security</b>	Configures transport-level security (TLS) on a SIP adjacency.

# call-policy-set default

To activate a default policy set within an signaling border element (SBE) entity, use the **call-policy-set default** command in the **SBE** configuration mode. To deactivate a default policy set, use the **no** form of this command.

**call-policy-set default** *policy-set-id* [**priority** *priority-value*]

**no call-policy-set default**

## Syntax Description

<i>policy-set-id</i>	The integer, ranging from 1 to 2147483647, that identifies a default call policy set.
<b>priority</b>	Specifies the priority for the administrative domains that are not configured.
<i>priority-id</i>	The priority value, ranging from 1 to 10, with 10 indicating the highest priority. By default, 6 is the priority value given to the policy set.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It replaces the <b>call-policy-set default</b> command.

## Usage Guidelines

If another policy set was previously active, it is made inactive by executing this command. The SBE is created with no active routing policy set; an active routing policy set must be explicitly configured using this command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to set policy set 1 as the default on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# call-policy-set default 1 priority 9
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Creates a new policy set on the session border controller (SBC).
	<b>first-inbound-na-table</b>	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
	<b>first-outbound-na-table</b>	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
	<b>show sbc sbe call-policy-set</b>	Lists the details of the policy sets configured on the SBC.
	<b>show sbc sbe call-policy-set default</b>	Lists the summary of the default policy set configured on the SBC.

## category (NA-)

To configure the entry category in the number analysis table with entries of the table matching a part of or the whole dialed number, use the **category** command in the NA routing table configuration mode. To deconfigure the category of an entry, use the **no** form of this command.

**category** *category-name*

**no category** *category-name*

### Syntax Description

<i>category-name</i>	Specifies a category to assign to the event.  The <i>category-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  Except for the underscore character, do not use any special character to specify field names.
----------------------	---

### Command Default

No default behavior or values are available.

### Command Modes

NA routing table configuration (config-sbc-sbe-rtgpolicy-natable)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to configure the category of entry 1 in the new number analysis table MyNaTable matching the whole number:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# category external
Router(config-sbc-sbe-rtgpolicy-natable-entry)# exit
Router(config-sbc-sbe-rtgpolicy-natable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
Router(config-sbc-sbe)#
```

# cause

To configure the cause, sub-cause, status-code, and reason of an internal error for an error profile, use the **cause** command in error profile configuration mode. To remove the cause, use the no form of this command.

**cause** *cause* [**sub-cause** *sub-cause*] **status-code** *status-code* [**reason** *reason*]

**no cause** *cause* [**sub-cause** *sub-cause*] **status-code** *status-code* [**reason** *reason*]

## Syntax Description

cause

Cause of the error. For a list of the causes, use the question mark (?) online help function. The following causes are currently available:

- **cac-in-call-msg-rate**—cac: The rate of mid-call messages has exceeded a maximum configured limit
- **cac-max-bandwidth**—cac: The bandwidth used has exceeded a maximum configured limit
- **cac-max-call-rate**—cac: Call setup rate exceeded a maximum configured limit
- **cac-max-channels**—cac: The number of media channels used has exceeded a maximum limit
- **cac-max-num-calls**—cac: The number of calls has exceeded a maximum limit
- **cac-max-reg**—cac: The number of registrations has exceeded a maximum configured limit
- **cac-max-reg-rate**—cac: The rate of registrations has exceeded a maximum configured limit
- **cac-max-updates**—cac: The number of call updates has exceeded the configured limit
- **cac-out-call-msg-rate**—cac: The rate of out of dialogue messages has exceeded a maximum configured limit
- **cac-rtp-disallowed**—cac: Disallowing rtp caused the call to fail
- **cac-srtp-disallowed**—cac: Disallowing srtp caused the call to fail
- **cac-srtp-rtp-interwork**—cac: call failed due to srtp to rtp interworking disallowed
- **enum-failure**—ENUM processing encountered an error
- **max-media-streams**—An offer cannot be reduced to meet the maximum number of media streams
- **mg-srtp-unsupported**—No MG was found which can support srtp
- **na-invalid-address**—na: Number validation failure
- **no-acceptable-codec**—No acceptable codec can be found for an offer
- **rtg-max-routes-tried**—rtg: The maximum number of routing attempts exceeded
- **rtg-no-route-found**—rtg: Routing failed to find a route
- **rtg-route-unavailable**—rtg: The route selected by call-policy is unavailable

- **srtplib-general-error**—srtplib general error
- **sub-media-bearer-chan-fail**—subscriber media bearer channel has failed mid-call
- **sub-media-bearer-chan-rej**—subscriber media bearer channel has rejected during setup or renegotiation
- **sub-sig-bearer-chan-fail**—subscriber signaling bearer channel is unavailable

---

*sub-cause*

(Optional) Sub cause of the error. To see the list of the available sub-causes for a specific cause, use the question mark (?) online help function after you have selected the cause. The following list shows all available sub-causes:

- **na-dst-number**—Destination number based analysis
- **na-src-adjacency**—Source adjacency based analysis
- **na-src-account**—Source account based analysis
- **na-sub-category**—Subscriber category based analysis
- **na-carrier-id**—Carrier identification code based analysis
- **na-src-number**—Source number based analysis
- **na-no-src-number**—No source number present for source number based analysis
- **rtg-src-address**—Source address based routing
- **rtg-dst-address**—Destination address based routing
- **rtg-src-adjacency**—Source adjacency based routing
- **rtg-src-account**—Source account based routing
- **rtg-category**—Category based routing
- **rtg-sub-category**—Subscriber category based routing
- **rtg-src-domain**—Source domain based routing
- **rtg-dst-domain**—Destination domain based routing
- **rtg-time**—Time based routing
- **rtg-dst-tgid**—Destination trunk group Identifier based routing
- **rtg-src-tgid**—Source trunk group identifier based routing
- **rtg-carrier-id**—Carrier identification code based routing
- **rtg-round-robin**—Round robin based routing
- **rtg-least-cost**—Least cost based routing
- **cac-unknown**—Unknown call admission control error
- **cac-per-call-scope**—Call admission control call scope error
- **cac-src-number-scope**—Call admission control source number scope error
- **cac-downstream-scope**—Call admission control downstream scope attribute error
- **cac-upstream-scope**—Call admission control upstream scope attribute error
- **sub-rx-reg-bearer-loss**—Failed to route to a subscriber because the Rx session for the subscriber registration suffered loss of bearer



- **sub-rx-reg-bearer-rel**—Failed to route to a subscriber because the rx session for the subscriber registration suffered release of bearer
- **sub-rx-reg-bearer-term**—Failed to route to a subscriber because the rx session for the subscriber registration was terminated
- **sub-rx-media-policy-rej**—Rx session for a call was rejected for policy reasons (for example, unsupported media)
- **sub-rx-media-error**—Rx session for a call was rejected for non-policy reasons (for example, service unavailable)
- **sub-rx-reg-bearer-loss**—Rx session for a call suffered loss of bearer
- **sub-rx-reg-bearer-rel**—Rx session for a call suffered release of bearer
- **sub-rx-reg-bearer-term**—Rx session for a call was terminated
- **enum-resource**—enum - encountered a resource shortage
- **enum-dst-not-number**—enum - destination address which was not a telephone number
- **enum-unknown-number**—enum - unable to resolve a telephone number
- **enum-interface-failure**—enum - failed in the enum interface
- **enum-regex-error**—enum - failed because a regex in a NAPTR record was invalid

<i>status-code</i>	Maps a SIP status-code to the selected cause/sub-cause. The SIP status-code numbers range from 400 to 699.
<i>reason</i>	(Optional) The reason that the error occurred. The reason allows system administrators to optionally configure a SIP "Reason:" header, which is inserted into the error response and displayed when an error occurs. The configured reason header must conform to the syntax rules defined in RFC 3326.

**Command Default** No default behavior or values are available.

**Command Modes** Error profile configuration (config-sbc-sbe-sip-err)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the cause of an internal error for an error profile:

```

Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip error-profile Error_profile_1
Router(config-sbc-sbe-sip-err)# cause rtg-no-route-found sub-cause rtg-src-adjacency
status-code 604 reason "SBC: No route found based on src adjacency"
Router(config-sbc-sbe-sip-err)#

```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>error-profile</b>	Configures an existing error profile as the outbound SIP error profile.
<b>sip error-profile</b>	Creates an error profile and enters error profile configuration mode.
<b>cause</b>	Configures the cause of an internal error for an error profile.
<b>show sbc sbe sip error-profile</b>	Displays the configuration information of an error profile.

---

# cdr

To add media information or endpoint information of a call to a billing record, use the **cdr** command in SBE billing configuration mode. To disable adding media information or endpoint information to billing records, use the **no** form of this command.

```
cdr {media-info | endpoint-info {addressing | adjacency}}
```

```
no cdr {media-info | endpoint-info {addressing | adjacency}}
```

## Syntax Description

<b>media-info</b>	Adds media information to billing records.
<b>endpoint-info</b>	Adds endpoint information to billing records
<b>addressing</b>	Adds address information and adjacency name to billing records in the format <i>IP address,port,transport type,adjacency name</i> . (For example, <i>2.0.0.36,5078,UDP,SIPPB</i> )
<b>adjacency</b>	Adds adjacency names to billing records.

## Command Default

By default, the media information and the adjacency names are not included in the call details records.

## Command Modes

SBE billing configuration (config-sbc-sbe-billing)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	Call details record CLI with <b>media-info</b> key word was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.6.1	The <b>adj-info</b> keyword was added.
Cisco IOS XE Release 2.6.2	The <b>adj-info</b> keyword was removed. The <b>endpoint-info</b> , <b>addressing</b> , and <b>adjacency</b> keywords were added.

## Usage Guidelines

The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to add media information to a billing record:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# cdr media-info
Router(config-sbc-sbe-billing)# end
```

The following example shows how to include endpoint addressing information to a billing record:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# cdr endpoint-info addressing
Router(config-sbc-sbe-billing)# end
Router#
```

#### Related Commands

Command	Description
<b>billing</b>	Configures billing.
method packetcable-em	Enables the packet-cable billing method.
packetcable-em <i>transport radius</i>	Configures a packet-cable billing instance.
show sbc sbe billing instance	Displays whether media creation information and endpoint information are included in the billing records for a specific billing instance.

## cdr alarm (XML Billing)

To configure the free disk space sizes, which, when exceeded, should generate, different types of alarms, use the **cdr alarm** command in SBE billing XML configuration mode. To disable the configuration of free disk space sizes, use the **no** form of this command.

**cdr alarm** {critical | major | minor} *kilobytes*

**no cdr alarm** [critical | major | minor]

Syntax Description		
	<b>critical</b>	Configures a critical alarm if the free disk space is less than the configured size in kilobytes.
	<b>major</b>	Configures a major alarm if the free disk space is less than the configured size in kilobytes.
	<b>minor</b>	Configures a minor alarm if the free disk space is less than the configured size in kilobytes.
	<i>kilobytes</i>	The free disk space size, which, if exceeded, will trigger a critical, major or minor alarm. The default value for a critical alarm is 100 MB, a major alarm is 500 MB, and a minor alarm is 1 GB.

**Command Default** By default, the free disk space alarm size that is set for a critical alarm is 100 MB, a major alarm is 500 MB, and a minor alarm is 1 GB.

**Command Modes** SBE billing XML configuration (config-sbc-sbe-billing-xml)

Command History	Release	Modification
	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

**Usage Guidelines** To inform the administrator for freeing disk space to store the XML billing records, the CDR alarm feature has been introduced. If there are too many calls, the free disk space available to store the XML billing records might be less. However, even if there is no space on the local machine, the calls will be active, although, because of non availability of disk space, the calls may not be billed.

To avoid such a situation, alarms must be configured using the **cdr alarm** command. Based on the free disk space size configured, minor, major, or critical alarms are generated.

**Examples** The following example shows how to configure a minor alarm for free disk space less than 800 MB:

```
Router(config)# sbc sbcbilling
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# xml method
Router(config-sbc-sbe-billing)# xml 1
Router(config-sbc-sbe-billing-xml)# cdr alarm minor 800
```

The following example shows how to configure a major alarm for free disk space less than 600 MB:

```
Router(config-sbc-sce-billing-xml)# cdr alarm major 600
```

The following example shows how to configure a major alarm for free disk space less than 200 MB:

```
Router(config-sbc-sce-billing-xml)# cdr alarm critical 200
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>xml (billing)</b>	Configures the method index for XML billing.
<b>method xml</b>	Configures the billing method as XML for the Billing Manager.
<b>ldr-check</b>	Configures the time at which long duration records are checked.

# cdr path

To store the CDR XML billing records on the local machine (Cisco ASR 1000 Series Router), use the **cdr path** *path* command in the SBE billing XML configuration mode. To disable the cdr path, use the **no** form of this command.

**cdr path** *path*

**no cdr path**

<b>Syntax Description</b>	<i>path</i>	Indicates the path in which to store the XML billing records locally on the Cisco ASR 1000 Series Router. The maximum length of the path is 128 bytes, and the directory should not be a root directory. The valid options to set CDR path are harddisk:, usb0:, and usb1:.
---------------------------	-------------	---

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	SBE billing XML configuration (config-sbc-sbe-billing-xml)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

<b>Usage Guidelines</b>	To store the XML billing records on the local machine (Cisco ASR 1000 Series Router), set the path using the <b>cdr path</b> <i>path</i> command from the SBE billing XML configuration mode. The maximum length of path is 128 bytes, and the directory should not be a root directory. Moreover, before the path is defined using the <b>cdr path</b> command, ensure that a directory has been created using the <b>mkdir</b> command from Privilege EXEC mode. The valid options to store the XML billing records are: harddisk:, usb0, and usb1:.
-------------------------	--

<b>Examples</b>	The following example shows how to define the path to store the XML billing records on the Cisco ASR 1000 Series Router:
-----------------	--

```
Router(config)# sbc sbcbilling
Router(config-sbc)# sce
Router(config-sbc-sce)# billing
Router(config-sbc-sce-billing)# xml method
Router(config-sbc-sce-billing)# xml 1
Router(config-sbc-sce-billing-xml)# cdr path harddisk:cdrbilling
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>xml (billing)</b>	Configures the method index for XML billing.

<b>Command</b>	<b>Description</b>
<b>method xml</b>	Configures the billing method as XML for the Billing Manager.
<b>ldr-check</b>	Configures the time at which long duration records are checked.



# clear platform hardware qfp active feature sbc sfx

To clear the Cisco QuantumFlow Processor SIP Fast-Register (SFX) counters, use the **clear platform hardware qfp active feature sbc sfx** command in Exec mode.

```
clear platform hardware qfp active feature sbc sfx [global]
```

## Syntax Description

global	Specifies SIP Fast-Register (SFX) global state information.
--------	---

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example clears information about the parsing of SIP fast-register (SFX) messages in the Cisco QuantumFlow Processor (QFP):

```
Router# clear platform hardware qfp active feature sbc sfx global
```

## Related Commands

Command	Description
show platform hardware qfp active feature sbc sfx	Displays information about SFX messages in Cisco QFP.

# clear platform software wccp

To clear Web Cache Communication Protocol version 2 statistics on the Cisco ASR 1000 Series Routers, use the **clear platform software wccp** command in privileged EXEC mode.

```
clear platform software wccp {slot [active | standby] statistics} | {counters | statistics}
```

Syntax Description	slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot.
		Valid options are: <ul style="list-style-type: none"> <li>• <b>F0</b>—Embedded Service Processor slot 0</li> <li>• <b>F1</b>—Embedded Service Processor slot 1</li> <li>• <b>FP</b>—Embedded Service Processor</li> <li>• <b>R0</b>—Route Processor slot 0</li> <li>• <b>R1</b>—Route Processor slot 1</li> <li>• <b>RP</b>—Route Processor</li> </ul>
	<b>active</b>	Clears active instances.
	<b>standby</b>	Clears standby instances.
	<b>statistics</b>	Clears statistics counters.
	<b>counters</b>	Clears packet processing counters.

**Command Default** WCCPv2 statistics are not cleared.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced.

**Examples** The following example shows how to clear WCCPv2 statistics on Embedded-Service-Processor slot 0:

```
Router# clear platform software wccp F0 statistics
```

Related Commands	Command	Description
	<b>clear ip wccp</b>	Removes WCCP statistics (counts) maintained on the router for a particular service.

# clear sbc

To clear a data border element (DBE), redundancy group, or signaling border element (SBE) information, use the **clear sbc** command in Privileged EXEC mode.

```
clear sbc sbc-name {dbe | rg | sbe}
```

Syntax Description		
<i>sbc-name</i>		The name of the Session Border Controller (SBC) service.
<b>dbe</b>		Clears DBE information.
<b>rg</b>		Clears redundancy group statistics. The SBC redundancy group creates and transports establishment.
<b>sbe</b>		Clears SBE information.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	The keyword <b>rg</b> was added to this command.

**Examples** The following example shows how to clear the DBE configuration:

```
Router# clear sbc mySbc dbe
```

## clear sbc dbe media-stats (session border controller)

To clear all the statistics collected by the media gateway manager of the DBE, use the **clear sbc dbe media-stats** command in Exec mode.

```
clear sbc sbc-name dbe media-stats
```

<b>Syntax Description</b>	<i>sbc-name</i>	Name of the SBC service.
---------------------------	-----------------	--------------------------

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for the distributed model.

<b>Usage Guidelines</b>	This command clears the statistics displayed by the <b>show sbc dbe media-stats</b> command.	
-------------------------	--	--

<b>Examples</b>	The following example clears all the statistics collected by the media gateway manager of a DBE on an SBC called mySbc:	
-----------------	---	--

```
Router(config)# clear sbc mySbc dbe media-stats
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc dbe media-stats</b>	Lists the statistics of one or more media flows collected on the DBE.

## clear sbc h248 bac

To clear the information pertaining to the Session Border Controller (SBC) H.248 Border Access Controller-related call context sessions, use the **clear sbc h248 bac** command in the privileged EXEC mode.

```
clear sbc h248 bac {context- sessions [correlator context-correlator] | {iad-sessions [correlator iad-correlator]}}
```

Syntax Description		
<b>context-sessions</b>		Clears the information pertaining to the SBC H.248 Border Access Controller (BAC) call context sessions.
<b>correlator</b>		Clears an SBC H.248 BAC call context session along with the specific context correlator.
<i>context-correlator</i>		Number of the context session correlator. Range: 1 to 4294967295.
<b>iad-sessions</b>		Clears the information pertaining to the SBC H.248 BAC Integrated Access Device (IAD) registry sessions.
<b>correlator</b>		Clears an SBC H.248 BAC IAD session along with the specific IAD correlator.
<i>iad-correlator</i>		Number of the IAD session correlator. Range: 0 to 4294967295.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** There is no **no** form of this command.

**Examples** The following example shows how to clear the information pertaining to the SBC H.248 BAC context sessions:

```
Router> enable
Router# clear sbc h248 bac context-sessions
```

# clear sbc sbe adjacency statistics

To clear the SIP method statistics counters and reset them to zero, use the **clear sbc sbe adjacency statistics** command in Privileged EXEC mode.

```
clear sbc sbc-name sbe adjacency adj-name adjacency
```

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
<i>adj-name</i>	Specifies the name of the adjacency.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command clears request and response counters that are displayed in the output of the **show sbc sbe sip-method-stats** command.

## Examples

The following example clears the SIP method statistics counters for the sipGW adjacency:

```
Router# clear sbc mySbc sbe adjacency sipGW statistics
```

## Related Commands

Command	Description
<b>show sbc sbe sip-method-stats</b>	Displays summary or detailed statistics for a SIP method.
<b>statistics-setting</b>	Configures an adjacency to support SIP method statistics.

# clear sbc sbe blacklist

To clear the blacklist for the specified Session Border Controller (SBC) service, use the **clear sbc sbe blacklist** command in privileged EXEC mode.

```
clear sbc sbc-name sbe blacklist [critical] {WORD}[ipv4 addr [{udp | tcp} port] ]
```

```
clear sbc sbc-name sbe blacklist [critical] {ipv4 addr | ipv6 addr} [{udp | tcp} port]
```

Syntax Description		
<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.	
critical	Allows you to clear critical blacklists.	
<i>WORD</i>	Specifies the VPN ID for which you want to clear critical blacklisting information.	
<b>ipv4</b> <i>addr</i>	Clears configured critical blacklisting for a single IPv4 address.	
tcp	Clear blacklisting for TCP protocol only.	
udp	Clear blacklisting for UDP protocol only.	
<b>ipv6</b> <i>addr</i>	Clears configured blacklisting for a single IPv6 address.	

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.4.2	The <b>critical</b> keyword and <b>critical</b> options were added.
	Cisco IOS XE Release 2.6	The <b>ipv6</b> keyword was added.

**Examples** The following example clears all the blacklists for the TCP port 1 for VRF test for the ipv4 address of 2.2.2.2:

```
Router# clear sbc aa sbe blacklist test ipv4 2.2.2.2 tcp 1
```

Related Commands	Command	Description
	<b>blacklist</b>	Enter the mode for configuring the event limits of a given source.

# clear sbc sbe cac-policy-set-stats

To clear all the call admission control (CAC) policy statistics, use the **clear sbc sbe cac-policy-set-stats** command in the Privileged EXEC mode.

```
clear sbc sbc-name sbe cac-policy-set-stats [all | policy-set cac-policy-number]
```

Syntax Description	Parameter	Description
	<b>sbc-name</b>	Name of the SBC service.
	<b>all</b>	Clears all the CAC policy set statistics.
	<b>policy-set</b>	Clears the CAC statistics pertaining to the specified policy set number.
	<i>cac-policy-number</i>	CAC policy set number that can range from 1 to 2147483647.

**Command Default** By default, the **all** keyword is used.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.3S	This command was modified. The <b>all</b> and <b>policy-set</b> keywords and the <i>cac-policy-number</i> argument were added.

**Examples** The following example shows how to clear all the CAC policy statistics in SBC global:

```
Router# clear sbc global sbe cac-policy-set-stats
```

The following example shows how to clear the CAC policy statistics for the CAC policy set number 21:

```
Router# clear sbc global sbe cac-policy-set-stats policy-set 21
```



## clear sbc sbe cac-rejection-stats

To clear all the call admission control policy rejection statistics, use the **clear sbc sbe cac-rejection-stats** command in privileged EXEC mode.

*clear sbc sbc-name sbe cac-rejection-stats*

<b>Syntax Description</b>	sbc-name	Name of the Session Border Controller (SBC) service.
---------------------------	----------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Examples</b>	The following example clears all the call admission control policy rejection statistics for the SBE mysbc: Router# <b>clear sbc mySbc sbe cac-rejection-stats</b>
-----------------	--

# clear sbc sbe call-policy-set-stats

To clear call policy set statistics, use the **clear sbc sbe call-policy-set-stats** command in privileged EXEC mode.

```
clear sbc sbc-name sbe call-policy-set-stats [all | na | rtg]
```

## Syntax Description

<b>sbc-name</b>	Specifies the name of the SBC service.
<b>all</b>	Clears all policy routing rejection statistics.
<b>na</b>	Clears all policy number analysis rejection statistics.
<b>rtg</b>	Clears call policy routing rejection statistics.

## Command Default

By default, clears **all** policy routing rejection statistics.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following examples shows how to clear policy number analysis rejection statistics in sbc “global”:

```
Router# clear sbc global sbe call-policy-stats na
```

## clear sbc sbe call-rate-stats

To clear all the call rate statistics, use the **clear sbc sbe call-rate-stats** command in privileged EXEC mode.

*clear sbc sbc-name sbe call-rate-stats*

<b>Syntax Description</b>	sbc-name	Name of the Session Border Controller (SBC) service.
---------------------------	----------	--

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example clears all the call rate statistics for the SBE mysbc:

```
Router# clear sbc mySbc sbe call-rate-stats
```

## clear sbc sbe call-rejection-stats

To clear all the call admission control policy rejection statistics, use the **clear sbc sbe call-rejection-stats** command in privileged EXEC mode.

*clear sbc sbc-name sbe call-rejection-stats*

<b>Syntax Description</b>	sbc-name	Name of the Session Border Controller (SBC) service.
---------------------------	----------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Examples</b>	<p>The following example clears all the call admission control policy rejection statistics for the SBE mysbc:</p> <pre>Router# clear sbc mySbc sbe call-rejection-stats</pre>
-----------------	---

# clear sbc sbe call-stats

To clear the call statistics on the SBE, use the **clear sbc sbe call-stats** command in the privileged EXEC mode.

```
clear sbc sbc-name sbe call-stats [all | dst-account account-name | dst-adjacency adjacency-name
| global | src-account account-name | src-adjacency adjacency-name | per-adjacency
adjacency-name] [all | current-indefinite]
```

```
clear sbc sbc-name sbe call-stats reject-threshold memory
```

Syntax Description		
	<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
	<i>account-name</i>	Name of the source or destination account.
	<i>adjacency-name</i>	Name of the source or destination adjacency.
	<b>all</b>	Clears all the call statistics.
	<b>dst-account</b>	Clears the statistics pertaining to a destination account.
	<b>dst-adjacency</b>	Clears the statistics pertaining to a destination adjacency.
	<b>global</b>	Clears the global call statistics.
	<b>per-adjacency</b>	Clears the statistics pertaining to a per adjacency. <ul style="list-style-type: none"> <li><b>all</b>—Clears the statistics for all the summary periods.</li> <li><b>current-indefinite</b>—Clears the statistics for only the current indefinite period.</li> </ul>
	<b>reject-threshold</b>	Clears the statistics related to reject threshold.
	<i>memory</i>	Clears the statistics related to call denials because of low memory.
	<b>src-account</b>	Clears the statistics pertaining to a source account.
	<b>src-adjacency</b>	Clear the statistics pertaining to a source adjacency.

**Command Default** By default, the **all** keyword is used.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.3S	This command was modified. The <b>per-adjacency</b> keyword and the <i>currentindefinite</i> parameter were added to the command.

**Examples** The following example shows how to clear all the call statistics pertaining to the mysbc SBE:

```
Router# clear sbc mysbc sbe call-stats
```

The following example shows how to clear the call statistics pertaining to the current indefinite period for the mysbc SBC:

```
Router# clear sbc mysbc sbe call-stats global current-indefinite
```

# clear sbc sbe call

To clear an identified call, use the **clear sbc sbe call** command in privileged EXEC mode.

```
clear sbc sbc-name sbe call {0-2147483647}
```

Syntax Description	Parameter	Description
	<b>sbc-name</b>	Specifies the name of the SBC service.
	<i>0-2147483647</i>	Specifies the call index number that is to be cleared.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following examples shows how to display calls on the global SBC service; how to clear specified call number 1; and how to show that call number 1 has been cleared:

```
Router# show sbc global sbe calls

SBC Service "global"
  Call      State      Type      Src Adjacency      Dest Adjacency
  -----
   1        Active     Audio     glophone           registrar

Router#
Router#
Router# clear sbc global sbe call 1
Router#

Router# show sbc global sbe calls

SBC Service "global"
  Call      State      Type      Src Adjacency      Dest Adjacency
  -----
No call information found.

Router#
```

# clear sbc sbe policy-failure-stats

To clear all the policy failure statistics of all adjacencies and accounts, use the **clear sbc sbe policy-failure-stats** command in privileged EXEC mode.

```
clear sbc sbc-name sbe policy-failure-stats [src-adjacency | src-account | dst-adjacency |
dst-sccount] name
```

## Syntax Description

<i>sbc-name</i>	Specifies the name of the Session Border Controller (SBC) service.
<i>src-adjacency</i>	(Optional) Clears statistic for a source adjacency.
<i>src-account</i>	(Optional) Clears statistic for a source account.
<i>dst-adjacency</i>	(Optional) Clears statistic for a destination adjacency.
<i>dst-account</i>	(Optional) Clears statistic for a destination account.
<i>name</i>	Specifies the adjacency name or the account name.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to clear all of the policy failure statistics for an adjacency named YY:

```
Router# clear sbc mysbc sbe policy-failure-stats src-adjacency YY
```



# clear sbc sbe policy-rejection-stats

To clear all the policy rejection statistics by the SBE, use the **clear sbc sbe policy-rejection-stats** command in privileged EXEC mode.

*clear sbc sbc-name sbe policy-rejection-stats*

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the Session Border Controller (SBC) service.
---------------------------	-----------------	--

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This clears all recorded policy rejection stats including the current and previous intervals.

**Examples** The following example clears all the policy rejection statistics by the SBE.

```
Router# clear sbc mySbc sbe policy-rejection-stats
```

# clear sbc sbe radius-client-stats

To clear all the statistics for the local RADIUS clients, use the **clear sbc sbe radius-client-stats** command in privileged EXEC mode.

```
clear sbc sbc-name sbe radius-client-stats {accounting word | authentication}
```

Syntax Description		
	<i>sbc-name</i>	Specifies the name of the Session Border Controller (SBC) service.
	<i>word</i>	The RADIUS client name. The maximum size is 80 characters.
	<i>accounting</i>	Clears accounting client statistics.
	<i>authentication</i>	Clears authentication client statistics.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example clears all the authentication statistics:

```
Router# clear sbc mySbc sbe radius-client-stats authentication
```

The following example clears all the accounting statistics for the local RADIUS client, radius1:

```
Router# clear sbc mySbc sbe radius-client-stats accounting radius1
```

# clear sbc sbe radius-client

To clear all the statistics for the specified RADIUS server, use the **clear sbc sbe radius-client** command in privileged EXEC mode.

```
clear sbc sbc-name sbe radius-client {accounting word | authentication | radius-server-stats word}
```

Syntax Description		
<i>sbc-name</i>		Specifies the name of the Session Border Controller (SBC) service.
<i>accounting</i>		Clears accounting client statistics.
<i>authentication</i>		Clears authentication client statistics.
<i>radius-server-stats</i>		Identifies the RADIUS server name.
<i>word</i>		For <b>accounting</b> , the RADIUS client name. The maximum size is 80 characters.  For <b>radius-server-stats</b> , the RADIUS server name. The maximum size is 80 characters.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example clears all the authentication statistics for the RADIUS server called svr:

```
Router# clear sbc mySbc sbe radius-client authentication radius-server-stats svr
```

The following example clears all the accounting client statistics for the local RADIUS client, acc, for the RADIUS server svr:

```
Router# clear sbc mySbc sbe radius-client accounting acc radius-server-stats svr
```

# clear sbc sbe script-set-stats

To clear the stored statistics related to a script set, use the **clear sbc sbe script-set-stats** command in the privileged EXEC mode.

```
clear sbc sbc-name sbe script-set-stats script-set-number [editors-stats editor-name]
```

## Syntax Description

<i>sbc-name</i>	Name of the SBC.
<i>script-set-number</i>	Script set number. The range is from 1 to 2147483647.
<b>editor-stats</b>	Specifies that the script-set statistics must be cleared for a specific editor.
<i>editor-name</i>	Name of the editor.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

These statistics cleared by this command are the same as those displayed when you run the **show sbc sbe script-set** command.

## Examples

In the following example, the **clear sbc sbe script-set-stats** command is used to clear stored statistics related to script set 10.

```
Router# clear sbc mySbc sbe script-set-stats 10
```

## Related Commands

Command	Description
<b>active-script-set</b>	Activates a script set,
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
<b>editor</b>	Specifies the order in which a particular editor must be applied.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.

<b>Command</b>	<b>Description</b>
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# clear sbc sbe sip statistics

To clear aggregated SIP statistics handled by the Cisco Unified Border Element (SP Edition) process on the Cisco ASR 1000 Series Routers, use the **clear sbc sbe sip statistics** command in Privileged EXEC mode.

```
clear sbc service-name sbe {sip statistics [global | adjacency adj-name method] blacklist |
cac-policy-set-stats | call-policy-set-stats [all | na | rtg] call-stats {global | all | src-account
name | dst-account name | src-adjacency name | dst-adjacency name} | radius-client |
radius-client-stats }
```

## Syntax Description

<i>service-name</i>	Name of the Session Border Controller (SBC) service.
<i>adj-name</i>	Name of the adjacency.
<i>name</i>	Name of the account for which you would like to display statistics. The maximum length of this value is 30 characters.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	Added new parameters to the command.

## Usage Guidelines

This command resets to zero all the packet counters of SIP statistics aggregated by the SBC.

## Examples

The following example resets to zero the packet counters of SIP statistics aggregated by the Cisco Unified Border Element (SP Edition) process on the Cisco ASR 1000 Series Routers:

```
Router# clear sbc global sbe sip statistics
```

## Related Commands

Command	Description
<b>show sbc sbe sip statistics</b>	Displays the aggregated SIP statistics handled by the Cisco Unified Border Element (SP Edition).

# clear sbc sbe sip subscriber aor

To clear the stuck registrations, use the **clear sbc sbe sip subscriber aor** command in privileged EXEC mode.

```
clear sbc sbc-name sbe sip subscriber aor address-of-record
```

## Syntax Description

<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
<i>address-of-record</i>	Subscriber's Address of Record.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	The command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must know the corresponding subscriber's Address of Record (AOR). The **show sbc sbe sip subscribers** command displays the details of all the Session Initiation Protocol (SIP) endpoints that have been registered with the SBC, including the AOR for each subscriber.

## Examples

The following example shows how the **clear sbc sbe sip subscriber aor** command is used to clear the stuck registrations in the privileged EXEC mode:

```
Router# clear sbc asr sbe sip subscriber aor sip:alice@open-ims.test
```

## Related Commands

Command	Description
<b>show sbc sbe sip subscribers</b>	Displays the details of all the SIP endpoints that have been registered with the SBC.

# clear sbc sbe statistics

To clear the summary statistics and the detailed response code statistics, use the **clear sbc sbe statistics** command in privileged EXEC mode.

*clear sbc sbc-name sbe adj-name statistics*

Syntax Description	
<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
<i>adj-name</i>	Name of the RADIUS client. The maximum size is 80 characters.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example clears all summary statistics and the detailed response code statistics:

```
Router# clear sbc mySbc sbe ttt statistics
```



# clear sbc sbe transcoding-stats

To clear the transcoding-related statistics, use the **clear sbc sbe transcoding-stats** command in the Privileged EXEC mode.

```
clear sbc sbc-name sbe transcoding-stats [adjacency adjacency-name | global] [all | currentindefinite]
```

Syntax Description		
	<i>sbc-name</i>	Name of the SBC service.
	<b>adjacency</b>	Clears the statistics pertaining to the specified adjacency.
	<i>adjacency-name</i>	Name of the specified adjacency.
	<b>global</b>	Clears the transcoding-related statistics globally.
	<b>all</b>	Clears statistics pertaining to all the summary periods.
	<b>currentindefinite</b>	Clears statistics pertaining to only the current indefinite period.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode.

**Examples** The following example shows how to clear the voice transcoding-related statistics pertaining to the SIPPI adjacency for the current indefinite period:

```
Router# clear sbc mySBC sbe transcoding-stats adjacency SIPPI currentindefinite
```

Related Commands	Command	Description
	<b>show sbc sbe transcoding-stats</b>	Displays the voice transcoding-related statistics.

# codec-list description

To provide a description of a codec list, use the **codec-list description** command in codec list configuration mode. To delete the description for the codec list, use the **no** form of this command.

**codec-list description** *text*

**no description**

## Syntax Description

<i>text</i>	An arbitrary text string that describes the codec list. The <i>text</i> field can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------	---

## Command Default

No default behavior or values are available.

## Command Modes

Codec list (sbc-codec-list)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to provide the my\_codecs codec list with a description (Legitimate codecs):

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
Router(config-sbc-sbe-codec-list)# codec-list description Legitimate codecs
```

# codec-preference-list

To configure the CAC to add preference to a codec list, use the **codec-preference-list** command in CAC table entry configuration mode. To remove the preference on the codeclist, use the **no** form of this command.

**codec-preference-list** *list-name*

**no codec-preference-list** *list-name*

## Syntax Description

<i>list-name</i>	Specifies the name of the codec list.
------------------	---------------------------------------

## Command Default

Default codec preference priority is 100.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Not setting this command, or issuing the **no** form of the command, means that the CAC entry does not impose any restriction on the codecs that can be used (but also it does not lift any restrictions set by entries encountered earlier).

## Examples

The following command configures the entry to restrict codecs to those named on the list my\_codecs:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table Mycactable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# codec-preference-list my_codecs
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

# codec-restrict-to-list

To configure the CAC to restrict the codecs used in signaling a call to the set of codecs given in the named list, use the **codec-restrict-to-list** command in CAC table entry configuration mode. To impose no restrictions on the codecs that can be used with the CAC entry, use the **no** form of this command.

**codec-restrict-to-list** *list-name*

**no codec-restrict-to-list** *list-name*

## Syntax Description

*list-name* Specifies the name of the codec list.

## Command Default

Not setting this command, or issuing the **no** form of the command, means that the CAC entry does not impose any restriction on the codecs that can be used (but also it does not lift any restrictions set by entries encountered earlier).

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

For each codec on this list, CAC restricts the packetization period for any stream using that codec to be greater than or equal to the packetization period configured along with that codec in the list. If a stream uses more than one codec in the list, the greater of all the packetization periods configured for each codec in the list is applied to the stream.

If the codec list is empty, all codecs recognized by the SBE will be allowed.

To clear all restrictions set by an earlier CAC entry, you must configure a **codec-restrict-to-list** *list-name*, where *list-name* is the name of a list containing no codecs.

You are not allowed to use this command if the table is part of the active policy set. You can only configure the **codec-restrict-to-list** command at per-call scope. If it is configured at any other scope, an error will be flagged when you type “complete” in the CAC policy set configuration.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command configures the entry to restrict codecs to those named on the list my\_codecs:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table Mycactable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
```

```
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable)# cac-scope dst-adjacency
Router(config-sbc-sbe-cacpolicy-cactable-entry)# codec-restrict-to-list my_codecs
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

# codec

To add a codec to a codec list, use the **codec** command in the Codec list configuration mode. To remove a named codec from a codec list, use the **no** form of this command.

**codec** *codec-name*

**no codec** *codec-name*

## Syntax Description

<i>codec-name</i>	Name of a codec. This value must be one of the list of codecs that the SBE is hard-coded to recognize. Otherwise, when you execute this command, the SBE displays an error.  The format of the codec name is the same as the string used to represent it in Session Description Protocol (SDP). For example, PCMU or VDVI. A codec can only be added to each list one time.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

Codec list (sbe-codec-list)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to assign the PCMU codec to the my\_codecs codec list:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
Router(config-sbc-sbe-codec-list)# codec PCMU
```

# codecs

To configure the codecs supported by the media gateway, use the **codecs** command in media gateway configuration mode. To set the codec support to nothing, use the **no** form of this command.

**codecs** *codec-list*

**no** **codecs**

Syntax Description	<i>codec-list</i>	Specifies the supported codecs.
--------------------	-------------------	---------------------------------

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	Media gateway configuration (config-sbc-sbe-mg)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to set media gateway 10.0.0.1's supported codecs to <i>m=audio 6000 RTP/AVP 4</i> and <i>a=rtpmap:0 PCMU/8000</i> (as defined in RFC 1890):
----------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway ipv4 10.0.0.1
Router(config-sbc-sbe-mg)# codecs m=audio 1234 RTP/AVP 0 18,a=rtpmap:=rtpmap:18 G729/80000
PCMU/8000,a=rtpmap:18 G729/8000
```

# codec custom

To configure or modify an existing hard coded codec, use the **codec custom** command in the config sbc sbe configuration mode. To delete a new codec or to restore a custom codec, use the **no** form of this command.

*codec custom custom-name id payload id*

*no codec custom custom-name id payload id*

## Syntax Description

<i>custom-name</i>	Unique name for the custom codec. This name is case insensitive and can contain a maximum of 30 characters.
<i>payload id</i>	Static payload id. The range is from 0 to 96.

## Command Default

No default value.

## Command Modes

Configure SBC SBE (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The following table contains details of the modes:

Mode	Values	Default Value
media	AUDIO, VIDEO, APPLICATION, DATA, CONTROL, IMAGE, OMIT, TEL-EVENT	AUDIO
rate (in Hz)	1-2147483647	8000
packet-time	1-65535	10
bandwidth	1-9223372036854775807	64000
sample-size	0-255	8
channels	0-255	1
max-frames-per-packet	0-65535	1
options	none, transrate, transcode	none
codec-type	fixed, sampling, format, variable, redundancy	N/A, mandatory

The Examples section shows the hierarchy of modes required to run the command.



---

**Examples**

The following example shows how to define a custom codec from a codec hardcoded in SBC:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec custom G726-40-4 id 4
Router(config-sbc-sbe-codec-def)# rate 64000
Router(config-sbc-sbe-codec-def)# packet time 100
Router(config-sbc-sbe-codec-def)# bandwidth 128000
Router(config-sbc-sbe-codec-def)# sample size 4
Router(config-sbc-sbe-codec-def)# channels 16
Router(config-sbc-sbe-codec-def)# max-frames-per-packet 12
Router(config-sbc-sbe-codec-def)# media video
Router(config-sbc-sbe-codec-def)# options transcode
Router(config-sbc-sbe-codec-def)# type sampling
```

# codec list

To create a codec list, use the **codec list** command in the signaling border element (SBE) configuration mode. To delete a codec list, use the **no** form of this command.

**codec list** *list-name*

**no codec list** *list-name*

## Syntax Description

<i>list-name</i>	The name of the codec list.  The <i>list-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  Except for the underscore character, do not use any special character to specify field names.
------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to enter a mode to create a codec list using the name my\_codecs:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
```

## Related Commands

Command	Description
<b>codec</b>	Sets a minimum packetization period for a codec.
<b>packetization-period</b>	
<b>policy</b>	Configures the packetization period policy.

# codec packetization-period

To set a minimum packetization period for a codec, use the **codec packetization-period** command in the codec list configuration mode. To remove a packetization period from a codec, use the **no** form of this command.

**codec** *codec-name* **packetization-period** *packet-period* [**priority** *priority-value*]

**no codec** *codec-name* **packetization-period** *packet-period* [**priority** *priority-value*]

## Syntax Description

<i>codec-name</i>	The name of a codec. This value must be taken from the list of codecs that the signaling border element (SBE) is hard-coded to recognize. Otherwise, when you execute this command, the SBE displays an error.  The format of the codec name is the same as the string used to represent it in Session Description Protocol (SDP), for example, PCMU, or VDVI.
<i>packet-period</i>	The minimum acceptable packetization period in milliseconds as indicated by <b>packetization-period</b> .  For example, <b>codec PCMU packetization-period 20</b> adds the codec PCMU to the list with a minimum acceptable packetization period of 20 ms. The range of packetization period is 0 to 1000.
<b>priority</b>	Specifies the priority used for reordering purposes.
<i>priority-value</i>	The value of the priority.



## Note

For each minimum packetization period, only one codec can be added to each list once.

## Command Default

No default behavior or values are available.

## Command Modes

Codec list (sbe-codec-list)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	The <b>priority</b> keyword and the <i>priority-value</i> argument were added to the command.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples**

The following example shows how to set a minimum packetization period for the PCMU and G729 codecs that are in the my\_codecs codec list. It also shows how to set the priority for the G729 codec:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list my_codecs
Router(config-sbc-sbe-codec-list)# codec PCMU packetization-period 20
Router(config-sbc-sbe-codec-list)# codec G729 packetization-period 10 priority 2
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>codec list</b>	Creates a codec list.
<b>policy</b>	Configures the packetization period policy.

# codec system

To modify a codec, use the **codec system** command in the configure sbc sbe mode.

*codec system sys-codec id payload id*

Syntax Description	sys-codec	Codec included in the SBC.
	id payload id	Static payload id. Value can be from 0 to 96.

**Command Default** No default value.

**Command Modes** Configure SBC SBE (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The following table contains details of the modes:

Mode	Values	Default Value
media	AUDIO, VIDEO, APPLICATION, DATA, CONTROL, IMAGE, OMIT, TEL-EVENT	AUDIO
rate (in Hz)	1-2147483647	8000
packet-time	1-65535	10
bandwidth	1-9223372036854775807	64000
sample-size	0-255	8
channels	0-255	1
max-frames-per-packet	0-65535	1
options	none, transrate, transcode	none
codec-type	fixed, sampling, format, variable, redundancy	N/A, mandatory

The Examples section shows the hierarchy of modes required to run the command.

---

**Examples**

The following example removes the rate configured on G726-40 codec:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system G726-40
Router(config-sbc-sbe-codec)# no clock rate
```

# codec variant

To configure the codec variants and the codec variant profiles, use the **codec variant** command in the Signaling border element (SBE) configuration mode. To remove the codec variants and the codec variant profiles, use the **no** form of this command.

```
codec variant { codec variant-name | profile profile-name }
```

```
no codec variant { codec variant-name | profile profile-name }
```

## Syntax Description

<b>codec</b>	Enters the codec variant mode to configure, modify, or delete a codec variant.
<i>variant-name</i>	The codec variant name.
<b>profile</b>	Enters the Codec variant profile mode to configure a codec variant profile.
<i>profile-name</i>	The codec profile name.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to enter the Codec variant mode to configure, modify, and delete a codec variant:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant codec G723-H-1
Router(config-sbc-sbe-codec-var-codec)#
```

The following example shows how to enter the Codec variant profile mode to configure the codec variant profile:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant profile profile-1
Router(config-sbc-sbe-codec-var-prof)#
```

# concurrent-requests

To set the maximum number of concurrent requests to the RADIUS server, use the **concurrent-request** command in the appropriate configuration mode. To set the default, use the **no** form of this command.

**concurrent-requests 0-4000**

**no concurrent-requests 0-4000**

<b>Syntax Description</b>	<b>0-4000</b>	Maximum number of concurrent requests to the RADIUS server. The range is from 0 to 4000. The default value is 250.
---------------------------	---------------	--

<b>Command Default</b>	Default value is 250.
------------------------	-----------------------

<b>Command Modes</b>	Server accounting (config-sbc-sbe-acc)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to set the maximum number of concurrent requests to the RADIUS server.
-----------------	--

```
Router# configure terminal
Router(config)# sbc uut105-1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting SBC1-account-1
Router(config-sbc-sbe-acc)# concurrent-requests 34
```

<b>Related Commands</b>	<b>retry-interval</b>	Sets the retry interval to connect to the RADIUS server.
	<b>retry-limit</b>	Sets the retry interval to the RADIUS server.
	<b>activate</b>	Activates the RADIUS client.



## condition (editor)

To specify a condition to match before taking an action on a SIP message editor, use the **condition** command in the SIP Header Editor header action configuration mode. To remove a condition from the editor, use the **no condition** form of this command.

**condition** [*comparison-type* | *boolean-operator* | *operator* | *comparison-value*]

**no condition** [*comparison-type* | *boolean-operator* | *operator* | *comparison-value*]

### Syntax Description

<i>comparison-type</i>	The supported comparison types are: <ul style="list-style-type: none"> <li>status-code—Response code value</li> <li>header-value—Current header content</li> <li>header-name <i>name</i> header-value—Content of a different header</li> <li>variable—Match on variable content</li> <li>adjacency—Match on adjacency settings</li> <li>header-uri—Match on parts of the URI (username)</li> <li>request-uri—Match on parts of the request URI (username)</li> <li><i>word</i>—Match on static strings</li> <li>src-address—Match the source address</li> <li>dst-address—Match the destination address</li> </ul>
<i>boolean-operator</i>	The supported boolean operators are: <ul style="list-style-type: none"> <li>is-sip-uri—Does the header contain a sip: URI</li> <li>is-tel-uri—Does the header contain a tel: URI</li> <li>is-request—Is the message a request</li> <li>is-100rel-required—Is the call performing 100rel</li> <li>is-defined—Test if a variable is defined</li> <li>is-private—Has privacy been invoked by the CAC policy: True</li> </ul>
<i>operator</i>	The supported operators are: <ul style="list-style-type: none"> <li>[not] eq—Equals or not equal</li> <li>[not] contains—Contains or does not contain</li> <li>[not] regex-match—Regular expression matching (BRE)</li> <li>store-as—Store rules only</li> <li>and—Logical AND to add another condition to an existing condition</li> <li>or—Logical OR to add another condition to an existing condition</li> </ul>
<i>comparison-value</i>	Specifies a character string or numeric value to compare.

### Command Default

No default behavior or values are available.

**Command Modes** SIP Header Editor header action configuration (config-sbc-sbe-mep-hdr-ele-act)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how the **header** command adds the *test* header to the *Myeditor* header editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Myeditor
Router(config-sbc-sbe-sip-hdr)# header test
Router(config-sbc-sbe-sip-hdr-ele)# action drop-msg
Router(config-sbc-sbe-sip-hdr-ele-act)# condition header-value contains "Cisco"
Router(config-sbc-sbe-sip-hdr-ele-act)# condition is-request eq true
```

Related Commands	Command	Description
	dst-address	Enables you to enter the Destination address configuration mode to create a list of prioritized headers to derive a destination address.
	src-address	Enables you to enter the Source address configuration mode to create a list of prioritized headers to derive a source address.

## condition (session border controller)

To specify a condition to match before taking an action on a SIP message profile, use the **condition** command in SIP header-profile configuration mode. To remove the condition from the profile, use the **no** form of this command.

**condition** [*comparison-type* | *boolean-operator* | *operator* | *comparison-value*]

**no condition** [*comparison-type* | *boolean-operator* | *operator* | *comparison-value*]

### Syntax Description

*comparison-type*

The supported comparison types are:

- status-code—Response code value
- header-value—Current header content
- header-name *name* header-value—Content of a different header
- variables—Match on variable content
- adjacency—Match on adjacency settings
- transport—Match on transport addresses or ports
- header-uri—Match on parts of the URI (username)
- request-uri—Match on parts of the request-URI (username)
- *word*—Match on static strings
- src-address—Match the source address
- dst-address—Match the destination address

*boolean-operator*

The supported boolean operators are:

- is-sip-uri—Does the header contain a sip: URI
- is-tel-uri—Does the header contain a tel: URI
- is-request—Is the message a request
- is-100rel-required—Is the call performing 100rel
- is-defined—Test if a variable is defined

*operator*

The supported operators are:

- [not] eq—Equals or not equal
- [not] contains—Contains or does not contain
- [not] regex-match—Regular expression matching (BRE)
- store-as—Store-rules only

*comparison-value*

Specifies any character string or numeric value to compare.

### Command Default

No default behavior or values are available.

### Command Modes

SIP header configuration (config-sbc-sbe-sip-hdr-ele-act)

**Command History**

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	The comparison types, boolean operators, and operators comparison types were added.
Cisco IOS XE Release 3.1S	The dst-address and src-address comparison types were added.

**Usage Guidelines**

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of modes required to run the command.

**Examples**

The following example shows how the **header** command adds the *test* header to the *Myprofile* header profile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile Myprofile
Router(config-sbc-sbe-sip-hdr)# header test
Router(config-sbc-sbe-sip-hdr-ele)# action drop-msg
Router(config-sbc-sbe-sip-hdr-ele-act)# condition condition header-value contains "Cisco"
Router(config-sbc-sbe-sip-hdr-ele-act)# condition is-request eq true
```

**Related Commands**

Command	Description
<b>action drop-msg</b>	Adds an action of dropping a message to a SIP message profile.
dst-address	Enables you to enter the destination address configuration mode to create a list of prioritized headers to derive the destination address.
src-address	Enables you to enter the source address configuration mode to create a list of prioritized headers to derive the source address.

# congestion-cleared

To configure that the congestion has cleared when the level of system resources reaches the congestion cleared threshold, use the **congestion-cleared** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

**congestion-cleared** [*percentage*]

**no congestion-cleared** [*percentage*]

<b>Syntax Description</b>	<i>percentage</i> (Optional) This is the percentage value of system resources to signal congestion to the SBE. The range is from 1 to 100.
---------------------------	--

<b>Command Default</b>	The system default percentage is 60 if you do not configure the <b>congestion-cleared</b> command or if you configure <b>no congestion-cleared</b> .
------------------------	--

<b>Command Modes</b>	VDBE configuration (config-sbc-dbe-vdbe)
----------------------	--

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.1</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for the distributed model.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for the distributed model.
Release	Modification				
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for the distributed model.				

<b>Usage Guidelines</b>	When the data border element (DBE) has previously signaled a congestion event to the signaling border element (SBE), the DBE will signal that the congestion has cleared when the level of system resources used reaches the congestion cleared threshold. Congestion cleared must be less than or equal to the threshold, however, equal to the threshold is not recommended because it may cause excessive messaging between the MG and media gateway controller (MGC).
-------------------------	---

<b>Examples</b>	The following example creates a DBE service on a session border controller (SBC) called mySbc and configures the DBE to signal to the SBE that congestion has cleared at 90% percent of system resources consumed:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# congestion-cleared 90
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>congestion-threshold</td> <td>Configures the DBE to signal a congestion event to the SBE when a maximum percentage has been reached.</td> </tr> </tbody> </table>	Command	Description	congestion-threshold	Configures the DBE to signal a congestion event to the SBE when a maximum percentage has been reached.
Command	Description				
congestion-threshold	Configures the DBE to signal a congestion event to the SBE when a maximum percentage has been reached.				

# congestion-threshold

To configure the DBE to signal a congestion event to the SBE when a maximum percentage has been reached, use the **congestion-threshold** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

**congestion-threshold** [*percentage*]

**no congestion-threshold** [*percentage*]

## Syntax Description

*percentage* (Optional) This is the percentage value of system resources to signal congestion to the SBE. The range is from 1 to 100.

## Command Default

The system default percentage is 80 if you do not configure the congestion-threshold, or if you issue the default **congestion-threshold** command, or if you configure **no congestion-threshold**.

## Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

When the DBE reaches the maximum configured congestion-threshold percentage for either number of calls or media bandwidth, it sends a congestion message to the SBE.

## Examples

The following example creates a DBE service on an SBC called mySbc, enters into SBC-DBE configuration and VDBE configuration modes, and shows how to configure the DBE to signal a congestion event to the SBE when 95% percent of capacity is reached.

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# congestion-threshold 95
```

## Related Commands

Command	Description
congestion-cleared	Configures that the congestion has cleared when the level of system resources reaches the congestion cleared threshold.

# congestion sip reject-code

To change the reject message code for signaling congestion handling, use the **congestion sip reject-code** command in the SBE configuration mode.

**congestion sip reject-code** *valid-reject-code*

<b>Syntax Description</b>	<i>valid-reject-code</i> The reject message code sent back to sender during congestion. Range is from 300 to 999.
---------------------------	---

<b>Command Default</b>	Signaling congestion handling is on by default. The default reject message code is 503.
------------------------	---

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to change the reject message code for signaling congestion handling:
-----------------	--

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# congestion sip reject-code 600
Router(config-sbc-sbe)#
```

# control-address h248 ipv4

To configure a DBE to use a specific IPv4 H.248 control address, use the **control-address h248 ipv4** command in VDBE configuration mode. To deconfigure a DBE from using an IPv4 H.248 control address, use the **no** form of this command.

```
control-address h248 ipv4 {A.B.C.D}
```

```
no control-address h248 ipv4 {A.B.C.D}
```

## Syntax Description

*A.B.C.D* This is the IP address for the IPv4 H.248 control address of the DBE, which is the local IP address used to connect to the SBE.

## Command Default

No default behavior or values are available.

## Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Neither the control-address nor the local-port can be changed when the controller exists. The controller must be deleted to change these parameters. To delete the controller, use the **no control-address h248 ipv4** command.

## Examples

The following command configures the DBE to use address 10.0.0.1 as its control address.

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# control address h248 ipv4 10.0.0.1
Router(config-sbc-sbe-vdbe)# controller h248 1
```

## Related Commands

Command	Description
attach-controllers	Configures a DBE to attach to an H.248 controller.



## control-address ipv4

To configure a local IPv4 H.248 signaling address for the Border Access Controller (BAC), use the **control-address ipv4** command in the H248 BAC adjacency configuration mode. To unconfigure the BAC from using a local IPv4 H.248 signaling address, use the **no** form of this command.

```
control-address ipv4 ipv4-address {port port-number}
```

```
control-address ipv4 ipv4-address {port-range minimum-port number maximum-port number}
```

```
no control-address ipv4 ipv4-address {prt port-number} | {port-range minimum-port number
maximum-port number}
```

Syntax Description	Field	Description
	<b>ipv4</b>	Configures an IPv4 media address.
	<i>ipv4-address</i>	IPv4 address assigned to an H.248 association.
	<b>port</b>	Specifies the port for the adjacency address.
	<i>port-number</i>	Number for the adjacency address port. The range is from 1 to 65535.
	<b>port-range</b>	Specifies the port range for the adjacency address.
	<i>minimum-port number</i>	Starting port number of the range. The possible values are from 1 to 65535, but the minimum port number specified must be less than or equal to the maximum port number specified.
	<i>maximum-port number</i>	Ending port number of the range. The possible values are from 1 to 65535, but the maximum port number specified must be greater than the minimum port number specified.

**Command Default** None

**Command Modes** H.248 BAC adjacency configuration (config-h248-bac-adj)

Command History	Release	Modification
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

The BAC handles two types of Message Identifiers (MIDs): domain name and IP address.

If the **control-address ipv4** command is configured in the core adjacency submode and the MID of an IAD is IP address, only the **port-range** is configured and not the **port**.

If the **control-address ipv4** command is configured in the access adjacency submode, irrespective of the MID type, only the **port** is configured.

---

**Examples**

The following example shows how the **control-address ipv4** command is used to configure a local IPv4 H.248 signaling address for the BAC in the core adjacency submode:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 core core_spec2
Router(config-h248-bac-adj)# control-address ipv4 192.168.102.222 port-range 2944 4000
```

The following example shows how the **control-address** command is used to configure a local IPv4 H.248 signaling address for the BAC in the access adjacency submode:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# control-address ipv4 172.16.104.14 port 2940
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>adjacency h248</b>	Configures an H.248 BAC access adjacency and core adjacency.

# controller h248

To configure the H.248 controller for a data border element (DBE) or enter into Controller H.248 configuration mode, use the **controller h248** command in VDBE configuration mode. To delete the H.248 controller, use the **no** form of this command.

```
controller h248 {controller-index}
```

```
no controller h248 {controller-index}
```

<b>Syntax Description</b>	<i>controller-index</i>	The number that identifies the H.248 controller for the DBE, in case you want to configure more than one controller.
---------------------------	-------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	VDBE configuration (config-sbc-dbe-vdbe)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	Once a controller is configured and attached, it must be detached with the <b>no attach-controllers</b> command before you can modify any controller information.
-------------------------	---



**Note**

This command is invalid for the unified model, where both the SBE and DBE logical entities co-exist on the same network element.

<b>Examples</b>	The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures an H.248 controller with index 1.
-----------------	--

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# controller h248 1
```

The following example configures an H.248 controller with index 1 and tries to configure an IPv4 remote address on the controller. The message indicates that the controller must be detached first before the remote address can be modified.

```
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 210.229.108.253
SBC: remote-address cannot be changed while controllers are attached.
```

**Related Commands**

<b>Command</b>	<b>Description</b>
sbc dbc	Creates the DBE service on an SBC and enters into SBC-DBE configuration mode.
vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.

## control address aaa

To configure an SBE to use a given IPv4 AAA control address when contacting an authentication or billing server, use the **control address aaa ipv4** command in **SBE** configuration mode. To deconfigure the IPv4 AAA control address, use the **no** form of this command.

```
control address aaa ipv4 ip_address [vrf vrf-name]
```

```
no control address aaa ipv4 ip_address
```

### Syntax Description

<b>ipv4 ip_address</b>	Specifies the IPv4 AAA control address.
<b>vrf vrf-name</b>	(Optional) Specifies the VRF name.

### Command Default

No default behavior or values are available.  
SBE configuration (config-sbc-sbe)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to configure the SBE to use address 10.1.0.1 as its AAA control address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address aaa ipv4 10.1.0.1 vrf myvrf
```

### Related Commands

Command	Description
control address h248 index	Configures IPv4 H.248 control addresses.

# control address h248 index

To configure an SBE to use a given IPv4 H.248 control address, port, or transport for H.248 communications when acting as a media gateway controller, use the **control address h248 index** command in SBE configuration mode. To deconfigure the given IPv4 H.248 control address when acting as a media gateway controller, use the **no** form of this command.

**control address h248 index** *index-number*

**no control address h248 index** *index-number*

<b>Syntax Description</b>	<i>index-number</i>	Specifies the unique identifier of the H.248 control address to set. The index number range is from 0 to 2147483647.
---------------------------	---------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The “Examples” section shows the hierarchy of modes required to run the command.
-------------------------	--

See the related commands: **control-address h248 ipv4**, **control address h248 port**, and **control address h248 transport** commands.

<b>Examples</b>	The following example shows the options available when you enter into SBC SBE CTRL-H248 configuration mode, after entering the <b>control address h248 index</b> <i>index-number</i> command:
-----------------	---

```
Router(config-sbc-sbe)# control address h248 index 0
Router(config-sbc-sbe-ctrl-h248)# ?
SBC SBE CTRL-H248 Configuration Commands:
  default      Set a command to its defaults
  exit         Exit the SBC SBE CTRL-H248 configuration mode
  ipv4         IPv4 address
  no           Negate a command or set its defaults
  port         Listening port number
  transport    Transport method to use for connection to H.248 controller

Router(config-sbc-sbe-ctrl-h248)#
```

The following example shows how to configure the SBE to use address 10.1.0.1 as its H.248 control address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 index 1
Router(config-sbc-sbe-ctrl-h248)# ipv4 10.1.0.1
Router(config-sbc-sbe-ctrl-h248)# exit
```

#### Related Commands

Command	Description
<b>ipv4 (SBE H.248)</b>	Configures an SBE to use a given IPv4 H.248 control address.
<b>port (SBE H.248)</b>	Configures an SBE to use a given IPv4 H.248 port.
<b>transport (SBE H.248)</b>	Configures an SBE to use a certain transport for H.248 communications.

# control address h248 port

To configure an SBE to use a given port for H.248 communications when acting as a media gateway controller, use the **control-address h248 port** command in SBE configuration mode. To deconfigure a h248 controller, use the **no** form of this command.

**control address h248 port** *port-number*

**no control address h248 port** *port-number*

## Syntax Description

*port-number* Port number assigned.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To change or remove this configuration, deconfigure the h248 controller by issuing the **no control address h248** command, then configure a new h248 control address.

If the port is not configured, or is configured with the value zero, then the H.248 default port number, 2944, is used.

## Examples

The following command configures the SBE to use port 123 as its H.248 port:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 port 123
Router(config-sbc-sbe)# exit
```

## Related Commands

Command	Description
control-address h248 transport	Configures an SBE to use a given transport for H.248 communications.



# control address h248 transport

To configure an SBE to use a given transport for H.248 communications when acting as a media gateway controller, use the **control-address h248 transport** command in SBE configuration mode. To deconfigure a h248 controller, use the **no** form of this command.

*control address h248 transport [udp | tcp]*

*no control address h248 transport [udp | tcp]*

Syntax Description	
<i>udp</i>	Selects UDP as the underlying transport.
<i>tcp</i>	Selects TCP as the underlying transport.

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To change or remove this configuration, deconfigure the h248 controller by issuing the **no control address h248** command, then configure a new h248 control address.

**Examples** The following command configures the SBE to use TCP as its H.248 transport:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 transport tcp
Router(config-sbc-sbe)# exit
```

Related Commands	Command	Description
	control-address h248 port	Configures an SBE to use a given port for H.248 communications.

# copy logs

To transfer debug and system logs off of the ACE for analysis, use the *copy logs uri* command in Exec mode.

*copy logs uri*

<b>Syntax Description</b>	uri	Specifies either image:/filename.tar or disk0:/filename.tar.
---------------------------	-----	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Exec (#)	
----------------------	----------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	You can specify the filename but it must end in <i>.tar</i> .	
-------------------------	---	--

<b>Examples</b>	<p>The following example copies the log files to the ku040708.tar file:</p> <pre>Router# <b>copy logs image:/ku040708.tar</b></pre> <p>Copying logs to tar file image:/ku040708.tar..</p>	
-----------------	---	--

# core-adj

To bind an H.248 Border Access Controller (BAC) core adjacency with its corresponding H.248 BAC access adjacency, use the **core-adj** command in the H248 BAC adjacency configuration mode. To unbind an H.248 BAC core adjacency from its corresponding H.248 BAC access adjacency, use the **no** form of this command.

**core-adj** *core adjacency-name*

**no core-adj** *core adjacency-name*

<b>Syntax Description</b>	<i>core adjacency-name</i>	Name of the core adjacency.  The <i>core adjacency-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------------	----------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	H248 BAC adjacency configuration (config-h248-bac-adj)
----------------------	--

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 3.7</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	This command can be configured only in the access adjacency submode and not in the core adjacency submode.
-------------------------	--

**Examples** The following example shows how the **core-adj** command is used to bind an H.248 BAC core adjacency with its corresponding H.248 BAC access adjacency:

```
Router# configure terminal
Router(config)# sbac h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# core-adj core_spec2
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>adjacency h248</b></td> <td>Configures an H.248 BAC access adjacency and core adjacency.</td> </tr> </tbody> </table>	Command	Description	<b>adjacency h248</b>	Configures an H.248 BAC access adjacency and core adjacency.
Command	Description				
<b>adjacency h248</b>	Configures an H.248 BAC access adjacency and core adjacency.				

# cost

To assign a cost to this route, use the **cost** command in the RTG routing table entry configuration mode. To destroy the cost given to the route, use the **no** form of this command.

*cost cost*

**no cost cost**

## Syntax Description

<i>cost</i>	Range: [1-0xFFFFFFFF] The value of "0" is not accepted. Enter "na" to mean this entry will never be matched.
-------------	---

## Command Default

The default is "na".

## Command Modes

RTG routing table entry configuration (config-sbc-sbe-rtgpolicy-rtgtable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to create an entry in the new admission control table, MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-least-cost-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# cost
Router(config-sbc-sbe-rtgpolicy-entry)# exit
```

## Related Commands

Command	Description
<b>rtg-least-cost-table</b>	Configures the least-cost routing table.

# critical-alert-size

To configure the number of specified events before a critical alert is triggered, use the **critical-alert-size** command in the blacklist reason mode. To disable the number of specified events, use the no form of this command.

**critical-alert-size** *number-of-events*

**no critical-alert-size**

<b>Syntax Description</b>	<i>number-of-events</i>	The number of events for alert to be triggered. This can be of any value ranging from 1 to 65535.
---------------------------	-------------------------	---

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Blacklist reason mode (config-sbc-sbe-blacklist-reason)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.
-------------------------	---

<b>Examples</b>	The following example shows how to configure the number of specified events for a critical alert to be triggered using the <b>critical-alert-size</b> command in the blacklist reason mode:
-----------------	---

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist)# reason na-policy-rejection
Router(config-sbc-sbe-blacklist-reason)# critical-alert-size 655
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>major-alert-size</b>	Configures the number of specified events before a major alert is triggered.
	<b>minor-alert-size</b>	Configures the number of specified events before a minor alert is triggered.
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).

<b>Command</b>	<b>Description</b>
<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
snmp-server enable traps sbc blacklist	To enable SNMP SBC Blacklist traps.
<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.

# current15minutes

To specify that QoS statistics must be calculated for 15-minute intervals, use the **current15minutes** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

```
current15minutes {adjacency adjacency-name {critical low value upper value | major low value
upper value [critical low value upper value] | minor low value upper value [[critical low
value upper value] | [major low value upper value [critical low value upper value]]]} |
default {critical low value upper value | major low value upper value [critical low value
upper value] | minor low value upper value [[critical low value upper value] | [major low
value upper value [critical low value upper value]]]}
```

```
no current15minutes {adjacency adjacency-name | default}
```

Syntax Description		
<b>adjacency</b>		Specifies that alert levels must be set for the specified adjacency.
<i>adjacency-name</i>		Name of the adjacency.
<b>critical</b>		Specifies the lower limit and upper limit for the Critical alert level.
<b>low</b>		Specifies the lower limit for the alert level.
<i>value</i>		Value of the lower limit or upper limit.
<b>upper</b>		Specifies the upper limit for the alert level.
<b>major</b>		Specifies the lower limit and upper limit for the Major alert level.
<b>minor</b>		Specifies the lower limit and upper limit for the Minor alert level.
<b>default</b>		Specifies that alert levels must be set for all adjacencies on the SBC.

**Command Default** *No default behavior or values are available.*

**Command Modes** Statistics SBE configuration (config-sbc-sbe-stats)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

**Examples** The following example shows how to specify that statistics must be calculated for 15-minute intervals using the **current15mins** command in the statistics SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
```

```
Router(config-sbc-sbe)# statistics lcl-jit
Router(config-sbc-sbe-stats)# current15minutes default critical low 30 upper 50
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>calc-mosqoe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
current5minutes	Specifies that QoS statistics must be calculated for 5-minute intervals.
currentday	Specifies that statistics must be calculated for 24-hour intervals.
currenthour	Specifies that QoS statistics must be calculated for 60-minute intervals.
currentindefinite	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
g107 bpl	Sets a value for the Packet-Loss Robustness (Bpl) factor.
g107 ie	Sets a value for the Equipment Impairment (Ie) factor.
g107a-factor	Sets a value for the Advantage (A) factor.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
show sbc sbe adjacencies	Displays details of the adjacencies configured on the SBE.
show sbc sbe call-stats	Displays the statistics pertaining to all the calls on a the SBE.
snmp-server enable traps sbc	Enables SBC notification types.
statistics	Specifies the QoS statistic for which alert levels must be set.



# current5minutes

To specify that QoS statistics must be calculated for 5-minute intervals, use the **current5minutes** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

```
current5minutes {adjacency adjacency-name {critical low value upper value | major low value
upper value [critical low value upper value] | minor low value upper value [[critical low
value upper value] | [major low value upper value [critical low value upper value]]]} |
default {critical low value upper value | major low value upper value [critical low value
upper value] | minor low value upper value [[critical low value upper value] | [major low
value upper value [critical low value upper value]]]}
```

```
no current5minutes {adjacency adjacency-name | default}
```

Syntax Description		
<b>adjacency</b>		Specifies that alert levels must be set for the specified adjacency.
<i>adjacency-name</i>		Name of the adjacency.
<b>critical</b>		Specifies the lower limit and upper limit for the Critical alert level.
<b>low</b>		Specifies the lower limit for the alert level.
<i>value</i>		Value of the lower limit or upper limit.
<b>upper</b>		Specifies the upper limit for the alert level.
<b>major</b>		Specifies the lower limit and upper limit for the Major alert level.
<b>minor</b>		Specifies the lower limit and upper limit for the Minor alert level.
<b>default</b>		Specifies that alert levels must be set for all adjacencies on the SBC.

**Command Default** *No default behavior or values are available.*

**Command Modes** Statistics SBE configuration (config-sbc-sbe-stats)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

**Examples** The following example shows how to specify that statistics must be calculated for 5-minute intervals using the **current5mins** command in the statistics SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
```

```
Router(config-sbc-sbe)# statistics mpl-pct
Router(config-sbc-sbe-stats)# current5minutes default major low 10 upper 29 critical low
30 upper 50
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
current15minutes	Specifies that QoS statistics must be calculated for 15-minute intervals.
currentday	Specifies that statistics must be calculated for 24-hour intervals.
currenthour	Specifies that QoS statistics must be calculated for 60-minute intervals.
currentindefinite	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
g107 bpl	Sets a value for the Packet-Loss Robustness (Bpl) factor.
g107 ie	Sets a value for the Equipment Impairment (Ie) factor.
g107a-factor	Sets a value for the Advantage (A) factor.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
show sbc sbe adjacencies	Displays details of the adjacencies configured on the SBE.
show sbc sbe call-stats	Displays the statistics pertaining to all the calls on a the SBE.
snmp-server enable traps sbc	Enables SBC notification types.
statistics	Specifies the QoS statistic for which alert levels must be set.

# currentday

To specify that statistics must be calculated for 24-hour intervals (starting from midnight), use the **currentday** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

```
currentday {adjacency adjacency-name {critical low value upper value | major low value upper value [critical low value upper value] | minor low value upper value [[critical low value upper value] | [major low value upper value [critical low value upper value]]]} | default {critical low value upper value | major low value upper value [critical low value upper value] | minor low value upper value [[critical low value upper value] | [major low value upper value [critical low value upper value]]]}
```

```
no currentday {adjacency adjacency-name | default}
```

Syntax Description		
<b>adjacency</b>		Specifies that alert levels must be set for the specified adjacency.
<i>adjacency-name</i>		Name of the adjacency.
<b>critical</b>		Specifies the lower limit and upper limit for the Critical alert level.
<b>low</b>		Specifies the lower limit for the alert level.
<i>value</i>		Value of the lower limit or upper limit.
<b>upper</b>		Specifies the upper limit for the alert level.
<b>major</b>		Specifies the lower limit and upper limit for the Major alert level.
<b>minor</b>		Specifies the lower limit and upper limit for the Minor alert level.
<b>default</b>		Specifies that alert levels must be set for all adjacencies on the SBC.

**Command Default** *No default behavior or values are available.*

**Command Modes** Statistics SBE configuration (config-sbc-sbe-stats)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

**Examples** The following example shows how to specify that statistics must be calculated for 15-minute intervals using the **currentday** command in the statistics SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
```

```
Router(config-sbc-sbe)# statistics mos-cqe
Router(config-sbc-sbe-stats)# currentday default critical low 2 upper 3
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
current15minutes	Specifies that QoS statistics must be calculated for 15-minute intervals.
current5minutes	Specifies that QoS statistics must be calculated for 5-minute intervals.
currenthour	Specifies that QoS statistics must be calculated for 60-minute intervals.
currentindefinite	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
g107 bpl	Sets a value for the Packet-Loss Robustness (Bpl) factor.
g107 ie	Sets a value for the Equipment Impairment (Ie) factor.
g107a-factor	Sets a value for the Advantage (A) factor.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
show sbc sbe adjacencies	Displays details of the adjacencies configured on the SBE.
show sbc sbe call-stats	Displays the statistics pertaining to all the calls on a the SBE.
snmp-server enable traps sbc	Enables SBC notification types.
statistics	Specifies the QoS statistic for which alert levels must be set.

# currenthour

To specify that QoS statistics must be calculated for 60-minute intervals, use the **currenthour** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

```
currenthour {adjacency adjacency-name {critical low value upper value | major low value upper value [critical low value upper value] | minor low value upper value [[critical low value upper value] | major low value upper value [critical low value upper value]]] | default {critical low value upper value | major low value upper value [critical low value upper value] | minor low value upper value [[critical low value upper value] | major low value upper value [critical low value upper value]]]}}
```

```
no currenthour {adjacency adjacency-name | default}
```

Syntax Description		
<b>adjacency</b>		Specifies that alert levels must be set for the specified adjacency.
<i>adjacency-name</i>		Name of the adjacency.
<b>critical</b>		Specifies the lower limit and upper limit for the Critical alert level.
<b>low</b>		Specifies the lower limit for the alert level.
<i>value</i>		Value of the lower limit or upper limit.
<b>upper</b>		Specifies the upper limit for the alert level.
<b>major</b>		Specifies the lower limit and upper limit for the Major alert level.
<b>minor</b>		Specifies the lower limit and upper limit for the Minor alert level.
<b>default</b>		Specifies that alert levels must be set for all adjacencies on the SBC.

**Command Default** *No default behavior or values are available.*

**Command Modes** Statistics SBE configuration (config-sbc-sbe-stats)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

**Examples** The following example shows how to specify that statistics must be calculated for 60-minute intervals using the **currenthour** command in the statistics SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# statistics mpd-pct
```

```
Router(config-sbc-sbe-stats)# currenthour adjacency adj1 minor low 5 upper 19 critical low 20 upper 30
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>calc-mosqoe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
current15minutes	Specifies that QoS statistics must be calculated for 15-minute intervals.
current5minutes	Specifies that QoS statistics must be calculated for 5-minute intervals.
currentday	Specifies that statistics must be calculated for 24-hour intervals.
currentindefinite	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
g107 bpl	Sets a value for the Packet-Loss Robustness (Bpl) factor.
g107 ie	Sets a value for the Equipment Impairment (Ie) factor.
g107a-factor	Sets a value for the Advantage (A) factor.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
show sbc sbe adjacencies	Displays details of the adjacencies configured on the SBE.
show sbc sbe call-stats	Displays the statistics pertaining to all the calls on a the SBE.
snmp-server enable traps sbc	Enables SBC notification types.
statistics	Specifies the QoS statistic for which alert levels must be set.

# currentindefinite

To specify that statistics must be calculated indefinitely starting from the last explicit reset, use the **currentindefinite** command in the statistics SBE configuration mode. To remove this configuration, use the **no** form of this command.

```
currentindefinite {adjacency adjacency-name {critical low value upper value | major low value upper value [critical low value upper value] | minor low value upper value [[critical low value upper value] | [major low value upper value [critical low value upper value]]]} | default {critical low value upper value | major low value upper value [critical low value upper value] | minor low value upper value [[critical low value upper value] | [major low value upper value [critical low value upper value]]]}
```

```
no currentindefinite {adjacency adjacency-name | default}
```

Syntax Description		
<b>adjacency</b>		Specifies that alert levels must be set for the specified adjacency.
<i>adjacency-name</i>		Name of the adjacency.
<b>critical</b>		Specifies the lower limit and upper limit for the Critical alert level.
<b>low</b>		Specifies the lower limit for the alert level.
<i>value</i>		Value of the lower limit or upper limit.
<b>upper</b>		Specifies the upper limit for the alert level.
<b>major</b>		Specifies the lower limit and upper limit for the Major alert level.
<b>minor</b>		Specifies the lower limit and upper limit for the Minor alert level.
<b>default</b>		Specifies that alert levels must be set for all adjacencies on the SBC.

**Command Default** *No default behavior or values are available.*

**Command Modes** Statistics SBE configuration (config-sbc-sbe-stats)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

**Examples** The following example shows how to specify that statistics must be calculated indefinitely starting from the last explicit reset using the **currentindefinite** command in the statistics SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
```

```
Router(config-sbc-sbe)# statistics mpl-pct
Router(config-sbc-sbe-stats)# currentindefinite adjacency adj1 minor low 31 upper 40 major
low 41 upper 50 critical low 51 upper 60
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
current15minutes	Specifies that QoS statistics must be calculated for 15-minute intervals.
current5minutes	Specifies that QoS statistics must be calculated for 5-minute intervals.
currentday	Specifies that statistics must be calculated for 24-hour intervals.
currenthour	Specifies that QoS statistics must be calculated for 60-minute intervals.
g107 bpl	Sets a value for the Packet-Loss Robustness (Bpl) factor.
g107 ie	Sets a value for the Equipment Impairment (Ie) factor.
g107a-factor	Sets a value for the Advantage (A) factor.
local-jitter-ratio	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
show sbc sbe adjacencies	Displays details of the adjacencies configured on the SBE.
show sbc sbe call-stats	Displays the statistics pertaining to all the calls on a the SBE.
snmp-server enable traps sbc	Enables SBC notification types.
statistics	Specifies the QoS statistic for which alert levels must be set.



## deact-mode (billing)

To configure the deactivate mode for the billing method, use the **deact-mode** command in the packetcable-em configuration mode. To disable the deactivate mode, use the **no** form of this command.

**deact-mode {abort | quiesce}**

**no deact-mode**

Syntax Description	
<b>abort</b>	Billing method is deactivated immediately. No further CDRs for existing calls and new calls are generated.
<b>quiesce</b>	Billing CDRs are not generated for new calls. CDRs continue to be generated for existing calls until the calls complete. This delays the deactivation of the method.

**Command Default** The default is abort.

**Command Modes** Packet-cable em configuration (config-sbc-sbe-billing-packetcable-em)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to delay the deactivation of the billing method:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
(config-sbc-sbe-billing)# packetcable-em 4 transport radius test
(config-sbc-sbe-billing-packetcable-em)# batch-size 256
(config-sbc-sbe-billing-packetcable-em)# batch-time 22
(config-sbc-sbe-billing-packetcable-em)# attach
(config-sbc-sbe-billing-packetcable-em)# activate
(config-sbc-sbe-billing-packetcable-em)# deact-mode quiesce
```

Related Commands	Command	Description
	<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
	<b>attach</b>	activate the billing for a RADIUS client

<b>Command</b>	<b>Description</b>
<b>batch-size</b>	Configures the batching or grouping of RADIUS messages sent to a RADIUS server.
<b>batch-time</b>	Configures the maximum number of milliseconds for which any record is held in the batch before the batch is sent
<b>deact-mode</b>	Configures the deactivate mode for the billing method.
<b>ldr-check</b>	Configures the time of day (local time) to run the Long Duration Check (LDR).
<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
<b>local-address ipv4 (packet-cable)</b>	Configures the local address of the packet-cable billing instance.
<b>method packetcable-em</b>	Enables the packet-cable billing method.
<b>packetcable-em transport radius</b>	Configures a packet-cable billing instance.
<b>show sbc sbe billing remote</b>	Displays the local and billing configurations.

## deact-mode (XML Billing)

To configure the deactivate mode for the XML billing method, use the **deact-mode** command in the SBE billing XML configuration mode. The **deact-mode** command defines the state after which the billing method will be deactivated. To disable the deactivate mode, use the **no** form of this command.

**deact-mode {normal | quiesce | abort}**

**no deact-mode**

### Syntax Description

<b>normal</b>	Billing CDRs are generated for the existing calls before the billing method is deactivated. The calls that are still in progress and have not ended are not included in the CDR billing cycle. The default mode is normal.
<b>quiesce</b>	Billing CDRs are generated for the existing calls, and the CDRs continue to be generated for the calls that have still not ended. This delays the XML billing method from being deactivated.
<b>abort</b>	The billing method is deactivated immediately. No further CDRs are generated for the existing calls and new calls.

### Command Default

By default, the deact-mode is normal.

### Command Modes

SBE billing XML configuration (config-sbc-sbe-billing-xml)

### Command History

Release	Modification
3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

### Usage Guidelines

The XML billing method can be deactivated forcefully using the **deact-mode** command from SBE billing XML configuration mode.

Since the calls are still in progress, it is important to bill the calls that are completed before the XML billing method is deactivated. To bill the CDRs for the existing calls before deactivating the XML billing method, use the **deact-mode normal** command.

As an option to wait for the calls that have still not ended, and to build the CDRs for the existing calls as well as the calls that are still in progress, use the **deact-mode quiesce** command.

To immediately abort the XML billing method without billing the CDRs, use the **deact-mode abort** command.

### Examples

The following example shows how to set the deactivation mode to normal. This will process the CDRs for the existing calls:

```
Router(config)# sbc sbcbilling
Router(config-sbc)# sce
Router(config-sbc-sce)# billing
```

```
Router(config-sbc-sce-billing)# xml method  
Router(config-sbc-sce-billing)# xml 1  
Router(config-sbc-sce-billing-xml)# deact-mode normal
```

The following example shows how to bill CDRs for the existing calls and will continue to build the CDRs for the calls that are still in progress:

```
Router(config-sbc-sce-billing-xml)# deact-mode quiesce
```

The following example shows how to deactivate the XML billing method without building the CDRs:

```
Router(config-sbc-sce-billing-xml)# deact-mode abort
```

#### Related Commands

Command	Description
<b>xml (billing)</b>	Configures the method index for XML billing.
<b>method xml</b>	Configures the billing method as XML for the Billing Manager.
<b>ldr-check</b>	Configures the time at which long duration records are checked.

# deactivation-mode (session border controller)

To specify the action to take upon DBE or SBE deactivation, use the **deactivation-mode** command in the appropriate configuration mode. To revert to the default value, use the **no** form of this command.

**deactivation-mode** *deact-type*

**no deactivation-mode**

## Syntax Description

<i>deact-type</i>	Specifies the action to take upon DBE deactivation: <ul style="list-style-type: none"> <li>• <b>abort</b>: All calls dropped with no signaling.</li> <li>• <b>normal</b>: Service change signaled to SBE, and all calls immediately terminated.</li> <li>• <b>quiesce</b>: No new calls accepted. Deactivation occurs only after existing calls have terminated naturally.</li> </ul>
	Specifies the action to take upon SBE deactivation: <ul style="list-style-type: none"> <li>• <b>abort</b>: All calls dropped with no signaling.</li> <li>• <b>normal</b>: Existing calls are torn down gracefully.</li> <li>• <b>quiesce</b>: No new calls accepted. Existing calls are allowed to terminate.</li> </ul>

## Command Default

By default, this command assumes the **normal** parameter.

## Command Modes

SBC-DBE configuration (config-sbc-dbe)  
SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.4	Support for SBE was added for unified SBC.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to set the DBE to deactivate in *quiesce* mode to prepare the device for hardware maintenance:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# deactivation-mode quiesce
```

Related Commands	Command	Description
	<b>sbc dbe</b>	Creates the DBE service on a SBC and enters into the DBE-SBE configuration mode.
	<b>activate</b>	Initiates the DBE service of the Session Border Controller (SBC).

# debug condition vrf

To limit debug output to a specific Virtual Routing and Forwarding (VRF) instance, use the **debug condition vrf** command in privileged EXEC mode. To remove the debug condition, use the **undebug** version of the command.

**debug condition vrf** *vrf-name*

**undebug condition vrf** *vrf-name*

## Syntax Description

<i>vrf-name</i>	Name of a VRF.
-----------------	----------------

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

## Usage Guidelines

Use this command to limit debug output to a single VRF.

### Note

EIGRP does not support the **debug condition vrf** command.

## Examples

The following example shows how to limit debugging output to VRF red:

```
Router# debug condition vrf red
```

## Related Commands

Command	Description
<b>vrf definition</b>	Defines a virtual routing and forwarding instance.

# debug ip bgp igp-metric ignore

To display information related to the system ignoring the Interior Gateway Protocol (IGP) metric during best path selection, use the **debug ip bgp igp-metric ignore** command in privileged EXEC mode. To disable such debugging output, use the **no** form of the command.

**debug ip bgp igp-metric ignore**

**no debug ip bgp igp-metric ignore**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines** You might use this command if the path you expected to be chosen as the best path at the shadow RR was not chosen as such. That could be because the **bgp bestpath igp-metric ignore** command makes the best path algorithm choose the same best path as the primary RR if they are not co-located.

**Examples** The following example turns on debugging of events related to the system ignoring the IGP metric during bestpath selection:

```
Router# debug ip bgp igp-metric ignore
```

Related Commands	Command	Description
	<b>bgp bestpath igp-metric ignore</b>	Specifies that the system ignore the Interior Gateway Protocol (IGP) metric during best path selection.



# debug ip bgp route-server

To turn on debugging for a BGP route server, use the **debug ip bgp route-server** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip bgp route-server {client | context | event | import | policy} [detail]
```

```
no debug ip bgp route-server {client | context | event | import | policy} [detail]
```

## Syntax Description

<b>client</b>	Displays information about BGP route server clients.
<b>context</b>	Displays information about BGP route server contexts.
<b>event</b>	Displays information about route server events, such as importing into the virtual RS table.
<b>import</b>	Displays information about BGP route server import maps.
<b>policy</b>	Displays information about the policy path process.
<b>detail</b>	(Optional) Displays detailed debugging information.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.

## Usage Guidelines

Use this command to turn on debugging of a BGP router server.

**Caution** The **detail** keyword is used for complex issues and should only be turned on when you are debugging with a Cisco representative.

## Examples

In the following example, BGP route server client debugging is turned on:

```
Router# debug ip bgp route-server client
```

## Related Commands

Command	Description
<b>import-map</b>	Configures flexible policy handling by a BGP route server.
<b>neighbor route-server-client</b>	Specifies on a BGP route server that a neighbor is a route server client.
<b>route-server-context</b>	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

# debug ip multicast topology

To enable debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream access control list (ACL) matching events, use the **debug ip multicast topology** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ip multicast topology**

**no debug ip multicast topology**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

**Usage Guidelines** Use this command when IP multicast stream topology creation, IP multicast stream topology deletion, or IP multicast stream ACL matching appears not to be functioning.

**Examples** The following example shows how to enable debugging output for IP multicast stream topology creation events, IP multicast stream topology deletion events, and IP multicast stream ACL matching events:

```
Router# debug ip multicast topology
```

Related Commands	Command	Description
	<b>ip multicast rpf select topology</b>	Associates a multicast topology with a multicast group with a specific mroute entry.
	<b>ip multicast topology</b>	Configures topology selection for multicast streams.
	<b>show ip multicast topology</b>	Displays IP multicast topology information.

## debug ip wccp

To display information about Web Cache Control Protocol (WCCP) services, use the **debug ip wccp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip wccp { default | vrf vrf-name { events | packets [control] } | events | packets [bypass | control | redirect] | platform | subblocks }
```

```
no debug ip wccp { default | vrf vrf-name { events | packets [control] } | events | packets [bypass | control | redirect] | platform | subblocks }
```

Syntax Description		
<b>default</b>		Displays information about default WCCP services.
<b>vrf</b> <i>vrf-name</i>		Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
<b>events</b>		Displays information about significant WCCP events.
<b>packets</b>		Displays information about every WCCP packet received or sent by the router.
<b>control</b>	(Optional)	Displays information about WCCP control packets.
<b>bypass</b>	(Optional)	Displays information about WCCP bypass packets.
<b>redirect</b>	(Optional)	Displays information about WCCP redirect packets.
<b>platform</b>		Displays information about WCCP platform API.
<b>subblocks</b>		Displays information about WCCP subblocks.

**Command Default** Debug information is not displayed.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	15.0(1)M	This command was introduced. This command replaces the <b>debug ip wccp packets</b> and <b>debug ip wccp events</b> commands.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

**Usage Guidelines** When the **vrf** keyword is not used, the command displays debug information about all WCCP services on the router. The **default** keyword is used to specify default WCCP services.

## Examples

The following is sample output from the **debug ip wccp events** command when a Cisco Cache Engine is added to the list of available Web caches:

```
Router# debug ip wccp events

WCCP-EVNT: Built I_See_You msg body w/1 usable web caches, change # 0000000A
WCCP-EVNT: Web Cache 192.168.25.3 added
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000B
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000C
```

The following is sample output from the **debug ip wccp packets** command. The router is sending keepalive packets to the Cisco Cache Engines at 192.168.25.4 and 192.168.25.3. Each keepalive packet has an identification number associated with it. When the Cisco Cache Engine receives a keepalive packet from the router, it sends a reply with the identification number back to the router.

```
Router# debug ip wccp packets

WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.4 w/rcvd_id 00003532
WCCP-PKT: Sending I_See_You packet to 192.168.25.4 w/ rcvd_id 00003534
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003533
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003535
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.4 w/rcvd_id 00003534
WCCP-PKT: Sending I_See_You packet to 192.168.25.4 w/ rcvd_id 00003536
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003535
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003537
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.4 w/rcvd_id 00003536
WCCP-PKT: Sending I_See_You packet to 192.168.25.4 w/ rcvd_id 00003538
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003537
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003539
```

## Related Commands

Command	Description
<b>clear ip wccp</b>	Clears the counter for packets redirected using WCCP.
<b>ip wccp</b>	Enables support of the specified WCCP service for participation in a service group.
<b>ip wccp redirect</b>	Enables packet redirection on an outbound or inbound interface using WCCP.
<b>show ip interface</b>	Lists a summary of the IP information and status of an interface.

# debug platform hardware qfp active feature wccp

To enable debug logging for the Web Cache Communication Protocol (WCCP) client in the Cisco Quantum Flow Processor (QFP), use the **debug platform hardware qfp active feature wccp** command in privileged EXEC mode. To disable WCCP QFP debug logging, use the **no** form of this command.

```
debug platform hardware qfp active feature wccp { { client | lib-client { all | error | info | trace | warning } } | datapath all }
```

```
no debug platform hardware qfp active feature wccp { { client | lib-client { all | error | info | trace | warning } } | datapath all }
```

Syntax Description		
	<b>client</b>	Enables WCCP QFP client debug logging.
	<b>lib-client</b>	Enables WCCP QFP client-library debug logging.
	<b>all</b>	Enables all logs.
	<b>error</b>	Enables error logs.
	<b>info</b>	Enables info logs.
	<b>trace</b>	Enables trace logs.
	<b>warning</b>	Enables warning logs.
	<b>datapath all</b>	Enables all WCCP QFP datapath debug logging.

**Command Default** WCCP QFP debug logging is disabled.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced.

**Usage Guidelines**

When the **debug platform hardware qfp active feature wccp** command is configured, QFP client debugs are enabled and can be collected from the forwarding processor (FP) from the file `cpp_cp_F0-0.log`.

When the **debug platform hardware qfp active feature wccp lib-client all** command is configured, QFP lib-client debugs are enabled and can be collected from the FP from the file `fman-fp_F0-0.log`.

When the **debug platform hardware qfp active feature wccp datapath all** command is configured, QFP datapath debugs are enabled and can be collected from the FP from the file `cpp_cp-F0-0.log`.

**Examples**

The following is sample output from the **debug platform hardware qfp active feature wccp** command:

```
Router# debug platform hardware qfp active feature wccp
```

A WCCP service is configured:

```
06/17 10:48:15.980 [(null)]: (debug): cpp_wccp_service_add_handler: service_params:: type
=0 id = 0priority = 240 is_closed = 0 assign = 0
06/17 10:48:15.980 [(null)]: (debug): cpp_wccp_dplane_init dplane cpp-init for all cpps
06/17 10:48:15.980 [(null)]: (debug): cpp_wccp_dplane_init_cpp Enter: cpp_info =
0x1027b970:
.
.
.
```

The sequence of messages repeats for each access control entry (ACE) of a merged access control list (ACL):

```
06/17 10:53:38.792 [(null)]: (debug): cpp_wccp_update_bind_obj_list:idx = 63
bind-info:no.lvl = 1 fobj = 80024000 bind-id = 0
06/17 10:53:38.792 [(null)]: (debug): cpp_wccp_update_bind_obj_list fobj:service-id = 0
type = 0 cache-id = 9action = 2 acl-log = 0
06/17 10:53:38.792 [(null)]: (debug): cpp_wccp_add_dplane_cache_desc service-index = 0,
cache_id = 9
06/17 10:53:38.792 [(null)]: (debug): cpp_wccp_get_dplane_cache_index service-index = 0,
cache_id = 9
06/17 10:53:38.792 [(null)]: (debug): cpp_wccp_create_dplane_cache_index Cache index = 0
exists for cache-id = 9,service-index = 0
.
.
.
```

WCCP redirection is configured on an interface:

```
06/17 13:15:44.655 [(null)]: (debug): cpp_wccp_intf_attach_msg req = 0x13116848, msg-len =
36
06/17 13:15:44.655 [(null)]: (debug): cpp_wccp_intf_attach_handler: type = 0 id = 0 ifh =
17dir = 0 vrfid = 0
06/17 13:15:44.655 [(null)]: (debug): cpp_wccp_get_service_index WCCP: service_id 0 vrfid
0service_desc_index 0
06/17 13:15:44.655 [(null)]: (debug): cpp_wccp_get_service_desc: service-id: 0 type = 0
index = 0
.
.
.
```

Debug messages appear for each ACE of the merged ACL for a service group:

```
06/17 13:15:44.670 [(null)]: (debug): cpp_wccp_translate_fobj_to_cce_result Entry
06/17 13:15:44.670 [(null)]: (debug): cpp_wccp_get_service_index WCCP: service_id 0 vrfid
0service_desc_index 0
06/17 13:15:44.670 [(null)]: (debug): cpp_wccp_get_service_desc: service-id: 0 type = 0
index = 0
06/17 13:15:44.670 [(null)]: (debug): cpp_wccp_get_dplane_cache_index service-index = 0,
cache_id = 9
.
.
.
```

Redirection is removed from an interface:

```
06/17 13:24:54.617 [(null)]: (debug): cpp_wccp_intf_detach_handler: type = 0 id = 0 ifh =
17dir = 0 vrfid = 0
06/17 13:24:54.617 [(null)]: (debug): cpp_wccp_get_service_index WCCP: service_id 0 vrfid
0service_desc_index 0
```

```
06/17 13:24:54.617 [(null)]: (debug): cpp_wccp_get_service_desc: service-id: 0 type = 0
index = 0
06/17 13:24:54.617 [(null)]: (debug): cpp_wccp_intf_detach_handler:hw_cg_node, ifh = 17
dir = 0vrfid = 0 service-index = 0 exists
.
.
```

A service group is unconfigured:

```
06/17 13:29:41.828 [(null)]: (debug): cpp_wccp_cache_delete_handler: cache-desc ip-addr =
5a140102 id-addr = 0cache-id = 9 cef_handle = 0x112d3b68 cef-obj-type = 10router-id =
42424242 ce_mac_addr fwd-method = 0 hw-addr = 0x11188f78
06/17 13:29:41.828 [(null)]: (debug): cpp_wccp_remove_dplane_ip_hash_entry cache_id= 9:
06/17 13:29:41.828 [(null)]: (debug): cpp_wccp_remove_dplane_ip_hash_entry ip-hash-index =
6934:
.
.
.
```

The following is sample output from the **debug platform hardware qfp active feature wccp lib-client all** command:

```
Router# debug platform hardware qfp active feature wccp lib-client all
```

A WCCP service group is configured:

```
06/17 13:47:00.158 [buginf]: (debug): cpp_wccp_service_group_add_a: API call from PAL
service-type = 0 id = 0vrfid = 0, priority = 240 is_closed = 0 has_ports = 1 assign-method
= 0
06/17 13:47:00.158 [buginf]: (debug): cpp_wccp_api_async_msg_send: data size = 28 for this
3message
06/17 13:47:00.158 [buginf]: (debug): cpp_wccp_api_async_send_cb: SMC async send call-back
.
.
.
```

The set of debug messages repeats for each ACE of the merged ACL of the WCCP service group:

```
06/17 13:47:29.474 [buginf]: (debug): Notification from CGM to WCCP, op:13, tid:0,async:
0, ctx: (nil)
06/17 13:47:29.474 [buginf]: (debug): cpp_wccp_cgm_notif_handler:cgm BIND num_lvl = 1,
bind-id = 0 fobj = 80028000
06/17 13:47:29.474 [buginf]: (debug): Notification from CGM to WCCP, op:2, tid:0,async:
1,ctx: 0x77
.
.
.
```

WCCP redirection is configured on an interface:

```
06/17 13:52:05.841 [buginf]: (debug): Notification from CGM to WCCP, op:1, tid:0,async:
0,ctx: (nil)
06/17 13:52:05.841 [buginf]: (debug): cpp_wccp_attach_service_to_intf_a: API call from PAL
service-type = 0 id = 0 vrfid = 0 if_h = 11 dir = 0
06/17 13:52:05.841 [buginf]: (debug): cpp_wccp_attach_service_to_intf_a:tid el= 0x11347470
ifh = 17, dir = 0 id = 0 type = 0 vrfid = 0
.
.
.
```

WCCP is unconfigured on an interface:

```
06/17 13:54:30.544 [buginf]: (debug): Notification from CGM to WCCP, op:1, tid:0,async:
0,ctx: (nil)
```

```
06/17 13:54:30.544 [buginf]: (debug): cpp_wccp_detach_service_from_intf_a: API call from
PALservice-type = 0 id = 0 vrfid = 0 if_h = 11 dir = 0
06/17 13:54:30.544 [buginf]: (debug): cpp_wccp_detach_service_from_intf_a:tid el=
0x11338890ifh = 17, dir = 0 id = 0 type = 0
06/17 13:54:30.544 [buginf]: (debug): Notification from CGM to WCCP, op:2, tid:0,async:
1,ctx: 0x79
.
.
.
```

A WCCP service group is unconfigured:

```
06/17 13:56:14.492 [buginf]: (debug): cpp_wccp_cache_delete_a: API call from PAL cache-id=
10
06/17 13:56:14.492 [buginf]: (debug): cpp_wccp_api_async_msg_send: data size = 2 for this
6 message
06/17 13:56:14.492 [buginf]: (debug): cpp_wccp_api_async_send_cb: SMC async send call-back
06/17 13:56:14.492 [buginf]: (debug): cpp_wccp_api_async_msg_send successfully sent
msg-type 6 to server.
06/17 13:56:14.492 [buginf]: (debug): Notification from CGM to WCCP, op:1, tid:0,async:
0,ctx: (nil)
06/17 13:56:14.492 [buginf]: (debug): Notification from CGM to WCCP, op:14, tid:0,async:
0, ctx: (nil)
06/17 13:56:14.493 [buginf]: (debug): cpp_wccp_cgm_notif_handler:cgm BIND num_lvl = 1,
bind-id = 0 fobj = 80028000
.
.
.
```

The debug messages repeat for each ACE of the merged ACL for the WCCP service group:

```
06/17 13:56:14.500 [buginf]: (debug): Notification from CGM to WCCP, op:14, tid:0,async:
0, ctx: (nil)
06/17 13:56:14.500 [buginf]: (debug): cpp_wccp_cgm_notif_handler:cgm BIND num_lvl = 1,
bind-id = 0 fobj = 80028000
06/17 13:56:14.501 [buginf]: (debug): Notification from CGM to WCCP, op:2, tid:0,async:
1,ctx: 0x7a
.
.
.
```

The following is sample output from the **debug platform hardware qfp active feature wccp datapath all** command:

```
Router# debug platform hardware qfp active feature wccp datapath all
```

A packet is successfully redirected:

```
06/17 14:49:28.935 [(null)]: (debug):
QFP:00 Thread:090 TS:00003918904609765795
#####
06/17 14:49:28.936 [(null)]: (debug):
QFP:00 Thread:090 TS:00003918904609777642 CCE IPV4 PKT
(src:3.3.3.2,dst:2.2.2.2,sp:0000,dprt:0050,prot:06,tos:00,len:0014,ttl:3f) , intf:3f3
06/17 14:49:28.936 [(null)]: (debug):
QFP:00 Thread:090 TS:00003918904609814715
#####
06/17 14:49:28.936 [(null)]: (debug):
QFP:00 Thread:090 TS:00003918904609825865 CCE IPV4 UIDB_INFO W0:00000004, W1:00084441,
tcam_region_index:0004, key_index:00, cmd:00084441
06/17 14:49:28.936 [(null)]: (debug):
.
.
.
```



<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ip wccp</b>	Removes WCCP statistics (counts) maintained on the router for a particular service.
	<b>ip wccp</b>	Enables support of the specified WCCP service for participation in a service group.
	<b>ip wccp check services all</b>	Enables enable all WCCP services.
	<b>ip wccp outbound-acl-check</b>	Enables execution of ACL applied on the actual outgoing interface of a packet before a decision is taken to redirect a packet.
	<b>ip wccp redirect</b>	Enables packet redirection on an outbound or inbound interface using WCCP.

# debug platform hardware qfp feature sbc

To enable debug logging for signaling border element (SBE) or the data border element (DBE) logs in the Cisco QuantumFlow Processor (QFP), use the **debug platform hardware qfp feature sbc** command in Privileged EXEC mode. To disable this form of debugging, use the **no** form of this command.

```
debug platform hardware qfp {active | standby} feature sbc {sbe {pfilter | sfx {datapath}} | dbe
  {client {all | clear | error | informational | trace | warning} | datapath {all | drop | dtmf | error |
  events | find | latch | proxy | rtcp}}
```

```
no debug platform hardware qfp {active | standby} feature sbc {sbe {pfilter | sfx {datapath}} | dbe
  {client {all | clear | error | informational | trace | warning} | datapath {all | drop | dtmf | error |
  events | find | latch | proxy | rtcp}}
```

## Syntax Description

active	Enables debug logging for the active processor.
standby	Enables debug logging for the standby processor.
sbe	SBC signaling border element. Enables SBE debug logging.
pfilter	Specifies SBC SBE packet filter.
sfx	Specifies SBC SIP Fast Register (SFX).
datapath	Specifies SBC datapath SIP Fast Register (SFX).
dbe	SBC data border element. Enables DBE debug logging.
client	Enables SBC DBE client debugging.
all	Specifies all client debugging.
clear	Specifies Clear the forwarding counters.
error	Specifies Client error debugging.
informational	Specifies Client informational debugging.
trace	Specifies Client trace debugging.
warning	Specifies Client warning debugging.
datapath	Enables SBC DBE datapath debugging.
all	Specifies datapath all debugs.
drop	Specifies datapath drop debugs.
dtmf	Specifies datapath DTMF debugs.
error	Specifies datapath errors debugs.
events	Specifies datapath events debugs.
find	Specifies datapath find debugs.
latch	Specifies datapath latch events debugs.
proxy	Specifies datapath proxy debugs.
rtcp	Specifies datapath RTCP debugs.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

**Command History**

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

The output of the debugs is stored in the `hddisk:tracelog/` directory.

**Examples**

The following example turns on debugging of SBE logs for SIP fast-register (SFX) datapath messages residing on the active processor in the Cisco QuantumFlow Processor (QFP):

```
Router# debug platform hardware qfp active feature sbc sbe sfx datapath
```

The following example turns on debugging of DBE logs for datapath DTMF debugs residing on the active processor in the Cisco QuantumFlow Processor (QFP):

```
Router# debug platform hardware qfp active feature sbc dbe datapath dtmf
```

**Related Commands**

Command	Description
<code>show platform hardware qfp active feature sbc sfx</code>	Displays information about SIP fast-register (SFX) messages in the Cisco QuantumFlow Processor (QFP).
<code>clear platform hardware qfp active feature sbc sfx</code>	Clears the Cisco QuantumFlow Processor (QFP) SIP Fast Register (SFX) counters.

# debug platform software wccp

To enable Web Cache Control Protocol (WCCP) platform debug messages, use the **debug platform software wccp** command in privileged EXEC mode. To disable WCCP platform debug messages, use the **no** form of this command.

```
debug platform software wccp { configuration | counters | detail | messages }
```

```
no debug platform software wccp { configuration | counters | detail | messages }
```

## Syntax Description

<b>configuration</b>	Enables configuration related debugs.
<b>counters</b>	Enables statistics collection related debugs.
<b>detail</b>	Enables detailed debugs for all WCCP related configurations.
<b>messages</b>	Enables debugs related to type definition language (TDL) messages being exchanged.

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. The <b>counters</b> keyword was added.

## Examples

The following is sample output from the **debug platform software wccp configuration** command:

```
Router# debug platform software wccp configuration
```

A WCCP service is configured:

```
*Jun 17 15:41:04.816: FMANRP-WCCP: Config Service Group (0, 0, 0)
    acl = , propagate_tos = TRUE, mode_is_closed = FALSE
    definition_is_valid = TRUE, protocol = 6, priority = 240
    ass_method = Unknown, fwd_method = Unknown, ret_method = Unknown
    num_mv_sets = 0, redirection_is_active = FALSE, num_wcs = 0
    use_source_port = FALSE, ports_defined = TRUE
    ports[0] = 80
    ports[1] = 0
    ports[2] = 0
    ports[3] = 0
    ports[4] = 0
    ports[5] = 0
    ports[6] = 0
    ports[7] = 0
*Jun 17 15:41:24.827: FMANRP-WCCP: create ce adjacency: CE = 90.20.1.2, fwd_method = GRE
oce= 0x30692230 adj = 0x306921C0 handle = 0x30692230 obj_id = 135
```

```

*Jun 17 15:41:24.827: FMANRP-WCCP: adjacency 90.20.1.2 (4500.0000.0000), router_id
66.66.66.66 proto=47
*Jun 17 15:41:39.807: FMANRP-WCCP: update mask data, Service Group (0, 0, 0)
    acl = , propagate_tos = TRUE, mode_is_closed = FALSE
    definition_is_valid = TRUE, protocol = 6, priority = 240
    ass_method = Mask, fwd_method = GRE, ret_method = L2
    num_mv_sets = 1, redirection_is_active = TRUE, num_wcs = 1
    use_source_port = FALSE, ports_defined = TRUE
    wc[0] = 90.20.1.2
    ports[0] = 80
    ports[1] = 0
    ports[2] = 0
    ports[3] = 0
    ports[4] = 0
    ports[5] = 0
    ports[6] = 0
    ports[7] = 0
*Jun 17 15:41:39.808: FMANRP-WCCP: Service Group (0, 0, 0) generate merged acl from IOS
*Jun 17 15:41:39.808: FMANRP-WCCP: wccp merged_acl(acl=), p=64 t=64 MCP wccp merged_acl,
num_port=1 result_len=64

```

#### A WCCP service is configured on an interface:

```

*Jun 17 15:45:17.083: FMANRP-WCCP: Config Service Group (0, 0, 0) to interface
GigabitEthernet0/3/1, direction = IN
*Jun 17 15:45:17.084: FMANRP-WCCP: Attach GigabitEthernet0/3/1 interface info for Service
group (0, 0, 0) if_handle 20, direction Input(0x2)

```

#### A WCCP service is removed from an interface:

```

*Jun 17 15:46:29.815: FMANRP-WCCP: Unconfig Service Group (0, 0, 0) to interface
GigabitEthernet0/3/1, direction = IN
*Jun 17 15:46:29.815: FMANRP-WCCP: Detach GigabitEthernet0/3/1 interface info for Service
group (0, 0, 0) if_handle 20, direction Input(0x2)

```

#### A WCCP service group is unconfigured:

```

*Jun 17 15:48:17.224: FMANRP-WCCP: (0 0 0) Delete ce = 90.20.1.2
*Jun 17 15:48:17.225: Failed to retrieve service group params while removing ce
*Jun 17 15:48:17.241: FMANRP-WCCP: Unconfig Service Group (0, 0, 0)

```

#### The following is sample output from **debug platform software wccp messages** command:

```
Router# debug platform software wccp messages
```

#### A WCCP service is configured:

```

*Jun 17 15:50:57.796: FMANRP-WCCP: send out (0, 0, 0) wccp_svc_cfg (ADD) to fman-rp
    pri=0, ce_num=0, ass=Unknown, fwd=Unknown, ret=Unknown
    protocol=6 use_source_port=0 is_closed=0
    ports[0] = 80
    ports[1] = 0
    ports[2] = 0
    ports[3] = 0
    ports[4] = 0
    ports[5] = 0
    ports[6] = 0
    ports[7] = 0
*Jun 17 15:51:14.864: FMANRP-WCCP: send out (0, 0, 0) wccp_ce_cfg (ADD) to fman-rp,
ce=90.20.1.2 ce_id=0.0.0.0 rtr_id=66.66.66.66 fwd_method=GRE obj_id=141
*Jun 17 15:51:29.846: FMANRP-WCCP: send out (0, 0, 0) wccp_svc_cfg (MODIFY) to fman-rp
    pri=0, ce_num=1, ass=Mask, fwd=GRE, ret=L2
    protocol=6 use_source_port=0 is_closed=0
    ports[0] = 80

```

```

        ports[1] = 0
        ports[2] = 0
        ports[3] = 0
        ports[4] = 0
        ports[5] = 0
        ports[6] = 0
        ports[7] = 0
*Jun 17 15:51:29.847: FMANRP-WCCP: send out (0, 0, 0) wccp_acl_begin to fman-rp
*Jun 17 15:51:29.886: FMANRP-WCCP: Service Group (0, 0, 0) send out ACL=WCCP_ACL_0x0, 64
ACEs to fman-rp
*Jun 17 15:51:29.886: FMANRP-WCCP: send out (0, 0, 0) wccp_acl_end to fman-rp

```

A WCCP service is removed from an interface:

```

*Jun 17 15:53:40.710: FMANRP-WCCP: send out (0, 0, 0) wccp_if_svc_bind (ADD) to fman-rp
if_handle=20 dir=IN

```

A WCCP service is removed from an interface:

```

*Jun 17 15:54:36.924: FMANRP-WCCP: send out (0, 0, 0) wccp_if_svc_bind (DELETE) to fman-rp
if_handle=20 dir=IN

```

A WCCP service group is unconfigured:

```

*Jun 17 15:55:13.117: FMANRP-WCCP: send out (0, 0, 0) wccp_ce_cfg (DELETE) to fman-rp,
ce=90.20.1.2 ce_id=0.0.0.0 rtr_id=0.0.0.0 fwd_method=Unknown obj_id=0
*Jun 17 15:55:13.128: FMANRP-WCCP: send out (0, 0, 0) wccp_svc_cfg (DELETE) to fman-rp
        pri=0, ce_num=0, ass=Unknown, fwd=Unknown, ret=Unknown
        protocol=0 use_source_port=0 is_closed=0
        ports[0] = 0
        ports[1] = 0
        ports[2] = 0
        ports[3] = 0
        ports[4] = 0
        ports[5] = 0
        ports[6] = 0
        ports[7] = 0

```

The following is sample output from the **debug platform software wccp detail** command:

```

Router# debug platform software wccp detail

```

WCCP service is configured:

```

*Jun 17 18:42:15.491: FMANRP-WCCP: create ce adjacency: CE = 90.20.1.2, fwd_method = GRE
oce= 0x30692230 adj = 0x306921C0 handle = 0x30692230 obj_id = 181
*Jun 17 18:42:30.472: FMANRP-WCCP: Converted adjacency (0x30692230), to ce_addr
(90.20.1.2)
*Jun 17 18:42:30.473: FMANRP-WCCP: Service Group (0, 0, 0) send out ACL=WCCP_ACL_0x0,
ACE=1, obj_id=181 PERMIT, srcopr 5, dstopr 3 to fman-rp
*Jun 17 18:42:30.473: FMANRP-WCCP: oce 0x30692230 adj 0x306921C0 handle 0x30692230

```

The debug messages appear for each access control entry (ACE) of the merged access control list (ACL) for the service group:

```

*Jun 17 18:42:30.487: FMANRP-WCCP: Converted adjacency (0x30692230), to ce_addr
(90.20.1.2)
*Jun 17 18:42:30.487: FMANRP-WCCP: Service Group (0, 0, 0) send out ACL=WCCP_ACL_0x0,
ACE=64, obj_id=181 PERMIT, srcopr 5, dstopr 3 to fman-rp
*Jun 17 18:42:30.487: FMANRP-WCCP: oce 0x30692230 adj 0x306921C0 handle 0x30692230

```

A WCCP service group is unconfigured:

```

*Jun 17 18:46:34.316: FMANRP-WCCP: (0 0 0) Delete ce = 90.20.1.2
*Jun 17 18:46:34.316: Failed to retrieve service group params while removing ce

```

The following is sample output from the **debug platform software wccp counters** command.

```
Router# debug platform software wccp counters
```

Statistics are collected for the first time on a WCCP-enabled interface:

```
*Jun 17 18:50:18.930: FMANRP-WCCP: Received wccp_if_stats intf 20, redirect(IN) 0 from fman-fp
```

The following debug messages are displayed every 10 seconds:

```
*Jun 17 18:51:18.929: FMANRP-WCCP: Received (0, 0, 0) svc_grp_stats from fman-fp
  unassigned_count = 0, dropped_closed_count = 0
  bypass_count = 0, bypass_failed_count = 0
  denied_count = 0, redirect_count = 0
  num_entries = 0
```

```
*Jun 17 18:51:18.929: FMANRP-WCCP: Received wccp_if_stats intf 20, redirect(IN) 0 from fman-fp
```

```
*Jun 17 18:51:28.929: FMANRP-WCCP: Received (0, 0, 0) svc_grp_stats from fman-fp
  unassigned_count = 0, dropped_closed_count = 0
  bypass_count = 0, bypass_failed_count = 0
  denied_count = 0, redirect_count = 0
  num_entries = 0
```

#### Related Commands

Command	Description
<b>clear ip wccp</b>	Removes WCCP statistics (counts) maintained on the router for a particular service.
<b>ip wccp</b>	Enables support of the specified WCCP service for participation in a service group.
<b>ip wccp check services all</b>	Enables all WCCP services.
<b>ip wccp outbound-acl-check</b>	Enables execution of ACL applied on the actual outgoing interface of a packet before a decision is taken to redirect a packet.
<b>ip wccp redirect</b>	Enables packet redirection on an outbound or inbound interface using WCCP.
<b>show platform software wccp</b>	Displays global statistics related to WCCP on Cisco ASR 1000 Series Routers.

# debug sbc alarm-filter

To configure the alarm types for which alarm logs must be generated, use the **debug sbc alarm-filter** command in the privileged EXEC mode. To unconfigure generation of alarm logs for a specified alarm type, use the **no** form of this command.

```
debug sbc sbc-name alarm-filter alarm-type
```

```
no debug sbc sbc-name alarm-filter alarm-type
```

## Syntax Description

<i>sbc-name</i>	Name of the SBC.
<b>alarm-filter</b> <i>alarm-type</i>	Specifies that logs must be generated for one of the following alarm types: <ul style="list-style-type: none"> <li>• <b>audit-congestion</b>—Call audit congestion.</li> <li>• <b>blacklist-alert</b>—Blacklist alert.</li> <li>• <b>blacklist-event</b>—Blacklist event.</li> <li>• <b>h248</b>—H248 connection failed.</li> <li>• <b>handled-exception</b>—Handled exception.</li> <li>• <b>routing-component</b>—Routing component set not active.</li> <li>• <b>routing-config</b>—Routing config set not active.</li> <li>• <b>routing-invalid</b>—Invalid routing configuration.</li> <li>• <b>sip-congestion</b>—Session Initiation Protocol (SIP) congestion detection.</li> <li>• <b>sip-peer</b>—SIP peer unavailable.</li> <li>• <b>vqm</b>—Voice Quality metrics (VQM) threshold exceeded.</li> </ul>

## Command Default

The default is that alarm logs are generated for all alarm types.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Run this command for each alarm type for which you want logs to be generated. You can use the **show debugging** command to display the debugging settings created by running the **debug sbc alarm-log-level** command.

## Examples

The following example shows how the **debug sbc alarm-filter** command is used to configure the generation of alarm logs for call audit congestion alarms:



```
Router# debug sbc MySbc alarm-filter audit-congestion
```

The following example shows how the **show debugging** command displays the configuration settings created by running the **debug sbc alarm-filter** command. For example:

```
Router# show debugging
```

```
SBC:
  SBC alarm filter 1 : AUDIT CONGESTION
```

#### Related Commands

Command	Description
<b>debug sbc alarm-log-level</b>	Specifies the output mode for and the alarm severity level at which alarms must be logged.
<b>sbc dump-alarms</b>	Moves alarm logs from the buffer to a file system.
<b>sbc periodic-dump-alarms</b>	Configures periodic movement of alarm logs from the buffer to a file system.
<b>show debugging</b>	Displays information about the types of debugging that are enabled for the router.

# debug sbc alarm-log-level

To configure the output mode and the alarm severity level at which alarms must be logged, use the **debug sbc alarm-log-level** command in the privileged EXEC mode. To unconfigure the display and storage of alarm logs, use the **no** form of this command.

```
debug sbc sbc-name alarm-log-level [buffer | console] severity-level
```

```
no debug sbc sbc-name alarm-log-level [buffer | console]
```

## Syntax Description

<i>sbc-name</i>	Name of the SBC.
<b>alarm-log-level</b>	Specifies that logs must be displayed or stored for alarms of the specified alarm severity level.
<b>buffer</b>	Specifies that alarm logs must be stored in the buffer.
<b>console</b>	Specifies that logging output must be displayed on the console.
<i>severity-level</i>	Alarm severity level for which logs must be generated. The range is from 0 to 100. For alarm logs stored in the buffer, the default is 40. For alarm logs displayed on the console, the default is 80. To disable logging, set the value to 100. If you set the value to 0, logs are generated for all levels of alarm severity.

## Command Default

This command applies to all the alarms for which you configure logging by running the **debug sbc alarm-filter** command.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

If you specify **buffer** as the output mode for the alarm logs, note that the logs are moved to a file in the specified file system when the capacity of the buffer is exceeded. The size of a single log file created on the file system cannot exceed 2 MB. When the size of a particular log file reaches 2 MB, a new file is created and logging output is stored in the new file. Use the **show debugging** command to display the debug settings created by running the **debug sbc alarm-log-level** command.

## Examples

In the following example, the **debug sbc alarm-log-level** command is run twice. The first run of this command is used to specify that logs must be generated for alarms that are of severity 20 or higher and that these logs must be stored in the buffer. The second run of the command is used to specify that logs must be generated for alarms that are of severity 40 or higher and that these logs must be displayed on the console.

```
Router# debug sbc MySbc alarm-log-level buffer 20
Router# debug sbc MySbc alarm-log-level console 40
```

The **show debugging** command shows the configuration settings created by running the **debug sbc alarm-log-level** command. For example:

```
Router# show debugging

SBC:
  SBC buffer alarm-log-level : 20
  SBC console alarm-log-level : 40
```

#### Related Commands

Command	Description
<b>debug sbc alarm-filter</b>	Specifies the alarm types for which alarm logs must be generated.
<b>sbc dump-alarms</b>	Moves alarm logs from the buffer to a file system.
<b>sbc periodic-dump-alarms</b>	Configures periodic movement of alarm logs from the buffer to a file system.
<b>show debugging</b>	Displays information about the types of debugging that are enabled for the router.

# debug sbc asr log-level filter

To set the problem determination (PD) log level at which filtering occurs, use the **debug sbc asr log-level filter** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

```
debug sbc asr log-level filter level
```

```
no debug sbc asr log-level filter level
```

## Syntax Description

level	The level to set. Range is 0 to 100. The default is 50. 0 applies filtering to all PD logs. Setting a filter log level of 60 will only apply filtering to logs 60 and above. For example, if you set the console log level to 100, set a SIP filter, and set the filter log level to 60, then only logs matching the SIP filter <i>and</i> above level 60 will output to the screen. Logs with severity greater than the specified threshold, matching the include/exclude filter set, or the log group filter are output regardless of the configured unconditional log levels for the buffer, file and console output streams. They are output to all three of those streams.
-------	--

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Logs with severity greater than the specified threshold, matching the include/exclude filter set, or the log group filter are output regardless of the configured unconditional log levels for the buffer, file and console output streams. They are output to all three of those streams.

Use the **show debug** command to see debug information.

## Examples

The following examples show various output for this command:

```
Router# show debug
SBC: SBC buffer log-level is 100
SBC console log-level is 100 SBC filter log-level is 2
SBC log filter 1 - combination of: SIP components
```

```
Router# debug sbc asr log-level ?
```

```

buffer Buffer log console
Console log filter
Filter log

```

```

Router# debug sbc asr log-level filter ?
<0-100> Filter log level (default 50)

```

### Related Commands

Command	Description
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc correlation-logs filter

To enable the correlation-logs filter, use the **debug sbc correlation-logs filter** command in the privileged EXEC mode. To disable the correlation-logs filter, use the **no** form of this command.

```
debug sbc sbc-name correlation-logs filter filter-name [pdtrc-log-level value]
```

```
no debug sbc sbc-name correlation-logs filter filter-name
```

## Syntax Description

<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
<i>filter-name</i>	Name of the filter used for filtering the correlation logs.
<b>pdtrc-log-level</b> <i>value</i>	(Optional) Specifies the value of the pdtrc log level. The range is from 0 to 100. The default is 60.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.5.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Use the **show debugging** command to display the debug logs, filters, and log levels.

## Examples

The following example shows the various filters available for filtering the correlation logs:

```
Router# debug sbc test correlation-logs filter ?
  adjacency      Adjacency,matching calls to or from this adjacency
  dn             Dialed/Dialing number,matching calls to or from this number
  remote-signalling-address Remote signalling address matching to or from this address
  sip-uri       SIP-URI,matching calls to or from this uri
  vrf           VRF name
```

The following example shows the filtering of correlation logs based on the adjacency parameter:

```
Router# debug sbc test correlation-logs filter adjacency abc
  Debugging filter log-level set to default level 60

Router# show debugging
  SBC correlator filter Adjacency name is abc
  IpsTracing is enabled
```

The following example shows the filtering of correlation logs based on the remote signalling address parameter:

```
Router# debug sbc test correlation-logs filter vrf new ipv4 rsa 192.0.2.1 pdtrc-log-level
70
    Debugging filter log-level set to default level 60

Router# show debugging
SBC correlator Filter Remote signalling-address ipv4 address is 192.0.2.1
SBC correlator Filter VRF is new with Vpn(id) = 3
Pd loglevel is 70
IpsTracing is enabled
SBC correlator Filter SIP-URI is 9.0.0.0
Pd loglevel is 0
IpsTracing is enabled
```

#### Related Commands

Command	Description
<b>debug sbc pd log-level</b>	Sets the file logging level.
<b>show debugging</b>	Displays the debug logs, filters, and log levels.

# debug sbc errors

To debug sbc service errors, use the **debug sbc errors** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc errors*

*no debug sbc errors*

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Exec (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **show debug** command to see debug information.

**Examples** The following command turns on sbc error debugging:

```
Router# debug sbc errors
Router# 2007 May 13 04:24:50.902717 sbc:
(ctx:0)hmstub_proc_rcv_hb_message:test_rcv_hb_failed = 1110000
2007 May 13 04:29:50.960623 sbc: (ctx:0)hmstub_proc_rcv_hb_message:test_rcv_hb_failed =
1112000
2007 May 13 04:34:50.960631 sbc: (ctx:0)hmstub_proc_rcv_hb_message:test_rcv_hb_failed =
1114000
```

Related Commands	Command	Description
	<b>debug sbc filter control</b>	Enables console logging based on a number of filters.
	<b>debug sbc ips</b>	Enables IPS tracing.
	<b>debug sbc log-level console</b>	Sets the console logging level.
	<b>debug sbc log-level file</b>	Sets the file logging level.
	<b>debug sbc events</b>	Enables debugging of sbc service events.
	<b>debug sbc ha</b>	Enables debugging of sbc high availability.
	<b>debug sbc info</b>	Enables debugging of sbc services information.
	<b>debug sbc nbase</b>	Enables debugging of sbc services nbase.





# debug sbc events

To debug sbc service events, use the **debug sbc events** command in privileged EXEC mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc events*

**no debug sbc events**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **show debug** command to see debug information.

**Examples** The following command turns on debugging for sbc events:

```
Router# debug sbc events
```

Related Commands	Command	Description
	<b>debug sbc filter control</b>	Enables console logging based on a number of filters.
	<b>debug sbc ips</b>	Enables IPS tracing.
	<b>debug sbc log-level console</b>	Sets the console logging level.
	<b>debug sbc log-level file</b>	Sets the file logging level.
	<b>debug sbc errors</b>	Enables debugging of sbc service errors.
	<b>debug sbc ha</b>	Enables debugging of sbc high availability.
	<b>debug sbc info</b>	Enables debugging of sbc services information.
	<b>debug sbc nbase</b>	Enables debugging of sbc services nbase.

## debug sbc filter

To enable logging based on a number of filters, use the **debug sbc filter** command in privileged EXEC mode. To disable logging based on these filters, use the **no** form of this command.

```
debug sbc {sbc-name} filter [adjacency {adj-name}] [bill {billing-id}] [ipv4 {ipv4-address}]
[ipv6 {ipv6-address}] [number {number}] [billing] [call] [media] [overview] [protocol] [bm]
| cac | control | h323 | icc | radius | routing | sip | mgm]
```

```
no debug sbc {sbc-name} filter [adjacency {adj-name}] [bill {billing-id}] [ipv4 {ipv4-address}]
[ipv6 {ipv6-address}] [number {number}] [billing] [call] [media] [overview] [protocol] [bm]
| cac | control | h323 | icc | radius | routing | sip | mgm]
```

### Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service.
<b>adjacency</b>	Output of logs relating to this adjacency.
<i>adj-name</i>	Name of the adjacency.
<b>bill</b>	Log output of calls with a specified billing ID.
<i>billing-id</i>	Billing ID.
<b>ipv4</b>	Output logs that include the IPv4 IP address.
<i>ipv4-address</i>	IPv4 IP address.
<b>ipv6</b>	Output logs that include the IPv6 IP address.
<i>ipv6-address</i>	IPv6 IP address.
<b>number</b>	Output logs of calls with a specified number.
<i>number</i>	Either the caller number or dialed number.
<b>billing</b>	Logs about billing events.
<b>call</b>	Logs about call events.
<b>media</b>	Logs about media events.
<b>overview</b>	Logs showing the flow of control through the session border controller (SBC) components.
<b>protocol</b>	Logs showing protocol messages.
<b>bm</b>	Logs from the Bandwidth Manager (BM) component.
<b>cac</b>	Logs from the Call Admission Control (CAC) components.
<b>control</b>	Logs from the H.248 controller components.
<b>h323</b>	Logs from the H.323 components.
<b>icc</b>	Logs from the Interworking Call Control (ICC) components.
<b>radius</b>	Logs from the RADIUS components.
<b>routing</b>	Logs from the routing components.
<b>sip</b>	Logs from the Session Initiation Protocol (SIP) components.
<b>mgm</b>	Logs from the Media Gateway Manager (MGM) component.

### Command Default

Debugging is off.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** You can specify any number of optional keywords, but each keyword can only be specified once. At least one keyword must be specified for the **debug sbc filter** command. You can issue multiple **debug sbc filter** commands.

**Note**

The debug logs are only output if the appropriate filter keywords have been specified.

The keywords are composed of the following types of filters:

- String filters—Allow the user to turn on logs about common SBC objects such as adjacencies. An object matches the string filter if the object exactly matches the string or the prefix matches the string.

String filters include the following keywords:

- **adjacency** {*adj-name*}
- **bill** {*billing-id*}
- **ipv4** {*ipv4-address*}
- **ipv6** {*ipv6-address*}
- **number** {*number*}

- Component filters—Turn on logs from individual components (or groups of components) within the SBC service. Only one component filter may be specified per **debug sbc filter** command.

Component filters include the following keywords:

**bm, cac, control, h323, icc, radius, routing, sip, mgm**

- Cross-SBC filters—Turn on logs across all components of the SBC service.

Cross-SBC filters include the following keywords:

**billing, call, media, overview, protocol**

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support personnel. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

**Examples**

The following example shows all debug logs for the H.248 control channel to the SBE on an SBC called “mySbc”:

```
Router# debug sbc mySbc filter control
```

The following example shows all debug logs relating to media flows on an SBC called “mySbc”:

```
Router# debug sbc mySbc filter media
```

The following example shows all debug logs relating to media flows with a source or destination address of 10.0.1.1 on an SBC called “mySbc” including output logs for the specified IPv4 IP address:

```
Router# debug sbc mySbc filter media ipv4 10.0.1.1
```

The following example shows that if you want to show all debug logs that relate to media flowing to and from 10.0.1.1 *or* 10.0.1.2, you must issue the following two commands:

```
Router# debug sbc mySbc filter media ipv4 10.0.1.1
```

```
Router# debug sbc mySbc filter media ipv4 10.0.1.2
```

**Related Commands**

Command	Description
<b>debug sbc log-level</b>	Sets the debug logging level for logging to the cyclic buffer or to the system logger.
<b>logging buffered</b>	Logs messages to an internal buffer.
<b>logging console</b>	Logs messages to console connections.
<b>logging host</b>	Logs messages to a syslog server host.
<b>logging monitor</b>	Limits messages logged to the terminal lines (monitors) based on severity.
<b>logging on</b>	Enables logging of system messages.
<b>logging synchronous</b>	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

# debug sbc filter billing\_id

To print log entries to the console and file based on a billing\_id context, use the **debug sbc filter billing\_id** command in privileged EXEC mode. To disable this form of debugging, use the **no** form of this command.

```
debug sbc sbc-name filter billing_id billing_id
```

```
no debug sbc sbc-name filter billing_id billing_id
```

## Syntax Description

<i>sbc-name</i>	This is the name of the SBC service.
<i>billing_id</i>	The billing ID to be filtered.

## Command Default

None.

## Command Modes

privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Use the **show debug** command to see debug information.

## Examples

The following command prints log entries to the console and file based on a billing\_id context:

```
Router# debug sbc test-sbc filter billing_id abc
Router# 2008 May 20 17:08:36.084825 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:
```

```

SBC inter-process logging is off
SBC log filter 0:
Billing ID : abc
```

## Related Commands

Command	Description
<b>debug sbc filter adjacency</b>	Prints log entries to the console and file based on an adjacency context.

<b>Command</b>	<b>Description</b>
<b>debug sbc filter ipv4</b>	Prints print log entries to the console and file based on an ipv4 address context.
<b>debug sbc filter number</b>	Prints log entries to the console and file based on a number context.

# debug sbc filter bm

To print log entries to the console and file from the bandwidth manager component group, use the **debug sbc filter bm** command in privileged EXEC mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc sbc-name filter bm*

*no debug sbc sbc-name filter bm*

## Syntax Description

*sbc-name* This is the name of the SBC service.

## Command Default

None.

## Command Modes

privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Use the **show debug** command to see debug information.

## Examples

The following command prints log entries to the console and file from the bandwidth manager component group:

```
Router# debug sbc test-sbc filter bm
Router# 2008 May 20 17:36:10.924908 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:
```

```
SBC inter-process logging is off
SBC log filter 1:
  BM components
```

## Related Commands

Command	Description
<b>debug sbc filter cac</b>	Prints log entries to the console and file from the call admission control (CAC) component group.
<b>debug sbc filter control</b>	



<b>Command</b>	<b>Description</b>
<b>debug sbc filter h323</b>	Prints log entries to the console and file from the h323 component group.
<b>debug sbc filter hm</b>	Prints log entries to the console and file from the hardware manager (hm) component group.
<b>debug sbc filter icc</b>	Prints log entries to the console and file from the Internetworking Call Control (ICC) component group.
<b>debug sbc filter mgm</b>	Prints log entries to the console and file from the media gateway manager (MGM) component group.
<b>debug sbc filter radius</b>	Prints log entries to the console and file from the RADIUS component group.
<b>debug sbc filter routing</b>	Prints log entries to the console and file from the routing component group.
<b>debug sbc filter sip</b>	Prints log entries to the console and file from the SIP component group.

# debug sbc filter cac

To print log entries to the console and file from the call admission control (CAC) component group, use the **debug sbc filter cac** command in privileged EXEC mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc sbc-name filter cac*

*no debug sbc sbc-name filter cac*

## Syntax Description

*sbc-name* This is the name of the SBC service.

## Command Default

None.

## Command Modes

privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Use the **show debug** command to see debug information.

## Examples

The following command prints log entries to the console and file from the CAC component group:

```
Router# debug sbc test-sbc filter cac
Router# 2008 May 20 17:39:18.748447 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:
```

```
SBC inter-process logging is off
SBC log filter 1:
CAC components
```

## Related Commands

Command	Description
<b>debug sbc filter bm</b>	Prints log entries to the console and file from the bandwidth manager component group.
<b>debug sbc filter control</b>	
<b>debug sbc filter h323</b>	Prints log entries to the console and file from the h323 component group.

<b>Command</b>	<b>Description</b>
<b>debug sbc filter hm</b>	Prints log entries to the console and file from the hardware manager (hm) component group.
<b>debug sbc filter icc</b>	Prints log entries to the console and file from the Internetworking Call Control (ICC) component group.
<b>debug sbc filter mgm</b>	Prints log entries to the console and file from the media gateway manager (MGM) component group.
<b>debug sbc filter radius</b>	Prints log entries to the console and file from the RADIUS component group.
<b>debug sbc filter routing</b>	Prints log entries to the console and file from the routing component group.
<b>debug sbc filter sip</b>	Prints log entries to the console and file from the SIP component group.

# debug sbc filter call

To print log entries to the console and file from the call product group, use the **debug sbc filter call** command in privileged EXEC mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc sbc-name filter call*

*no debug sbc sbc-name filter call*

## Syntax Description

*sbc-name* This is the name of the SBC service.

## Command Default

None.

## Command Modes

privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Use the **show debug** command to see debug information.

## Examples

The following command prints log entries to the console and file from the call product group:

```
Router# debug sbc test-sbc filter call
Router# 2008 May 20 17:43:16.078547 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:
```

```
SBC inter-process logging is off
SBC log filter 0:
  Call Logging Group
```

## Related Commands

Command	Description
<b>debug sbc filter billing</b>	Prints log entries to the console and file from the billing product group.
<b>debug sbc filter media</b>	Prints log entries to the console and file from the media product group.

<b>Command</b>	<b>Description</b>
<b>debug sbc filter overview</b>	Prints log entries to the console and file from the overview product group.
<b>debug sbc filter protocol</b>	Prints log entries to the console and file from the protocol product group.

# debug sbc filter (session border controller)

To enable logging based on a number of filters, use the **debug sbc filter** command in privileged EXEC mode. To disable logging based on these filters, use the **no** form of this command.

```
debug sbc {sbc-name} filter [adjacency {adj-name}] [bill {billing-id}] [ipv4 {ipv4-address}] [ipv6 {ipv6-address}] [number {number}] [billing] [call] [media] [overview] [protocol] [bm | cac | control | h323 | icc | radius | routing | sip | mgm]
```

```
no debug sbc {sbc-name} filter [adjacency {adj-name}] [bill {billing-id}] [ipv4 {ipv4-address}] [ipv6 {ipv6-address}] [number {number}] [billing] [call] [media] [overview] [protocol] [bm | cac | control | h323 | icc | radius | routing | sip | mgm]
```

## Syntax Description

sbc-name	Name of the Session Border Controller (SBC) service.
adjacency	Output of logs relating to this adjacency.
adj-name	Name of the adjacency.
bill	Log output of calls with a specified billing ID.
billing-id	Billing ID.
ipv4	Output logs that include the IPv4 IP address.
ipv4-address	IPv4 IP address.
<b>ipv6</b>	Output logs that include the IPv6 IP address.
<b>ipv6-address</b>	IPv6 IP address.
number	Output logs of calls with a specified number.
number	Either the caller number or dialed number.
billing	Logs about billing events.
call	Logs about call events.
media	Logs about media events.
overview	Logs showing the flow of control through the Session Border Controller (SBC) components.
protocol	Logs showing protocol messages.
bm	Logs from the Bandwidth Manager (BM) component.
cac	Logs from the Call Admission Control (CAC) components.
control	Logs from the H.248 controller components.
h323	Logs from the H.323 components.
icc	Logs from the Interworking Call Control (ICC) components.
radius	Logs from the RADIUS components.
routing	Logs from the routing components.
sip	Logs from the Session Initiation Protocol (SIP) components.
mgm	Logs from the Media Gateway Manager (MGM) component.

## Command Default

Debugging is off.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** You can specify any number of optional keywords, but each keyword can only be specified once. At least one keyword must be specified for the **debug sbc filter** command. You can issue multiple **debug sbc filter** commands.

**Note**

The debug logs are only output if the appropriate filter keywords have been specified.

The keywords are composed of the following types of filters:

- String filters—Allow the user to turn on logs about common SBC objects such as adjacencies. An object matches the string filter if the object exactly matches the string or the prefix matches the string.

String filters include the following keywords:

- **adjacency** {*adj-name*}
- **bill** {*billing-id*}
- **ipv4** {*ipv4-address*}
- **ipv6** {*ipv6-address*}
- **number** {*number*}

- Component filters—Turn on logs from individual components (or groups of components) within the SBC service. Only one component filter may be specified per **debug sbc filter** command.

Component filters include the following keywords:

**bm, cac, control, h323, icc, radius, routing, sip, mgm**

- Cross-SBC filters—Turn on logs across all components of the SBC service.

Cross-SBC filters include the following keywords:

**billing, call, media, overview, protocol**

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support personnel. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

## Examples

The following example shows all debug logs for the H.248 control channel to the SBE on an SBC called “mySbc”:

```
Router# debug sbc mySbc filter control
```

The following example shows all debug logs relating to media flows on an SBC called “mySbc”:

```
Router# debug sbc mySbc filter media
```

The following example shows all debug logs relating to media flows with a source or destination address of 10.0.1.1 on an SBC called “mySbc” including output logs for the specified IPv4 IP address:

```
Router# debug sbc mySbc filter media ipv4 10.0.1.1
```

The following example shows that if you want to show all debug logs that relate to media flowing to and from 10.0.1.1 or 10.0.1.2, you must issue the following two commands:

```
Router# debug sbc mySbc filter media ipv4 10.0.1.1
Router# debug sbc mySbc filter media ipv4 10.0.1.2
```

The following command prints log entries to the console and file based on an adjacency context:

```
Router# debug sbc test-sbc filter adjacency sip-1
Router# 2008 May 20 15:08:50.114277 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 0:
Adjacency : sip-1
```

Filter output:

```
SBC/SIP: **** Overview 0x5001 - 108 (0000) **** 00001100000000000000000100
000000
SBC/SIP: (vpsuafsm.c 914) at 18:26:11, 20 May 2008 (82249142 ms)
SBC/SIP: << INVITE
SBC/SIP: Adj=sip-1,DN=service,CN=sipp
```

The following command prints log entries to the console and file from the billing product group:

```
Router# debug sbc test-sbc filter billing
Router# 2008 May 20 17:14:51.758095 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 0:
Billing Logging Group
```

The following command prints log entries to the console and file from the bandwidth manager component group:

```
Router# debug sbc test-sbc filter bm
Router# 2008 May 20 17:36:10.924908 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```



SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 1:
  BM components
```

The following command prints log entries to the console and file from the ICC component group:

```
Router# debug sbc test-sbc filter icc
Router# 2008 May 20 17:52:15.801682 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 1:
  ICC components
```

Log:

```
SBC/ICC: **** UNEXPECTED 0x1504 - 15 (0001) **** 00000000000000000000000000000000
000000
SBC/ICC: (dblblack.c 253) at 18:25: 3, 20 May 2008 (82180687 ms)
SBC/ICC: The Dynamic Blacklisting component is blacklisting a source.
SBC/ICC: Subfamily = 0X0000000C
SBC/ICC: Cause = 1
SBC/ICC: Time period = 600000 ms
SBC/ICC:
SBC/ICC: Event=["Routing failure" VPN=0X00000000 10.10.1.1]
```

The following command prints log entries to the console and file from the h323 component group:

```
Router# debug sbc test-sbc filter h323
Accessing H323
Completed TNRPC : H323
2008 May 20 17:45:22.058599 sbc: (ctx:0) SBC: New log filter enabled.
```

BC Daemon:

```
SBC inter-process logging is off
SBC log filter 1:
  H323 components
```

The following command prints log entries to the console and file from the ICC component group:

```
Router# debug sbc test-sbc filter icc
Router# 2008 May 20 17:52:15.801682 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 1:
  ICC components
```

Log:

```
SBC/ICC: **** UNEXPECTED 0x1504 - 15 (0001) **** 00000000000000000000000000000000
000000
SBC/ICC: (dblblack.c 253) at 18:25: 3, 20 May 2008 (82180687 ms)
SBC/ICC: The Dynamic Blacklisting component is blacklisting a source.
```

```
SBC/ICC: Subfamily = 0X0000000C
SBC/ICC: Cause = 1
SBC/ICC: Time period = 600000 ms
SBC/ICC:
SBC/ICC: Event=["Routing failure" VPN=0X00000000 10.10.1.1]
```

The following command prints log entries to the console and file based on an ipv4 address context:

```
Router# debug sbc test-sbc filter ipv4 10.10.10.1
Router# 2008 May 20 17:12:16.128077 sbc: (ctx:0)Len IPV4: 10
2008 May 20 17:12:16.128159 sbc: (ctx:0)IPV4: 10.10.10.1
2008 May 20 17:12:16.128239 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:

SBC inter-process logging is off
SBC log filter 0:
IPv4: 10.10.10.1
2008 May 20 17:12:18.371175 sbc: (ctx:0)Filter IPv4 Len: 10
2008 May 20 17:12:18.371256 sbc: (ctx:0)Filter IPv4 string: 10.10.10.1
```

The following command prints log entries to the console and file from the media product group:

```
Router# debug sbc test-sbc filter media
Router# 2008 May 20 17:57:59.071693 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:

SBC inter-process logging is off
SBC log filter 0:
Media Logging Group
```

The following command prints log entries to the console and file from the media product group:

```
Router# debug sbc test-sbc filter media
Router# 2008 May 20 17:57:59.071693 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:

SBC inter-process logging is off
SBC log filter 0:
Media Logging Group
```

The following command prints log entries to the console and file from the media product group:

```
Router# debug sbc test-sbc filter media
Router# 2008 May 20 17:57:59.071693 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:
```

```
SBC inter-process logging is off
SBC log filter 0:
  Media Logging Group
```

The following command prints log entries to the console and file from the media product group:

```
Router# debug sbc test-sbc filter media
Router# 2008 May 20 17:57:59.071693 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 0:
  Media Logging Group
```

The following command prints log entries to the console and file from the MGM component group:

```
Router# debug sbc test-sbc filter mgm
Router# 2008 May 20 18:24:17.552046 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 1:
  MGM components
```

Log:

```
SBC/MGM: << Gate allocate req BillingID (sideA) 48331709 20202020 20202030 000
00000 00000000 00001064 BillingID (sideB) 48331709 20202020 20202030 00000000 0
0000000 00001063
```

The following command prints log entries to the console and file based on a number context:

```
Router# debug sbc test-sbc filter number 1234
Router# 2008 May 20 17:13:26.138304 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 0:
Number : 1234
```

The following command prints log entries to the console and file based on a number context:

```
Router# debug sbc test-sbc filter number 1234
Router# 2008 May 20 17:13:26.138304 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 0:
Number: 1234
```

The following command prints log entries to the console and file from the overview product group:

```
Router# debug sbc test-sbc filter overview
Router# 2008 May 20 18:25:54.811973 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 0:
  Overview Logging Group
```

Log:

```
SBC/SIP: **** Operational 0x3801 - 43 (0001) **** 00001110000000000000000000
000000
SBC/SIP: (siphsrcv.c 45) at 18:26:37, 20 May 2008 (82274720 ms)
SBC/SIP: SIP message received:
SBC/SIP: INVITE sip:service@10.10.1.110:5060 SIP/2.0^M
SBC/SIP: Via: SIP/2.0/UDP 10.10.1.3:5060;branch=z9hG4bK-28511-243-0^M
SBC/SIP: From: sipp <sip:sipp@10.10.1.3:5060>;tag=28511SIPpTag00243^M
SBC/SIP: To: sut <sip:service@10.10.1.110:5060>^M
SBC/SIP: Call-ID: 243-28511@10.10.1.3^M
SBC/SIP: CSeq: 1 INVITE^M
SBC/SIP: Contact: sip:sipp@10.10.1.3:5060^M
SBC/SIP: Max-Forwards: 70^M
SBC/SIP: Subject: Performance Test^M
SBC/SIP: Content-Type: application/sdp^M
SBC/SIP: Content-Length: 129^M
SBC/SIP: ^M
SBC/SIP: v=0^M
SBC/SIP: o=user1 53655765 2353687637 IN IP4 10.10.1.3^M
SBC/SIP: s=-^M
SBC/SIP: c=IN IP4 10.10.1.3^M
SBC/SIP: t=0 0^M
SBC/SIP: m=audio 6000 RTP/AVP 0^M
SBC/SIP: a=rtpmap:0 PCMU/8000^M
```

The following command prints log entries to the console and file from the overview product group:

```
Router# debug sbc test-sbc filter overview
Router# 2008 May 20 18:25:54.811973 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:

```
Router# show debug
```

SBC Daemon:

```
SBC inter-process logging is off
SBC log filter 0:
  Overview Logging Group
```

Log:

```
SBC/SIP: **** Operational 0x3801 - 43 (0001) **** 00001110000000000000000000
000000
SBC/SIP: (siphsrcv.c 45) at 18:26:37, 20 May 2008 (82274720 ms)
```

```

SBC/SIP: SIP message received:
SBC/SIP: INVITE sip:service@10.10.1.110:5060 SIP/2.0^M
SBC/SIP: Via: SIP/2.0/UDP 10.10.1.3:5060;branch=z9hG4bK-28511-243-0^M
SBC/SIP: From: sipp <sip:sipp@10.10.1.3:5060>;tag=28511SIPpTag00243^M
SBC/SIP: To: sut <sip:service@10.10.1.110:5060>^M
SBC/SIP: Call-ID: 243-28511@10.10.1.3^M
SBC/SIP: CSeq: 1 INVITE^M
SBC/SIP: Contact: sip:sipp@10.10.1.3:5060^M
SBC/SIP: Max-Forwards: 70^M
SBC/SIP: Subject: Performance Test^M
SBC/SIP: Content-Type: application/sdp^M
SBC/SIP: Content-Length: 129^M
SBC/SIP: ^M
SBC/SIP: v=0^M
SBC/SIP: o=user1 53655765 2353687637 IN IP4 10.10.1.3^M
SBC/SIP: s=-^M
SBC/SIP: c=IN IP4 10.10.1.3^M
SBC/SIP: t=0 0^M
SBC/SIP: m=audio 6000 RTP/AVP 0^M
SBC/SIP: a=rtpmap:0 PCMU/8000^M

```

The following command prints log entries to the console and file from the protocol product group:

```

Router# debug sbc test-sbc filter protocol
Router# 2008 May 20 18:28:13.622095 sbc: (ctx:0) SBC: New log filter enabled.
.

```

The following command shows debugging information:

```
Router# show debug
```

```
SBC Daemon:
```

```

SBC inter-process logging is off
SBC log filter 0:
  Protocol Logging Group

```

```
Router#
```

```
Log:
```

```

SBC/SIP: **** Operational 0x3801 - 43 (0001) **** 00001110000000000000000000
000000
SBC/SIP: (siphsrcv.c 45) at 18:29: 1, 20 May 2008 (82418949 ms)
SBC/SIP: SIP message received:
SBC/SIP: INVITE sip:service@10.10.1.110:5060 SIP/2.0^M
SBC/SIP: Via: SIP/2.0/UDP 10.10.1.3:5060;branch=z9hG4bK-28511-259-0^M
SBC/SIP: From: sipp <sip:sipp@10.10.1.3:5060>;tag=28511SIPpTag00259^M
SBC/SIP: To: sut <sip:service@10.10.1.110:5060>^M
SBC/SIP: Call-ID: 259-28511@10.10.1.3^M
SBC/SIP: CSeq: 1 INVITE^M
SBC/SIP: Contact: sip:sipp@10.10.1.3:5060^M
SBC/SIP: Max-Forwards: 70^M
SBC/SIP: Subject: Performance Test^M
SBC/SIP: Content-Type: application/sdp^M
SBC/SIP: Content-Length: 129^M
SBC/SIP: ^M
SBC/SIP: v=0^M
SBC/SIP: o=user1 53655765 2353687637 IN IP4 10.10.1.3^M
SBC/SIP: s=-^M
SBC/SIP: c=IN IP4 10.10.1.3^M
SBC/SIP: t=0 0^M
SBC/SIP: m=audio 6000 RTP/AVP 0^M
SBC/SIP: a=rtpmap:0 PCMU/8000^M

```

The following command prints log entries to the console and file from the RADIUS component group:

```
Router# debug sbc test-sbc filter radius
Router# 2008 May 20 18:33:02.845280 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:  
Router# **show debug**

```
SBC Daemon:

SBC inter-process logging is off
SBC log filter 1:
  Radius components
```

The following command prints log entries to the console and file from the routing component group:

```
Router# debug sbc test-sbc filter routing
Router# 2008 May 20 18:36:38.995736 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:  
Router# **show debug**

```
SBC Daemon:

SBC inter-process logging is off
SBC log filter 1:
  Routing components

Log:
SBC/ROUTING:Number validation begins.
SBC/ROUTING:SBC Index = 0X00000001
SBC/ROUTING:Config set Index = 0X00000003
SBC/ROUTING:Input Called Address Type = 0X00030003
SBC/ROUTING:Input Called Address = CE
SBC/ROUTING:mwCallIccIndex=2909
```

The following command prints log entries to the console and file from the SIP component group:

```
Router# debug sbc test-sbc filter sip
Router# 2008 May 20 18:38:43.795675 sbc: (ctx:0) SBC: New log filter enabled.
```

The following command shows debugging information:  
Router# **show debug**

```
SBC Daemon:

SBC inter-process logging is off
SBC log filter 1:
  SIP components

Log:
SBC/SIP: **** Operational 0x3801 - 43 (0001) **** 00001110000000000000000000
000000
SBC/SIP: (siphsrcv.c 45) at 18:39:19, 20 May 2008 (83037087 ms)
SBC/SIP: SIP message received:
SBC/SIP: INVITE sip:service@10.10.1.110:5060 SIP/2.0^M
SBC/SIP: Via: SIP/2.0/UDP 10.10.1.3:5060;branch=z9hG4bK-28511-1002-0^M
SBC/SIP: From: sipp <sip:sipp@10.10.1.3:5060>;tag=28511SIPpTag001002^M
SBC/SIP: To: sut <sip:service@10.10.1.110:5060>^M
SBC/SIP: Call-ID: 1002-28511@10.10.1.3^M
SBC/SIP: CSeq: 1 INVITE^M
SBC/SIP: Contact: sip:sipp@10.10.1.3:5060^M
SBC/SIP: Max-Forwards: 70^M
SBC/SIP: Subject: Performance Test^M
```

```

SBC/SIP: Content-Type: application/sdp^M
SBC/SIP: Content-Length: 129^M
SBC/SIP: ^M
SBC/SIP: v=0^M
SBC/SIP: o=user1 53655765 2353687637 IN IP4 10.10.1.3^M
SBC/SIP: s=-^M
SBC/SIP: c=IN IP4 10.10.1.3^M
SBC/SIP: t=0 0^M
SBC/SIP: m=audio 6000 RTP/AVP 0^M
SBC/SIP: a=rtpmap:0 PCMU/8000^M

```

## Related Commands

Command	Description
<b>debug sbc log-level</b>	Sets the debug logging level for logging to the cyclic buffer or to the system logger.
<b>logging buffered</b>	Logs messages to an internal buffer.
<b>logging console</b>	Logs messages to console connections.
<b>logging host</b>	Logs messages to a syslog server host.
<b>logging monitor</b>	Limits messages logged to the terminal lines (monitors) based on severity.
<b>logging on</b>	Enables logging of system messages.
<b>logging synchronous</b>	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

# debug sbc ha

To turn on debugging for Session Border Controller high availability, use the *debug sbc ha* command in privileged EXEC mode. To disable this form of debugging, use the **no** form of this command.

```
debug sbc ha
```

```
no debug sbc ha
```

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **show debug** command to see debug information.

**Examples** The following command turns on debugging for sbc high availability:

```
Router# debug sbc ha
Router#
2007 May 13 06:04:51.504671 sbc: (ctx:0)hmstub_send_hb: test_send_hb OK 1150000
```

Related Commands	Command	Description
	<b>debug sbc filter control</b>	Enables console logging based on a number of filters.
	<b>debug sbc ips</b>	Enables IPS tracing.
	<b>debug sbc log-level console</b>	Sets the console logging level.
	<b>debug sbc log-level file</b>	Sets the file logging level.
	<b>debug sbc errors</b>	Enables debugging of sbc service errors.
	<b>debug sbc events</b>	Enables debugging of sbc service events.
	<b>debug sbc info</b>	Enables debugging of sbc services information.
	<b>debug sbc nbase</b>	Enables debugging of sbc services nbase.



# debug sbc info

To debug sbc services information, use the *debug sbc info* command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc info*

**no debug sbc info**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Exec (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **show debug** command to see debug information.

**Examples** The following command turns on debugging for sbc information:

```
Router# debug sbc info
2007 May 13 06:07:42.071738 sbc: (ctx:0)Received debug msg
2007 May 13 06:07:42.071961 sbc: (ctx:0)Exit mts or debug msg recv
```

Related Commands	Command	Description
	<b>debug sbc filter control</b>	Enables console logging based on a number of filters.
	<b>debug sbc ips</b>	Enables IPS tracing.
	<b>debug sbc log-level console</b>	Sets the console logging level.
	<b>debug sbc log-level file</b>	Sets the file logging level.
	<b>debug sbc errors</b>	Enables debugging of sbc service errors.
	<b>debug sbc events</b>	Enables debugging of sbc service events.
	<b>debug sbc ha</b>	Enables debugging of sbc high availability.
	<b>debug sbc nbase</b>	Enables debugging of sbc services nbase.

# debug sbc ips (session border controller)

To turn on IPS tracing (giving details of inter-component signals flowing between the internal components of the Session Border Controller (SBC) process), use the **debug sbc ips** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

```
debug sbc sbc-name ips {file | in-memory}
```

```
no debug sbc sbc-name ips {file | in-memory}
```

## Syntax Description

<i>sbc-name</i>	This is the name of the SBC service.
<i>file</i>	Configures file IPS tracing.
<i>in-memory</i>	Configures in-memory IPS tracing.

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command provides details of inter-component signals flowing between the internal components of the SBC process. Events should be logged on IPS trace file for further debugging.

Use the **show debug** command to see debug information.

## Examples

The following command turns on IPS tracing:

```
Router# debug sbc mySbc ips
```

## Related Commands

Command	Description
<b>debug sbc errors</b>	Debugs SBC service errors.
<b>debug sbc events</b>	Debugs SBC service events.
<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.
<b>debug sbc info</b>	Debugs SBC services information.
<b>debug sbc ips</b>	Turns on IPS tracing.
<b>debug sbc logging</b>	Debugs SBC logging information.
<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
<b>debug sbc nbase</b>	Debugs SBC

<b>Command</b>	<b>Description</b>
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc log-level console

To set the console logging level, use the **debug sbc log-level console** command in Exec mode. To disable this form of debugging, use the **no** form of this command.

**debug sbc** *name* **log-level console** *level*

**no debug sbc** *name* **log-level console** *level*

## Syntax Description

<i>name</i>	This is the name of the Session Border Controller (SBC) service.
<i>level</i>	The level to set. 0 gives all pd logging and 100 gives none.  The log levels are defined as follows: 90+ Fatal errors 80+ Errors 70+ Unexpected conditions 60+ Operational events 50+ Auditable events 40+ Statistics 30+ Verbose operational events 20+ Verbose statistics 10+ Internal diagnostic logs  The following values are used for specific types of logs. 55 Call logs 63 Configuration errors

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command configures the display of the most serious logs directly to the console. Note that when you run the **debug sbc name log-level console 0** command, a large number of log messages are generated. This could cause an increase in the response time of the system. To limit the rate of messages logged per second, use the **logging rate-limit console** command in global configuration mode.

Use the **show debug** command to see debug information.

**Examples**

The following command sets the log level for fatal errors to the console at 90:

```
Router# # debug sbc mySbc log-level console 90
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug sbc filter control</b>	Enables console logging based on a number of filters.
<b>debug sbc ips</b>	Enables IPS tracing.
<b>debug sbc log-level file</b>	Sets the file logging level.
<b>debug sbc errors</b>	Enables debugging of sbc service errors.
debug sbc events	Enables debugging of sbc service events.
<b>debug sbc ha</b>	Enables debugging of sbc high availability.
<b>debug sbc info</b>	Enables debugging of sbc services information.
<b>debug sbc nbase</b>	Enables debugging of sbc services nbase.
<b>logging rate-limit</b>	Limits the rate of messages logged per second.

# debug sbc log-level file

To set the file logging level, use the **debug sbc log-level file** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

**debug sbc** *name* **log-level file** *level*

**no debug sbc** *name* **log-level file** *level*

## Syntax Description

<i>name</i>	This is the name of the Session Border Controller (SBC) service.
<i>level</i>	The level to set. 0 gives all pd logging and 100 gives none.  The log levels are defined as follows: 90+ Fatal errors 80+ Errors 70+ Unexpected conditions 60+ Operational events 50+ Auditable events 40+ Statistics 30+ Verbose operational events 20+ Verbose statistics 10+ Internal diagnostic logs  The following values are used for specific types of logs. 55 Call logs 63 Configuration errors

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command logs the most serious logs directly to file.  
Use the **show debug** command to see debug information.

## Examples

The following command sets the log level to send to file to 60:

```
Router# debug sbc mySbc log-level file 60
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug sbc filter control</b>	Enables console logging based on a number of filters.
<b>debug sbc ips</b>	Enables IPS tracing.
<b>debug sbc log-level console</b>	Sets the console logging level.
<b>debug sbc errors</b>	Enables debugging of sbc service errors.
<b>debug sbc events</b>	Enables debugging of sbc service events.
<b>debug sbc ha</b>	Enables debugging of sbc high availability.
<b>debug sbc info</b>	Enables debugging of sbc services information.
<b>debug sbc nbase</b>	Enables debugging of sbc services nbase.

# debug sbc logging

To debug SBC logging information, use the *debug sbc logging* command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc logging*

**no debug sbc logging**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Exec (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **show debug** command to see debug information.

**Examples** The following command turns on debugging for sbc information:

```
Router# debug sbc logging
```

Related Commands	Command	Description
	<b>debug sbc errors</b>	Debugs SBC service errors.
	<b>debug sbc events</b>	Debugs SBC service events.
	<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.
	<b>debug sbc info</b>	Debugs SBC services information.
	<b>debug sbc ips</b>	Turns on IPS tracing.
	<b>debug sbc logging</b>	Debugs SBC logging information.
	<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
	<b>debug sbc nbase</b>	Debugs SBC
	<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
	<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.



<b>Command</b>	<b>Description</b>
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc mem-trace dump

To dump current memory usage statistics to file, use the *debug sbc mem-trace dump* command in the Exec mode. To disable printing to the terminal, use the **no** form of this command.

*debug sbc sbc-name mem-trace dump*

**no** *debug sbc sbc-name mem-trace dump*

## Syntax Description

*sbc-name* This is the name of the SBC service.

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Use the **show debug** command to see debug information.

## Examples

The following example dumps current memory usage statistics to file:

```
Router# debug sbc mysbc mem-trace dump.
```

## Related Commands

Command	Description
<b>debug sbc errors</b>	Debugs SBC service errors.
<b>debug sbc events</b>	Debugs SBC service events.
<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.
<b>debug sbc info</b>	Debugs SBC services information.
<b>debug sbc ips</b>	Turns on IPS tracing.
<b>debug sbc logging</b>	Debugs SBC logging information.
<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
<b>debug sbc nbase</b>	Debugs SBC
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.

<b>Command</b>	<b>Description</b>
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc nbase

To enable printing to the terminal for the **debug sbc log-level console** command, use the *debug sbc nbase* command in the Exec mode. To disable printing to the terminal, use the **no** form of this command.

**debug sbc nbase**

**no debug sbc nbase**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Exec (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **show debug** command to see debug information.

**Examples** The following command enables printing to the terminal for the **debug sbc log-level console** command:

```
Router# debug sbc nbase
Router# 2007 May 13 07:58:45.133136 sbc: (ctx:0)SBC/MG-CTRL:**** Audit      0x2e01 - 35
(0000) **** 000000000000000000000000000000000000000000010 SBC/MG-CTRL:(gctpassn.c 1157) at 7:58:45, 13
May 2007 (0x0X00060464 ms) SBC/MG-CTRL: Megaco has created an association with a peer.
SBC/MG-CTRL: Remote address = 22.22.22.100 SBC/MG-CTRL: Remote port = 2940
2007 May 13 07:58:45.232974 sbc: (ctx:0)SBC/MGM: **** Operational 0x4d02 - 10 (0000)
**** 000100000000000000000000000010000000 SBC/MGM: (zmxsipcp.c 490) at 7:58:45, 13 May 2007
(0x0X000604C8 ms) SBC/MGM: MPF stub sent MCI req #0X000061D8 (0X00000401) to agent.
```

Related Commands	Command	Description
	<b>debug sbc errors</b>	Debugs SBC service errors.
	<b>debug sbc events</b>	Debugs SBC service events.
	<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.
	<b>debug sbc info</b>	Debugs SBC services information.
	<b>debug sbc ips</b>	Turns on IPS tracing.
	<b>debug sbc logging</b>	Debugs SBC logging information.
	<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
	<b>debug sbc nbase</b>	Debugs SBC

<b>Command</b>	<b>Description</b>
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc off

To turn off all sbc filters and set the log-level back to default (63), use the **debug sbc off** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

**debug sbc *sbc-name* off**

**no debug sbc *sbc-name* off**

<b>Syntax Description</b>	<i>sbc-name</i> This is the name of the SBC service.
---------------------------	--

<b>Command Default</b>	Log-levels set to 63.
------------------------	-----------------------

<b>Command Modes</b>	Exec (#)
----------------------	----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	Use the <b>show debug</b> command to see debug information.
-------------------------	---

**Examples** The following command turns on debugging for sbc information:

```
Router# debug sbc test-sbc off
Router# 2008 May 20 14:55:51.410879 sbc: (ctx:0)This option will disable all SBC debugs
2008 May 20 14:55:51.410978 sbc: (ctx:0) SBC: Log filter removed.
2008 May 20 14:55:51.411014 sbc: (ctx:0) SBC: Log filter removed.
```

The following command shows debugging information:

```
Router# show debug
SBC Daemon:

SBC inter-process logging is off
SBC log filter 0:
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>debug sbc log-level console</b>	
	<b>debug sbc log-level file</b>	
	<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
	<b>debug sbc pd log-level</b>	Sets the file logging level.



# debug sbc pd filter component

To turn on problem determination (PD) filter components, use the **debug sbc pd** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

```
debug sbc sbc-name pd filter component [bm | cac | control | h323 | hm | icc | mgm | radius | routing | sip]
```

```
no debug sbc sbc-name pd filter component [bm | cac | control | h323 | hm | icc | mgm | radius | routing | sip]
```

## Syntax Description

<i>sbc-name</i>	This is the name of the SBC service.
bm	Logs from the bm components.
cac	Logs from the cac components.
control	Logs from the H.248 controller components.
h323	Logs from the H.323 components.
hm	Logs from the bm components.
icc	Logs from the icc components.
mgm	Logs from the mgm components.
radius	Logs from the radius components.
routing	Logs from the routing components.
sip	Logs from the sip components.

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command provides details of inter-component signals flowing between the internal components of the SBC process. Events should be logged on IPS trace file for further debugging.

Use the **show debug** command to see debug information.

## Examples

The following command turns on IPS tracing:

```
Router# debug sbc mySbc ips
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug sbc errors</b>	Debugs SBC service errors.
<b>debug sbc events</b>	Debugs SBC service events.
<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.
<b>debug sbc info</b>	Debugs SBC services information.
<b>debug sbc ips</b>	Turns on IPS tracing.
<b>debug sbc logging</b>	Debugs SBC logging information.
<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
<b>debug sbc nbase</b>	Debugs SBC
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc pd filter context

To turn on different logs from the problem determination (PD) filters, use the **debug sbc pd filter context** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

```
debug sbc sbc-name pd filter context [adjacency name | billing_id name | ipv4 name | number name]
```

```
no debug sbc sbc-name pd filter context [adjacency name | billing_id name | ipv4 name | number name]
```

## Syntax Description

<i>sbc-name</i>	This is the name of the SBC service.
<i>adjacency</i>	Logs from the adjacency filter.
<i>billing_id</i>	Logs from the billing_id filter.
<i>ipv4</i>	Logs from the ipv4 filter.
<i>number</i>	Logs from the number filter.
<i>name</i>	Name for the specific filter context.

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command provides details of inter-component signals flowing between the internal components of the SBC process. Events should be logged on IPS trace file for further debugging.

Use the **show debug** command to see debug information.

## Examples

The following command turns on the adjacency log filter:

```
Router# debug sbc pd filter context adjacency test
```

## Related Commands

Command	Description
<b>debug sbc errors</b>	Debugs SBC service errors.
<b>debug sbc events</b>	Debugs SBC service events.
<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.

<b>Command</b>	<b>Description</b>
<b>debug sbc info</b>	Debugs SBC services information.
<b>debug sbc ips</b>	Turns on IPS tracing.
<b>debug sbc logging</b>	Debugs SBC logging information.
<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
<b>debug sbc nbase</b>	Debugs SBC
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc pd filter product

To turn on problem determination (PD) filter product group logs, use the **debug sbc pd filter product** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

*debug sbc sbc-name pd filter context [billing | call | media | overview | protocol]*

*no debug sbc sbc-name pd filter context [adjacency | billing\_id | ipv4 | number]*

## Syntax Description

<i>sbc-name</i>	This is the name of the SBC service.
<i>billing</i>	Logs from the billing product group.
<i>call</i>	Logs from the call product group.
<i>media</i>	Logs from the media product group.
<i>overview</i>	Logs from the overview product group.
<i>protocol</i>	Logs from the protocol product group.

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command provides details of inter-component signals flowing between the internal components of the SBC process. Events should be logged on IPS trace file for further debugging.

Use the **show debug** command to see debug information.

## Examples

The following command turns on the logs from the protocol product group:

```
Router# debug sbc pd filter product protocol
```

## Related Commands

Command	Description
<b>debug sbc errors</b>	Debugs SBC service errors.
<b>debug sbc events</b>	Debugs SBC service events.
<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.
<b>debug sbc info</b>	Debugs SBC services information.
<b>debug sbc ips</b>	Turns on IPS tracing.

<b>Command</b>	<b>Description</b>
<b>debug sbc logging</b>	Debugs SBC logging information.
<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
<b>debug sbc nbase</b>	Debugs SBC
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug sbc pd log-level

To set the file logging level, use the **debug sbc pd log-level** command in the Exec mode. To disable this form of debugging, use the **no** form of this command.

**debug sbc** *sbc-name* **pd log-level** { **console** *level* | **file** *level* | **filter** *level* }

**no debug sbc** *sbc-name* **pd log-level** { **console** *level* | **file** *level* | **filter** *level* }

## Syntax Description

<i>sbc-name</i>	This is the name of the Session Border Controller (SBC) service.
level	The level to set. 0 gives all problem determination (pd) logging and 100 gives none. The log levels are defined as follows: 90+ Fatal errors 80+ Errors 70+ Unexpected conditions 60+ Operational events 50+ Auditable events 40+ Statistics 30+ Verbose operational events 20+ Verbose statistics 10+ Internal diagnostic logs The following values are used for specific types of logs. 55 Call logs 63 Configuration errors

## Command Default

No default behavior or values are available.

## Command Modes

Exec (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command logs the most serious logs directly to file.  
Use the **show debug** command to see debug information.

## Examples

The following command sets the log level to send to file to 60:

```
Router# debug sbc mySbc pd log-level file 60
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug sbc errors</b>	Debugs SBC service errors.
<b>debug sbc events</b>	Debugs SBC service events.
<b>debug sbc ha</b>	Debugs SBC high availability (HA) services.
<b>debug sbc info</b>	Debugs SBC services information.
<b>debug sbc ips</b>	Turns on IPS tracing.
<b>debug sbc logging</b>	Debugs SBC logging information.
<b>debug sbc mem-trace dump</b>	Dumps current memory usage statistics to file.
<b>debug sbc nbase</b>	Debugs SBC
<b>debug sbc pd filter component</b>	Turns on problem determination (PD) filter components.
<b>debug sbc pd filter context</b>	Turns on different logs from the problem determination (PD) filters.
<b>debug sbc pd filter product</b>	Turns on problem determination (PD) filter product group logs.
<b>debug sbc pd log-level</b>	Sets the file logging level.

# debug vrf

To get debugging information on virtual routing and forwarding (VRF) instances, use the **debug vrf** command in privileged EXEC mode. To turn off the debug output, use the **undebug** version of the command.

```
debug vrf { create | delete | error | ha | initialization | interface | ipv4 | ipv6 | issu | lock | lookup
           | mpls | selection }
```

```
undebug vrf { create | delete | error | ha | initialization | interface | ipv4 | ipv6 | issu | lock | lookup
            | mpls | selection }
```

## Syntax Description

<b>create</b>	Specifies VRF creation debugging.
<b>delete</b>	Specifies VRF deletion debugging.
<b>error</b>	Specifies VRF error debugging.
<b>ha</b>	Specifies VRF high-availability debugging.
<b>initialization</b>	Specifies VRF subsystem initialization debugging.
<b>interface</b>	Specifies VRF interface assignment debugging.
<b>ipv4</b>	Specifies VRF IPv4 address family debugging.
<b>ipv6</b>	Specifies VRF IPv6 address family debugging.
<b>issu</b>	Specifies VRF in-service software upgrade debugging.
<b>lock</b>	Specifies VRF lock debugging.
<b>lookup</b>	Specifies VRF database lookup debugging.
<b>mpls</b>	Specifies VRF multiprotocol label switching debugging.
<b>selection</b>	Specifies VRF selection debugging.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

## Usage Guidelines

Use this command to get debugging information on VRFs.

## Examples

The following example shows how to turn on debugging of VRF interface assignment:

```
Router# debug vrf interface
```

## Related Commands

Command	Description
<b>vrf definition</b>	Defines a virtual routing and forwarding instance.



# default-port-limit

To enter the mode for configuring the default event limits for the ports of a given address, use the **default-port-limit** command in the SBE blacklist IPv4 configuration mode. To remove the event limits set, use the **no** form of this command.

**default-port-limit**

**no default-port-limit**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No event limits are defined for ports.

**Command Modes** SBE blacklist IPv4 configuration (config-sbc-sbe-blacklist-ipv4)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **blacklist default-port-limit** command is used to enter the mode for configuring the default event limits for the ports of the source address 123.123.2.2:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 123.123.2.2
Router(config-sbc-sbe-blacklist-ipv4)# default-port-limit
Router(config-sbc-sbe-blacklist-ipv4-port-lmt)#
```

Related Commands	Command	Description
	<b>blacklist</b>	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	<b>ipv4 (blacklist)</b>	Enters the mode for applying blacklisting options to a single IP address.
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source.
	<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.

<b>Command</b>	<b>Description</b>
<b>trigger-period</b>	Defines the period over which events are considered.
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.

# delegate-profile

To configure a delegate client registration profile that can be applied to a delegate subscriber, use the **delegate-profile** command in SBE configuration mode. To remove a delegate client registration profile, use the **no delegate-profile** command.

**delegate-profile** *{profile name}*

**no delegate-profile** *{profile name}*

<b>Syntax Description</b>	<i>profile name</i>	This is the name of the delegate client registration profile that can be applied to a delegate subscriber.  The profile name is a string field of 24 characters maximum length.
---------------------------	---------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** After a delegate profile is configured, the following profile parameters may optionally be configured:

- duration
- retry-count
- retry-interval
- refresh-buffer

Before configuring provisioned delegate registration, you need to configure a delegate registration profile and a SIP contact for a subscriber for whom a subscriber detail table exists, and then you can configure delegate registration for the subscriber. See the Examples section.

Delegate registration is done underneath the SBE configuration for globally unique subscribers.

**Examples** The following example configures a delegate registration profile that can be applied to a delegate registration subscriber:

```
sbc mySbc sbe
  delegate-profile my-profile
  dur 1000
  retry-cnt 5
  retry-interval 60
  refresh-timeout 200
```

The following example configures a SIP contact for a subscriber, for whom a subscriber detail table exists, and for whom, after the SIP contact is configured, Provisioned Delegate Registration can be configured:

```
sbc mySbc
  sbe
    subscriber sip:bob@isp.example
    sip-contact sip:steve@10.1.1.2
    adjacency CallMgrB
  exit
```

The following example configures a delegate registration aor= sip:bob@isp.example

```
(config)# sbc mySbc
(config)# sbe
(config-sbc-sbe)# subscriber sip:bob@isp.example
(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
(config-sbc-sbe-subscriber-contact)# exit
(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
(config-sbc-sbe-subscriber-delegate)# activate
```

**Related Commands**

Command	Description
<b>sip-contact</b>	Configures the SIP contact information for a specified Uniform Resource Identifier (URI) for a delegate subscriber.
<b>subscriber</b>	Configures a delegate registration for a specified subscriber associated with a client device.
<b>delegate-registration</b>	Configures provisioned delegate registration for a specific delegate client.
<b>adjacency</b>	Configures the adjacency facing the registrar.
<b>profile</b>	Applies a delegate registration profile to a delegate registration subscriber.
<b>show sbc sbe sip subscribers</b>	Displays subscribers for whom Provisioned Delegate Registration has been provisioned.
<b>show sbc sbe sip delegate-profile</b>	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.

# delegate-registration

To configure provisioned delegate registration for a specific delegate client, use the **delegate-registration** command in subscriber-entry configuration mode. To remove provisioned delegate registration for a specific delegate client, use the **no delegate-registration** command.

```
delegate-registration {hostname}
```

```
no delegate-registration {hostname}
```

## Syntax Description

<i>hostname</i>	Specifies the name of the delegate client.  The <i>hostname</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	--

## Command Default

No default behavior or values are available.

## Command Modes

subscriber-entry configuration mode (config-sbc-sbe-subscriber-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command allows you to configure a provisioned delegate registration for a specific delegate client. While in the subscriber-delegate configuration mode, you typically configure adjacency and profile, as shown in the examples section.

Before configuring provisioned delegate registration, you need to configure a delegate registration profile, a SIP contact for a subscriber for whom a subscriber detail table exists, and then you can configure delegate registration for the subscriber. See the Examples section.

## Examples

The following example configures a delegate registration aor= sip:bob@isp.example:

```
(config)# sbc mySbc
(config)# sbe
(config-sbc-sbe)# subscriber sip:bob@isp.example
(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
(config-sbc-sbe-subscriber-contact)# exit
(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
(config-sbc-sbe-subscriber-delegate)# profile my-profile
(config-sbc-sbe-subscriber-delegate)# activate
```

The following example configures a delegate registration profile that can be applied to a delegate registration subscriber.

```
sbc mySbc sbe
  delegate-profile my-profile
    duration 1000
    retry-count 5
    retry-interval 60
    refresh-buffer 200
```

The following example configures a SIP contact for a subscriber, for whom a subscriber detail table exists, and for whom, after the SIP contact is configured, delegate registration can be configured:

```
sbc mySbc
  sbe
    subscriber sip:bob@isp.example
    sip-contact sip:steve@10.1.1.2
    adjacency CallMgrB
  exit
```

The following example configures a delegate registration for a specified client device address location, after the SIP contact information has been configured:

```
sbc mySbc
  sbe
    subscriber sip:bob@isp.example
    sip-contact sip:steve@10.1.1.2
    adjacency CallMgrB          =====> client adjacency
  exit
  delegate-registration sip:registrar@1.1.1.1
  adjacency CallMgrA          =====> registrar adjacency
  profile my-profile
  activate
```

**Related Commands**

Command	Description
<b>delegate-profile</b>	Configures a delegate registration profile that is applied to a delegate registration subscriber.
<b>sip-contact</b>	Configures the SIP contact information for a specified Uniform Resource Identifier (URI) for a delegate subscriber
<b>subscriber</b>	Configures a delegate registration for a specified subscriber associated with a client device.
<b>adjacency</b>	Configures the adjacency facing the registrar.
<b>profile</b>	Applies a delegate registration profile to a delegate registration subscriber.
<b>show sbc sbe sip subscribers</b>	Displays subscribers for whom Provisioned Delegate Registration has been provisioned.
<b>show sbc sbe sip delegate-profile</b>	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.

# description (route server context)

To specify a description for a BGP route server context, use the **description** command in route server context configuration mode. To remove the description, use the **no** form of this command.

**description** *string*

**no description**

<b>Syntax Description</b>	<i>string</i>	Description of the route server context. The string can be up to 80 characters long.
---------------------------	---------------	--

<b>Command Default</b>	No description for a route server context exists.
------------------------	---

<b>Command Modes</b>	Route server context configuration (config-router-rsctx)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.3S	This command was introduced.

**Usage Guidelines**

Create a route server context if you want your BGP route server to support customized, flexible policies. The routes needing flexible policy handling are selected for import into a route server context by an import map that you configure. The import map references a route map, where the actual policy is defined.

The **description** command allows an optional description of a route server context to remind you of the purpose of the context or policy, for example. This is more user-friendly and scannable than trying to interpret the route map commands when looking at a configuration file or **show** output.

**Examples**

In the following example, the description is a user-friendly way to see the purpose of the context, without having to interpret the import map and route map:

```
Router(config)# router bgp 65000
Router(config-router)# route-server-context only_AS27_context
Router(config-router-rsctx)# description Context references route map permitting only routes with AS 27 in AS path.
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>import-map</b>
	<b>route-server-context</b>	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

## description (session border controller)

To configure descriptive text for a policy set, an adjacency, a source and its event limits, a number analysis table, a stream list, or an administrative domain, use the **description** command in the appropriate configuration mode. To remove this configuration, use the **no** form of this command.

**description** *description*

**no description** *description*

### Syntax Description

<i>description</i>	Object you are describing.
--------------------	----------------------------

### Command Default

No default behavior or values are available.

### Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
 Adjacency SIP configuration (config-sbc-sbe-adj-sip)  
 Routing policy table (config-sbc-sbe-rtgpolicy)  
 CAC policy-set configuration (config-sbc-sbe-cacpolicy)  
 CAC table configuration (config-sbc-sbe-cacpolicy-cactable)  
 NA routing table configuration (config-sbc-sbe-rtgpolicy-natable)  
 RTG routing table configuration (config-sbc-sbe-rtgpolicy-rtgtable)  
 SBE blacklist configuration (config-sbc-sbe-blacklist)  
 SIP header configuration (config-sbc-sbe-sip-hdr)  
 SIP method profile configuration (config-sbc-sbe-sip-mth)  
 Administrative domain configuration (config-sbc-sbe-ad)  
 Stream list configuration (config-sbc-sbe-stream-list)  
 SIP Body Editor configuration (config-sbc-sbe-mep-bdy)  
 SIP Method Editor configuration (config-sbc-sbe-mep-mth)  
 SIP Option Editor configuration (config-sbc-sbe-mep-opt)  
 SIP Header Editor configuration (config-sbc-sbe-mep-hdr)  
 SIP Parameter Editor configuration (config-sbc-sbe-mep-prm)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.



Release	Modification
Cisco IOS XE Release 3.2S	This command was added in the Administrative domain mode.
Cisco IOS XE Release 3.3S	This command was added in the Stream list, SIP Body Editor, SIP Method Editor, SIP Option Editor, SIP Header Editor, and SIP Parameter Editor configuration modes.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

The use of special characters, such as backslash (\), and a three or larger digit for character settings such as **description**, results in incorrect translation.

### Examples

The following example shows how to configure the h323ToIsp42 H.323 adjacency to use the description test adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# description test adjacency
```

The following example shows how to set the SipToIsp42 SIP adjacency to use the description test adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# description test adjacency
```

The following example shows how to create a description for the MyNaTable number analysis table with entries that match the entire dialed number:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-number-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# description "My first number analysis table"
```

The following example shows how to create an empty policy set, identified by the number 1, on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# description "empty set"
```

The following example shows how to set the description of the MyCacTable admission control table:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# description "My first CAC table"
```

The following example shows how to create a description for the MyNaTable number analysis table with entries that match the start of the dialed number:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-prefix-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# description "My first number analysis table"
```

The following example shows how to add a description for a specific source IP address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4
Router(config-sbc-sbe-blacklist)# ipv4 125.12.12.15
Router(config-sbc-sbe-blacklist-ipv4)# description "test"
```

The following example shows how to create an empty policy set, identified by the number 1, on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# description "empty set"
```

The following example shows how to add a description for an administrative domain:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# admin-domain ADMIN1
Router(config-sbc-sbe-ad)# description "My first administrative domain"
```

The following example shows how to add a description for a stream list:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# stream-list my-stream
Router(config-sbc-sbe-stream-list)# description "This is my first stream list"
```

The following examples shows how to add a description to the header, body, option, parameter, and method editors.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-editor paramedit1
Router(config-sbc-sbe-mep-prm)# description "The Parameter Editor"
```

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor header1
Router(config-sbc-sbe-mep-hdr)# description "The Header Editor"
```

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# sip option-editor option1  
Router(config-sbc-sbe-mep-opt)# description "The Option Editor"
```

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# sip body-editor Body1  
Router(config-sbc-sbe-mep-bdy)# description "The Body Editor"
```

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# sip method-editor Method1  
Router(config-sbc-sbe-mep-mth)# description "The Method Editor"
```

## description (sip-opt)

To set the description for the profile, use the **description** command in SIP option mode. Use the **no** form of this command to remove description from this profile.

**description** *line*

**no description** *line*

---

### Syntax Description

---

*line* The description of the profile. The maximum number of characters is 80.

---



---

### Command Default

The global default is used.

---

### Command Modes

SIP option (sip-opt)

---

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

---



---

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command:

---

### Examples

The following example shows how to set the description for the profile.

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-profile optpr1
Router(config-sbc-sbe-sip-opt)# description test
```

# dial-plan-suffix

To configure the dial plan suffix used for the ENUM query, use the **dial-plan-suffix** command in ENUM entry configuration mode. To return the dial plan suffix to the default value, use the no form of this command.

**dial-plan-suffix** *suffix*

**no dial-plan-suffix** *suffix*

<b>Syntax Description</b>	<i>suffix</i>	ENUM dialing plan suffix. The maximum length is 255.
---------------------------	---------------	--

<b>Command Default</b>	The default suffix is e164.arpa.	
------------------------	----------------------------------	--

<b>Command Modes</b>	ENUM entry configuration (config-sbc-sbe-enum-entry)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the dial plan suffix used for the ENUM query:
-----------------	--

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# entry ENUM_1
Router(config-sbc-sbe-enum-entry)# server ipv4 10.10.10.10 vrf VRF1
Router(config-sbc-sbe-enum-entry)# dial-plan-suffix Example.Suffix
Router(config-sbc-sbe-enum-entry)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).

<b>Command</b>	<b>Description</b>
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe</b> <b>call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum</b> <b>entry</b>	Displays the contents of an ENUM client entry.

# diameter

To enable the Diameter protocol on a node and enter the Diameter configuration mode, use the **diameter** command in SBE configuration mode. To disable the Diameter protocol on a node, use the no form of this command.

**diameter**

**no diameter**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Diameter is an Authentication Authorization Accounting (AAA) protocol and is an enhanced version of the RADIUS (Remote Authentication Dial-In User Service) protocol. Diameter is the protocol of choice for the next generation network IP Multimedia Subsystem (IMS) developed by 3rd Generation Partnership Project (3GPP).

## Examples

The following example shows how to enable the Diameter protocol on a node and enter the diameter configuration mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# diameter
Router(config-sbc-sbe-diameter)#
```

## Related Commands

Command	Description
<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
<b>origin-realm</b>	Configures the domain name of an IMS local realm.
<b>origin-host</b>	Configures the domain name of an IMS local host.

<b>Command</b>	<b>Description</b>
<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.



# div-address

To enter the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only), use the **div-address** command in SIP header configuration mode. To exit the diverted-by address mode, use the **no** form of this command or the **exit** command.

**div-address**

**no div-address**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SIP header configuration (config-sbc-sbe-sip-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of modes required to run the command.

This command puts you in the diverted-by address mode where you use the **header-prio header-name** command to set the priority of the header or headers from which a diverted-by address is derived.

 **Note**

The header list is for inbound calls only.

**Examples** The following example shows how to enter the diverted-by address mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile HP1
Router(config-sbc-sbe-sip-hdr) div-address
Router(config-sbc-sbe-sip-hdr-div)#
```

Related Commands	Command	Description
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.

<b>Command</b>	<b>Description</b>
<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

## div-address (header)

To enter the Diverted-by address mode and set the priority of the header or headers from which to derive a diverted-by address (inbound only), use the **div-address** command in the Session Initiation Protocol (SIP) Header Editor configuration mode. To remove the priority list of headers, use the **no** form of this command.

**div-address**

**no div-address**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

This command puts you in the Diverted-by address mode from where you can use the **header-prio header-name** command to set the priority of the header or headers from which a diverted-by address is derived.

**Examples** The following example shows how to enter the Diverted-by address mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor HP1
Router(config-sbc-sbe-mep-hdr) div-address
Router(config-sbc-sbe-mep-hdr-div)#
```

Related Commands	Command	Description
	<b>sip header-editor</b>	Configures a header editor.

# domain-name

To specify the domain name of a Border Access Controller (BAC) adjacency that replaces the domain name of the Access Gateway Control Function (AGCF) and the Media Gateway Control Function (MGCF), use the **domain-name** command in the H248 BAC adjacency configuration mode. To remove the specification of the domain name for a BAC adjacency, use the **no** form of this command.

**domain-name** *domain-name*

**no domain-name** *domain-name*

## Syntax Description

<i>domain-name</i>	Specifies the domain name of a BAC adjacency. The <i>domain-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
--------------------	--

## Command Default

None

## Command Modes

H248 BAC adjacency configuration (config-h248-bac-adj)

## Command History

Release	Modification
Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command can be configured only in the access adjacency submode and not in the core adjacency submode.

## Examples

The following example shows how the **domain-name** command is used to specify the domain name of a BAC adjacency:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# domain-name cisco
```

## Related Commands

Command	Description
<b>adjacency h248</b>	Configures an H.248 access adjacency and core adjacency.

# dscp

To configure a DSCP with which to mark IP packets belonging to a given QoS profile, use the **dscp** command in the appropriate configuration mode. To return to the default, use the **no** form of this command.

**dscp** *value*

**no dscp**

## Syntax Description

<i>value</i>	Specifies the DSCP value with which to mark packets. Range is 0 to 63.
--------------	--

## Command Default

The default DSCP value is 0.

## Command Modes

QoS sig configuration (config-sbc-sbe-qos-sig)  
 QoS video configuration (config-sbc-sbe-qos-video)  
 QoS voice configuration (config-sbc-sbe-qos-voice)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the QoS profile for sig to mark IP packets with a DSCP of 10:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos sig residential
Router(config-sbc-sbe-qos-fax)# dscp 10
```

The following example shows how to configure the QoS profile for video to mark IP packets with a DSCP of 10:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos video residential
Router(config-sbc-sbe-qos-video)# dscp 10
```

The following example shows how to configure the QoS profile for voice to mark IP packets with a DSCP of 10:

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# qos voice residential  
Router(config-sbc-sbe-qos-voice)# dscp 10
```

# dst-address

To enter the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only), use the **dst-address** command in SIP header configuration mode. To exit the destination address mode, use the **no** form of this command or the **exit** command.

**dst-address**

**no dst-address**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SIP header configuration (config-sbc-sbe-sip-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of modes required to run the command.

This command puts you in the destination address mode where you use the **header-prio header-name** command to set the priority of the header or headers from which a called party address is derived.

 **Note**

The header list is for inbound calls only.

**Examples** The following example shows how to enter the destination address mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile HP1
Router(config-sbc-sbe-sip-hdr) dst-address
Router(config-sbc-sbe-sip-hdr-dst)#
```

Related Commands	Command	Description
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.

<b>Command</b>	<b>Description</b>
<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.



## dst-address (editor)

To enter the Destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only), use the **dst-address** command in the Session Initiation Protocol (SIP) Header Editor configuration mode. To exit the Destination address mode, use the **no** form of this command or the **exit** command.

**dst-address**

**no dst-address**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

This command enables you to enter the Destination address mode from where you can use the **header-prio header-name** command to set the priority of the header or headers from which a called party address is derived.

 **Note**

The header list is for inbound calls only.

**Examples** The following example shows how to enter the Destination address mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor HP1
Router(config-sbc-sbe-mep-hdr) dst-address
Router(config-sbc-sbe-mep-hdr-dst)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>div-address</b>	Enables entry into the Diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enables entry into the Destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>header-prio header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>src-address</b>	Enables entry into the Source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>sip header-editor</b>	Configures a header editor.

# dst-adjacency

To configure the destination adjacency of an entry in a routing table, use the **dst-adjacency** command in RTG routing table configuration mode. To delete the destination adjacency, use the **no** form of this command.

**dst-adjacency** *target-adjacency*

**no dst-adjacency** *target-adjacency*

<b>Syntax Description</b>	<i>target-adjacency</i> Specifies the string that identifies the destination adjacency to use.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	RTG routing table configuration (config-sbc-sbe-rtgpolicy-rtgtable)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

The *target-adjacency* argument is mandatory for routing tables entries with table-type **round-robin**.

<b>Examples</b>	The following example shows how to configure the destination adjacency of an entry in the new routing table MyRtgTable to softswitch1:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency softswitch1
```

The following example shows how to configure the destination adjacency of an entry in the new routing table MyRtgTable to softswitch1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency softswitch1
```

The following example shows how to configure the destination adjacency of an entry in the new routing table MyRtgTable to softswitch1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency softswitch1
```

The following example shows how to configure the destination adjacency of an entry in the new routing table MyRtgTable to softswitch1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-account-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency softswitch1
```

The following example shows how to configure the destination adjacency of an entry in the new routing table MyRtgTable to softswitch1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-round-robin-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency softswitch1
```

# dtmf-duration (session border controller)

To configure the default duration of a dual tone multifrequency (DTMF) event in milliseconds, use the **dtmf-duration** command in VDBE configuration mode. To reconfigure the default duration of a DTMF event in milliseconds, use the **no** form of this command.

**dtmf-duration** *duration*

**no dtmf-duration** *duration*

## Syntax Description

*duration* This is the default duration of a DTMF event in milliseconds. The range is 0-1000. The default is 200.

## Command Default

The default is 200 ms if this command is not configured, or the **no dtmf-duration** command is issued.

## Command Modes

VDBE configuration (config-sbc-dbe-vdbe) for distributed SBC

VDBE configuration (config-sbc-vdbe) for unified SBC

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.4	This command was modified for unified SBC.

## Usage Guidelines

This command can be used on both unified and distributed SBC, but in slightly different configuration modes. Note the correct mode to use for either unified or distributed SBC.

## Examples

The following example configures the duration of a DTMF event to be 250 milliseconds for a unified SBC:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc)# vdbe
Router(config-sbc-vdbe)# dtmf-duration 250
Router(config-sbc-vdbe)# end
```

The following example configures the duration of a DTMF event to be 250 milliseconds for a distributed SBC:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# dtmf-duration 250
Router(config-sbc-dbe-vdbe)# end
```

Related Commands	Command	Description
	vdbe	Enter into VDBE configuration mode.

# dtmf disable sip

To turn off automatic detection of dual tone multifrequency-specific options, use the **dtmf disable sip** command in adjacency SIP configuration mode. To turn on the automatic detection of dual tone multifrequency (DTMF) relay, use the **no** form of this command.

```
dtmf disable sip {info | notify}
```

```
no dtmf disable sip {info | notify}
```

## Syntax Description

<b>info</b>	Specifies INFO-based DTMF relay.
<b>notify</b>	Specifies NOTIFY-based DTMF relay.

## Command Default

The default is automatic detection of DTMF relay.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

## Examples

The following example shows how to turn off automatic detection of DTMF relay using the INFO method as the preferred DTMF transport method for the endpoints on an adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp4
Router(config-sbe-adj-sip)# dtmf disable sip info
```

# dtmf sip

To configure DTMF SIP, use the **dtmf sip** command in adjacency SIP configuration mode. To unconfigure DTMF SIP, use the **no** form of this command.

```
dtmf sip {default duration millisec | info always-supported | notify interval millisec}
```

```
no dtmf sip {default duration millisec | info always-supported | notify interval millisec}
```

## Syntax Description

<b>default</b>	Specifies default values.
<b>duration</b>	Specifies the duration for which the SBC advertises on outbound DTMF transport.
<b>info</b>	Specifies INFO-based DTMF relay.
<b>always-supported</b>	Overrides automatic detection of DTMF support, assuming the INFO method as the preferred DTMF transport method for endpoints on an adjacency.
<b>notify</b>	Specifies NOTIFY-based DTMF relay.
<b>interval</b>	Specifies the maximum time for which the SBC waits between the NOTIFY messages for a single DTMF event.
<i>millisec</i>	The time in milliseconds, ranging from 1 to 65535.

## Command Default

The default is automatic detection of DTMF relay.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

## Examples

The following example shows how to configure DTMF SIP:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp4
Router(config-sbe-adj-sip)# dtmf sip notify interval 1000
Router(config-sbe-adj-sip)# dtmf sip info always-supported
```



# duration

To configure the expiration time during which the Cisco Unified Border Element (SP Edition) tries to perform provisioned delegate registration before stopping, use the **duration** command in subscriber delegate profile configuration mode. To reset the expiration time to the default duration time, use the **no duration** command.

**duration** *{dur time in secs}*

**no duration** *{dur time in secs}*

Syntax Description	<i>dur time in secs</i>	This is the duration time in seconds. The range is 1 to 2,147,483 seconds. The default duration time is 1800 seconds.
--------------------	-------------------------	---

**Command Default** The default duration time is 1800 seconds.

**Command Modes** Subscriber delegate profile configuration mode (config-sbc-sbe-subscriber-delegate-prof)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command configures the expiration time when the delegate client is due to expire, that is, the length of time in seconds during which the SBC tries to perform delegate registration before stopping. This is one of the delegate profile parameters you can configure.

After a delegate profile is configured, the following profile parameters may optionally be configured:

- duration
- retry-count
- retry-interval
- refresh-buffer

**Examples** The following example configures a provisioned delegate registration profile that can be applied to a delegate registration subscriber and configures a delegate registration for delegate client (aor=sip:bob@isp.example). The delegate registration profile is configured with a duration expiration time of 1000 seconds, a retry count of 5 times, a retry interval of 60 seconds, and a refresh timeout time of 200 seconds:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# delegate-profile my-profile
Router(config-sbc-sbe-subscriber-delegate-prof)# duration 1000
Router(config-sbc-sbe-subscriber-delegate-prof)# retry-count 5
```

```

Router(config-sbc-sbe-subscriber-delegate-prof)# retry-interval 60
Router(config-sbc-sbe-subscriber-delegate-prof)# refresh-buffer 200
Router(config-sbc-sbe-subscriber-delegate-prof)# exit
Router(config-sbc-sbe)# subscriber sip:bob@isp.example
Router(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
Router(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
Router(config-sbc-sbe-subscriber-contact)# exit
Router(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
Router(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
Router(config-sbc-sbe-subscriber-delegate)# profile my-profile
Router(config-sbc-sbe-subscriber-delegate)# activate
Router(config-sbc-sbe-subscriber-delegate)# end

```

**Related Commands**

<b>Command</b>	<b>Description</b>
retry-count	Configures the number of times the SBC repeats the delegate registration processing after the retry interval ends.
retry-interval (registration)	Configures the length of time the SBC waits before it retries delegate registration.
refresh-buffer	Configures the length of time by which the SBC attempts to refresh the address location with a delegate registration before the specified expiration time.
delegate-profile	Configures a delegate registration profile that is applied to a delegate registration subscriber.
delegate-registration	Configures a delegate registration for a delegate client.
show sbc sbe sip delegate-profile	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.

# early-media-deny

To configure whether to disallow early-media for an entry in an admission control table, use the **early-media-deny** command in CAC table configuration mode. To return to the default value, use the **no** form of this command.

**early-media-deny**

**no early-media-deny**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, early-media is allowed.

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to disallow early-media for an existing entry in the admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# early-media-deny
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Related Commands	Command	Description
	early-media-timeout	Configures the time to allow early-media before a call is established.

# early-media-timeout

To configure the amount of time for which to allow early-media before a call is established, use the **early-media-timeout** command in CAC table configuration mode. To return to the default value, use the **no** form of this command.

**early-media-timeout** *value*

**no early-media-timeout**

## Syntax Description

<i>value</i>	Specifies the timeout period (in seconds). A value of 0 means that calls are not timed out.
--------------	---

## Command Default

*value*: 0

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the early-media-timeout for an existing entry in the admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# early-media-timeout 90
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
```

## early-media-type

To configure the direction of early media to allow for an entry in a call admission control table, use the **early-media-type** command in CAC table configuration mode. To return to the default value, use the **no** form of this command.

**early-media-type** {**backward-half-duplex** | **forward-half-duplex** | **full-duplex**}

**no early-media-type**

### Syntax Description

<b>backward-half-duplex</b>	Allows early media in the backwards direction only.
<b>forward-half-duplex</b>	Allows early media in the forwards direction only.
<b>full-duplex</b>	Allows early media in both directions.

### Command Default

The default direction is full-duplex.

### Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to disallow early-media for an existing entry in the admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# early-media-type full-duplex
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

Command	Description
<b>early-media-timeout</b>	Configures the time to allow early-media before a call is established.

# edit-cic

To manipulate a carrier identification code in number analysis and routing tables, use the **edit-cic** command call policy set table mode. The **no** form of the command removes the configured string.

**edit-cic** [**del-prefix** *pd*] | [**del-suffix** *sd*] | [**add-prefix** *pa*] | [**replace** *ds*]

## Syntax Description

<b>del-prefix</b>	Specifies digits to delete from the front of the carrier ID string.
<b>del-suffix</b>	Specifies digits to delete from the end of the carrier ID string.
<b>add-prefix</b>	Specifies digits to add to the front of the carrier ID string.
<b>replace</b>	Replaces the carrier ID string with the configured string of digits.
<i>pd</i>	A positive integer specifying the number of digits to delete from the front of the carrier ID string.
<i>sd</i>	A positive integer specifying the number of digits to delete from the end of the carrier ID string.
<i>pa</i>	A string of digits to add to the front of the carrier ID string.
<i>ds</i>	A string of digits with which to replace the carrier ID string.

## Command Default

No default behavior or values are available.

## Command Modes

NA-DST-address-table configuration (config-sbc-sbe-rtgpolicy-natable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command is used to manipulate the carrier identification code (cic) address in number analysis and routing tables. You can configure more than one edit action (**del-prefix**, **del-suffix**, and **add-prefix**) and configure combinations of edit actions, as long as you follow the rules. The rules are as follows:

- The edit-cic action keywords **del-prefix**, **del-suffix**, and **add-prefix** can be combined in any order, with at least one keyword required.
- Combinations of edit-cic actions are implemented from left to right. For example, the combination **edit-cic del-prefix 3 add-prefix 919 del-suffix 4** command changes the dialed digit string, 2025551212, into 919555.
- The **edit-cic replace** action cannot be combined with other edit actions.

If you want to remove the carrier ID entirely from outgoing messages, specify a replacement string of 0000 or a prefix deletion length of 4. For example:

**edit-cic del-prefix 4**

or

**edit-cic replace 0000**

Re-entering the **edit-cic** command with a new combination of edit actions replaces the existing combination.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure entry 1 to delete four digits from the end of the dialed string, delete three digits from the beginning of the dialed string, and then add 202 to the beginning of the dialed string in the new number analysis table *MyNaTable*:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic del-suffix 4 del-prefix 3
add-prefix 202
Router(config-sbc-sbe-cacpolicy-natable-ent)# exit
Router(config-sbc-sbe-cacpolicy-natable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

The following example replaces the entire carrier code identification address of dialed digits with the digits 2025551212:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-cic replace 2025551212
Router(config-sbc-sbe-cacpolicy-natable-ent)# exit
Router(config-sbc-sbe-cacpolicy-natable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

The following command sets entry 1 to delete the first digit of the carrier ID in NA table *MyNaTable*:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-account-table mytable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# edit-cic del-prefix 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)#
```

## Related Commands

Command	Description
<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.
<b>na-src-account-table</b>	Enters the mode for configuring a number analysis table within an SBE policy set, with entries that match the source account.

<b>Command</b>	<b>Description</b>
<b>edit</b>	Configures a dial-string manipulation action in number analysis and routing tables with entries of the table matching the whole dialed number.
<b>edit-src</b>	Configures a source number manipulation action in number analysis and routing tables.



# edit-src

To configure a source address manipulation action in the number analysis table and the routing table, use the **edit-src** command in the appropriate configuration mode. To remove a configured string, use the **no** form of this command.

**edit-src** [**del-prefix** *pd*] | [**del-suffix** *sd*] | [**add-prefix** *pa*] | [**replace** *ds*]

## Syntax Description

<b>del-prefix</b>	Specifies the digits to be deleted from the beginning of the dialed string.
<b>del-suffix</b>	Specifies the digits to be deleted from the end of the dialed string.
<b>add-prefix</b>	Specifies the digits to be added to the beginning of the dialed string.
<b>replace</b>	Replaces the dialed string with the configured digits.
<i>pa</i>	A string of digits to be added to the beginning of the source number string.
<i>pd</i>	A positive integer specifying the number of digits to be deleted from the beginning of the source number string.
<i>sd</i>	A positive integer specifying the number of digits to be deleted from the end of the source number string.
<i>ds</i>	A string of digits with which to replace the source number string.

## Command Default

No default behavior or values are available.

## Command Modes

Number Analysis table entry (config-sbc-sbe-rtgpolicy-natable-entry)  
 rtg-carrier-id-table entry  
 rtg-dst-address-table entry  
 rtg-dst-domain-table entry  
 rtg-round-robin-table entry  
 rtg-src-account-table entry  
 rtg-src-address-table entry  
 rtg-src-adjacency-table entry  
 rtg-src-domain-table entry  
 rtg-category-table entry  
 rtg-least-cost-table entry  
 rtg-time-table entry

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	The command was modified. The source address can now be edited in the number analysis table.

## Usage Guidelines

You cannot use this command *if the table is a part of the active policy set*.

This command is used to manipulate the source address in the number analysis table and the routing table. You can configure more than one edit action (**del-prefix**, **del-suffix**, and **add-prefix**) or combinations of edit actions, as long as you follow these rules:

- The **del-prefix**, **del-suffix**, and **add-prefix** edit-src action keywords can be combined in any order, with at least one keyword being mandatory.
- Combinations of edit-src actions are implemented from left to right. For example, the **edit-src del-prefix 3 add-prefix 919 del-suffix 4** combination command changes the dialed digit string 2025551212 into 919555.
- The **edit-src replace** action command cannot be combined with other edit actions.

Re-entering the **edit-src** command with a new combination of edit actions replaces the existing combination.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure entry 1 to delete four digits from the end of the dialed string, delete three digits from the beginning of the dialed string, and then add 202 to the beginning of the dialed string in the new number analysis table, MyNaTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# edit-src del-suffix 4 del-prefix 3
add-prefix 202
Router(config-sbc-sbe-cacpolicy-natable-ent)# exit
Router(config-sbc-sbe-cacpolicy-natable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

The following example shows how to replace the entire source address of the dialed digits with the digit 2025551212:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# edit-src replace 2025551212
Router(config-sbc-sbe-cacpolicy-natable-ent)# exit
Router(config-sbc-sbe-cacpolicy-natable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

The following command shows how to set entry 1 to delete the first digit of the source address in the *MyTable* routing table:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table mytable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit-src del-prefix 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)#
```

#### Related Commands

Command	Description
<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.
<b>edit</b>	Configures a dial-string manipulation action in the number analysis table and the routing table, with the entries in the table matching the complete dialed number.
<b>edit-cic</b>	Manipulates a carrier identification code in the number analysis table and the routing table.

# edit

To configure a string manipulation action in number analysis and routing tables with entries of the table matching the whole dialed number or the source number, use the **edit** command in NA routing table entry configuration mode. To return to the default value, use the **no** form of this command.

```
edit [del-prefix pd] | [del-suffix sd] | [add-prefix pa] | [replace ds]
```

```
no edit
```

## Syntax Description

<b>del-prefix</b>	Positive integer specifying a number of digits to delete from the front of the dialed digit string.
<b>del-suffix</b>	Positive integer specifying a number of digits to delete from the end of the dialed digit string.
<b>add-prefix</b>	String of digits to add to the front of the dialed string.
<b>replace</b>	String of digits with which to replace the dialed string.
<i>pd</i>	A positive integer specifying the number of digits to delete from the front of the carrier ID string.
<i>sd</i>	A positive integer specifying the number of digits to delete from the end of the carrier ID string.
<i>pa</i>	A string of digits to add to the front of the carrier ID string.
<i>ds</i>	A string of digits with which to replace the carrier ID string.

## Command Default

No default behavior or values are available.

## Command Modes

NA routing table entry configuration (config-sbc-sbe-rtgpolicy-natable-ent)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command is used to manipulate the source address or a destination address in number analysis and routing tables. You can configure more than one edit action (**del-prefix**, **del-suffix**, and **add-prefix**) and configure combinations of edit actions, as long as you follow the rules. The rules are as follows:

- The edit action keywords **del-prefix**, **del-suffix**, and **add-prefix** can be combined in any order, with at least one keyword required.
- Combinations of edit actions are implemented from left to right. For example, the combination **edit del-prefix 3 add-prefix 919 del-suffix 4** command changes the dialed digit string, 2025551212, into 919555.
- The **edit replace** action cannot be combined with other edit actions.

Re-entering the **edit** command with a new combination of edit actions replaces the existing combination.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to configure entry 1 to delete four digits from the end of the dialed string, delete three digits from the beginning of the dialed string, and then add 202 to the beginning of the dialed string in the new number analysis table MyNaTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit del-suffix 4 del-prefix 3 add-prefix 202
Router(config-sbc-sbe-cacpolicy-natable-ent)# exit
Router(config-sbc-sbe-cacpolicy-natable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

The following example replaces the entire address of dialed digits with the digits 2025551212:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# edit replace 2025551212
Router(config-sbc-sbe-cacpolicy-natable-ent)# exit
Router(config-sbc-sbe-cacpolicy-natable)# exit
Router(config-sbc-sbe-cacpolicy)# exit
```

### Related Commands

Command	Description
<b>edit-cic</b>	Manipulates a carrier identification code in number analysis and routing tables.
<b>edit-src</b>	Configures a source number manipulation action in number analysis and routing tables.

# editor-list

To specify the stage at which you want the editors to be applied, use the **editor-list** command in the adjacency SIP editor configuration mode. To remove the configuration of the editor list, use the **no** form of this command.

**editor-list** {after-send | before-receive}

**no editor-list** {after-send | before-receive}

## Syntax Description

<b>after-send</b>	Specifies that the outgoing message must be edited after the message is processed by the adjacency and just before it is forwarded from the adjacency.
<b>before-receive</b>	Specifies that the incoming message must be edited just after it is received on the adjacency and before the adjacency begins processing it.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP editor configuration (config-sbc-sbe-adj-sip-ed)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

Note that the editors must be configured before you run this command.

## Examples

In the following example, the **editor-list** command is used to specify that the editors must be applied to the messages after the messages are received:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip my_adjacency
Router(config-sbc-sbe-adj-sip)# editor-type editor
Router(config-sbc-sbe-adj-sip)# editor-list after-send
```

Related Commands	Command	Description
	<b>active-script-set</b>	Activates a script set,
	<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
	<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
	<b>editor</b>	Specifies the order in which a particular editor must be applied.
	<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
	<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
	<b>load-order</b>	Specifies the load order of a script in a script set.
	<b>script</b>	Configures a script written using the Lua programming language.
	<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
	<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
	<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
	<b>sip header-editor</b>	Configures a header editor.
	<b>sip method-editor</b>	Configures a method editor.
	<b>sip option-editor</b>	Configures an option editor.
	<b>sip parameter-editor</b>	Configures a parameter editor.
	<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
	<b>test script-set</b>	Tests the working of a script set.
	<b>type</b>	Specifies the type of a script written using the Lua programming language.

# editor-type

To configure an editor type for a SIP adjacency to apply, use the **editor-type** command in the SIP adjacency configuration mode. To unconfigure an editor type, use the **no** form of this command.

**editor-type** { **editor** | **profile** }

**no editor-type**

## Syntax Description

<b>editor</b>	Uses the method, header, option, parameter, or body editor.
<b>profile</b>	Uses the method, header, option, parameter, or body profile.

## Command Default

No default behavior or values are available.

## Command Modes

SIP adjacency configuration (config-sbc-sbe-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure an editor type for a SIP adjacency to apply:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency SIP SIPP
Router(config-sbc-sbe-sip)# editor-type editor
```

## Related Commands

Command	Description
<b>sip method-editor</b>	Configures a method editor.
<b>sip header-editor</b>	Configures a header editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>sip body-editor</b>	Configures a body editor.
<b>sip option-editor</b>	Configures an option editor.





# editor

If multiple editors have been configured in an editor list, to specify the order in which a particular editor must be applied in the sequence defined by the list, use the **editor** command in the adjacency SIP editor configuration mode. To remove the configuration of the editor, use the **no** form of this command.

**editor** *order-number editor-name* [**condition** [**body contains sdp**]]

**no editor** *order-number editor-name* [**condition** [**body contains sdp**]]

## Syntax Description

<i>order-number</i>	Order in which the editor must be applied.
<i>editor-name</i>	Name of the editor that you want to apply to messages that are processed by the adjacency.
<b>condition</b>	Specifies that there are one or more conditions for the editor to be applied.
<b>body contains sdp</b>	Specifies that the message body must contain SDP-based content. The editor is applied only if this condition is met. Include <b>body contains sdp</b> in the command for script-based editors.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP editor configuration (config-sbc-sbe-adj-sip-ed)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **editor** command is used to set the load order for the my\_editor editor to 4. A header editor is configured in this example.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip editor-type editor
Router(config-sbc-sbe)# sip parameter-editor my_parameter_editor
Router(config-sbc-sbe-mep-prm)# exit
Router(config-sbc-sbe)# sip header-editor my_header_editor
Router(config-sbc-sbe-mep-hdr)# exit
Router(config-sbc-sbe)# adjacency sip my_adjacency
```

```

Router(config-sbc-sbe-adj-sip)# editor-type editor
Router(config-sbc-sbe-adj-sip)# header-editor inbound my_header_editor
Router(config-sbc-sbe-adj-sip)# editor-list after-send
Router(config-sbc-sbe-adj-sip-ed)# editor 4 my_editor condition body contains sdp

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>active-script-set</b>	Activates a script set,
<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# entry

To create or modify an entry in a table or an SDP media profile, use the **entry** command in the appropriate configuration mode. To destroy the given entry, use the **no** form of this command.

**entry** *entry-id*

**no entry** *entry-id*

## Syntax Description

*entry-id* Specifies the table entry.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)  
 NA routing table configuration (config-sbc-sbe-rtgpolicy-natable)  
 RTG routing table configuration (config-sbc-sbe-rtgpolicy-rtgtable)  
 SIP SDP media profile configuration (config-sbc-sbe-sip-sdp-media)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	Command usage was expanded to support SDP media profiles for the Customized Option for Late-to-Early Media Interworking.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

You cannot change the configuration of tables in the context of the active policy set. An entry may not be destroyed if the table is a part of the active policy set.

## Examples

The following example shows how to create an entry in the new admission control table, MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

# entry (enum)

To configure the ENUM client entry name and enter the ENUM entry configuration mode, use the **entry (enum)** command in SBE configuration mode. To remove the ENUM client entry name, use the no form of this command.

**entry** *entry-name*

**no entry** *entry-name*

## Syntax Description

<i>entry-name</i>	ENUM client entry name.
-------------------	-------------------------

## Command Default

No default behavior or values are available.

## Command Modes

ENUM configuration (config-sbc-sbe-enum)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the ENUM client entry name:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# entry ENUM_1
```

## Related Commands

Command	Description
<b>activate (enum)</b>	Activates ENUM client.
<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.

<b>Command</b>	<b>Description</b>
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe</b> <b>call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum</b> <b>entry</b>	Displays the contents of an ENUM client entry.

# enum

To configure the ENUM client ID number and enter the ENUM configuration mode, use the **enum** command in SBE configuration mode. To remove the ENUM client ID number, use the no form of this command.

```
enum enum-id
```

```
no enum enum-id
```

<b>Syntax Description</b>	<i>enum-id</i> ENUM client ID number. Currently, only the number 1 is allowed.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The ENUM ID number is used by the Routing Policy Service (RPS) to initiate service requests.

At the SBE level, multiple ENUM client entries can be provisioned.

**Examples**

The following example shows how to configure the ENUM client ID number and enter the ENUM configuration mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).

<b>Command</b>	<b>Description</b>
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.



# error-profile

To configure an existing error profile as the outbound SIP error profile, use the **error-profile outbound** command in adjacency SIP configuration mode. To remove an error profile as the SIP error profile, use the no form of this command.

**error-profile outbound** *profile-name*

**no error-profile outbound** *profile-name*

<b>Syntax Description</b>	<i>profile-name</i>	Name of the existing error profile to be used as the inbound or outbound SIP error profile.
---------------------------	---------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure an existing error profile as the outbound SIP error profile:
-----------------	---

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip MySIP
Router(config-sbc-sbe-adj-sip) error-profile outbound OUT_Err_profile_1
Router(config-sbc-sbe-adj-sip)
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>error-profile</b>	Configures an existing error profile as the outbound SIP error profile.
	<b>sip error-profile</b>	Creates an error profile and enters error profile configuration mode.
	<b>cause</b>	Configures the cause of an internal error for an error profile.
	<b>show sbc sbe sip error-profile</b>	Displays the configuration information of an error profile.

# exit-if-vnet

To exit virtual network interface mode, use the **exit-if-vnet** command in virtual network interface mode.

**exit-if-vnet**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Virtual network interface mode (config-if-vnet)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

**Usage Guidelines** This command is not saved in a configuration and therefore does not appear in **show running-config** output.

The **exit-if-vnet** command is one of the commands that will be displayed in system help if you enter a ? at the Router(config-if-vnet)# prompt. However, the **exit** command performs the same function as the **exit-if-vnet** command and is a shorter command to enter.

**Examples** The following example shows how to exit virtual network interface mode:

```
Router(config)# vrf definition red
Router(config-vrf)# vnet tag 100
R1(config-vrf)# description guest access
R1(config-vrf)# address-family ipv4
R1(config-vrf-af)# exit-address-family
R1(config-vrf)# vrf definition blue
R1(config-vrf)# vnet tag 200
R1(config-vrf)# description Finance
R1(config-vrf)# address-family ipv4
R1(config-vrf-af)# exit-address-family
R1(config-vrf)# interface fastethernet 1/1/1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# vnet trunk
R1(config-if)# vnet name blue
R1(config-if-vnet)# exit-if-vnet
R1(config-if)#
```

Related Commands	Command	Description
	<b>exit</b>	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.
	<b>vnet</b>	Configures overrides of an interface's attributes on a per-VRF basis and enters virtual network interface mode.

# exit-route-server-context

To exit a route server context and return to router configuration mode, use the **exit-route-server-context** command in route server context configuration mode.

## exit-route-server-context

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Route server context configuration (config-router-rsctx)

Command History	Release	Modification
	Cisco IOS XE 3.3S	This command was introduced.

**Usage Guidelines** When you configure a BGP route server with a flexible policy, you create a route server context with an import map, which is when you might use the **exit-route-server-context** command. The **exit-route-server-context** command is one of the commands that will be displayed in system help if you enter a ? at the Router(config-router-rsctx)# prompt. However, the **exit** command performs the same function as the **exit-route-server-context** command.

**Examples** In the following example, a route server context is created and the **exit-route-server-context** command is used to exit route server context configuration mode:

```
router bgp 65000
  route-server-context ONLY_AS27_CONTEXT
  address-family ipv4 unicast
    import-map only_AS27_routemap
  exit-address-family
  exit-route-server-context
  !
Router(config)#
```

Related Commands	Command	Description
	<b>route-server-context</b>	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

# exit-vrf-list

To exit VRF list submode, use the **exit-vrf-list** command in VRF list submode.

**exit-vrf-list**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** VRF list submode (config-vrf-list)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

**Usage Guidelines** This command is not saved in a configuration and therefore does not appear in **show running-config** output.

The **exit-vrf-list** command is one of the commands that will be displayed in system help if you enter a ? at the Router(config-vrf-list)# prompt. However, the **exit** command performs the same function as the **exit-vrf-list** command and is a shorter command to enter.

**Examples** The following example shows how to exit VRF list submode:

```
Router(config)# vrf list external
Router(config-vrf-list)# member blue
Router(config-vrf-list)# exit-vrf-list
Router(config)#
```

Related Commands	Command	Description
	<b>exit</b>	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.
	<b>vrf list</b>	Defines a list of VRFs.

# expires-header

To configure expires parameter in the SIP contact header, use the **expires-header** command in adjacency SIP configuration mode. To remove an expires parameter from the header, use the no form of this command.

**expires-header** *options*

**no expires-header** *options*

## Syntax Description

*options*

The options for the expires header parameters are:

- *add-not-present*—SBC provides expiry information in the format provided by the endpoint, or as indicated by other configurations.
- *add-smallest*—The value of the expires header is set to the value of the smallest expires parameter on any provided contact.
- *add-value*—SBC adds an expires header to any REGISTER request sent out on the specified adjacency that does not contain an expiry value.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

### Release

### Modification

Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
---------------------------	--

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure an expires header parameter on the SIP contact header:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip) expires-header add-not-present
Router(config-sbc-sbe-adj-sip)
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>softswitch-shield</b>	Configures softswitch shielding support on SIP adjacency.
<b>show sbc sbe adjacencies</b>	Displays all the detailed field output pertaining to a specified Session Initiation Protocol (SIP) adjacency.

# fast-register-interval

To configure the fast-path register interval (in seconds), use the **fast-register-interval** command in adjacency SIP configuration mode. To unconfigure the fast-path register interval, use the **no** form of this command.

**fast-register-interval** *interval*

**no fast-register-interval**

<b>Syntax Description</b>	<i>interval</i> Specifies the interval value in seconds. Range is 1 to 2000000.
---------------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

If fast-path register support is enabled on this adjacency, this is the minimum expiry period accepted on a subscriber registration. The interval at which registrations are forwarded on to the softswitch is governed by the registration minimum expiry value.

 **Note**

The *interval* must be less than the *minimum expiry* value.

<b>Examples</b>	The following example shows how to enable the fast-register interval on the SIP adjacency SipToIsp42 to 10 seconds:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# fast-register-interval 10
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>fast-register disable</b>	Disables fast-path register support on the SIP adjacency.

# fast-register disable

To disable fast-path register support on the SIP adjacency, use the **fast-register disable** command in adjacency SIP configuration mode. To enable fast-path register support, use the **no** form of this command.

**fast-register disable**

**no fast-register disable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Fast-path register is used to prevent the SBC from forwarding all SIP register messages to the softswitch, thus reducing the load on the softswitch. This is enabled by default and can be disabled using this command. When active, a SIP register message received from the same host and port as an existing registration, and with a nonzero expires interval, is immediately responded to without further parsing or other processing performed.

**Examples** The following example shows how to disable fast-path register support on the SIP adjacency SipToIsp42:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# fast-register disable
```

Related Commands	Command	Description
	<b>fast-register-interval</b>	Configures the fast-path register interval.



# filename (session border controller)

To specify the path and name of the script file written using the Lua programming language, use the **filename** command in the SBE script-set script configuration mode.

**filename** *{device-type:file-path-and-name}*

## Syntax Description

<i>device-type</i>	<p>One of the following or any other storage device installed on the router:</p> <ul style="list-style-type: none"> <li>• <b>bootflash:</b></li> <li>• <b>flash:</b></li> <li>• <b>fpd:</b></li> <li>• <b>nvram:</b></li> <li>• <b>obfl:</b></li> </ul> <p>The list of file system devices is dynamically generated and displayed. Other devices, such as a hard disk, that are available on the platform can also be used in this command.</p>
<i>file-path-and-name</i>	Full path and name of the script file on the specified storage device.

## Command Default

No default behavior or values are available.

## Command Modes

SBE script-set script configuration (config-sbc-sbe-scrpset-script)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **filename** command specifies that the script file is mySBCScript.lua and is located on the bootflash device:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# script-set 10 lua
Router(config-sbc-sbe-script-set)# script mySBCScript
Router(config-sbc-sbe-scrpset-script)# load-order 2
Router(config-sbc-sbe-scrpset-script)# type wrapped edit-point both
```

```
Router(config-sbc-sbe-scrpset-script)# filename bootflash:mySBCScript.lua
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>active-script-set</b>	Activates a script set,
<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
<b>editor</b>	Specifies the order in which a particular editor must be applied.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# first-cac-scope

To configure the scope at which to begin defining limits when performing the admission control stage of policy, use the **first-cac-scope** command in CAC-policy-set configuration mode. Use the **no** form of this command to delete the routing table.

**first-cac-scope** *scope-name*

**no first-cac-scope**

## Syntax Description

*scope-name*

Specifies the scope at which limits should be initially defined when performing the admission control stage of policy. Possible values are:

- **adj-group**—Limits for events from members of the same adjacency group.
- **call**—Limits are per single call.
- **category**—Limits per category.
- **dst-account**—Limits for events sent to the same account.
- **dst-adj-group**—Limits for events sent to the same adjacency group.
- **dst-adjacency**—Limits for events sent to the same adjacency.
- **dst-number**—Limits for events that have the same adjacency number.
- **global**—Limits are global (May not be combined with any other option).
- **src-account**—Limits for events from the same account.
- **src-adj-group**—Limits for events from the same adjacency group.
- **src-adjacency**—Limits for events from the same adjacency.
- **src-number**—Limits for events that have the same source number.
- **sub-category-pfx** *prefix-len*—The limits specified at this scope apply to all events sent to or received from members of the same subscriber category prefix.

**Note** The prefix-len is included as part of the **first-cac-scope** command. For example, the command would be: **first-cac-scope sub-category-pfx prefix-len**.

## Command Default

No default behavior or values are available.

## Command Modes

CAC-policy-set configuration (config-sbc-sbe-cacpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	The <b>sub-category-pfx</b> <i>prefix-len</i> scope was added.

---

**Usage Guidelines**

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

---

**Examples**

The following example shows how to set the scope category as the first scope at which to define an admission control policy in configuration set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-scope src-adjacency
```

# first-cac-table

To configure the name of the first policy table to process when performing the admission control stage of policy, use the **first-cac-table** command in CAC-policy-set configuration mode. To remove this configuration, use the **no** form of this command.

**first-cac-table** *table-name*

**no first-cac-table**

<b>Syntax Description</b>	<i>table-name</i>	Specifies the admission control table that should be processed first.
---------------------------	-------------------	---

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	CAC-policy-set configuration (config-sbc-sbe-cacpolicy)	
----------------------	---	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to set the table RootCacTable as the first admission control table in configuration set 1 on mySbc:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table RootCacTable
```

# first-call-routing-table

To configure the name of the first policy table to process when performing the routing stage of policy for new-call events, use the **first-call-routing-table** command in routing policy table mode. To unconfigure the name of the first policy table, use the **no** form of this command.

**first-call-routing-table** *table-name*

**no first-call-routing-table**

## Syntax Description

<i>table-name</i>	Specifies the routing table that should be processed first.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

Routing policy table (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the table RootCallRtgTable as the first routing table for new-call events in configuration set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# first-call-routing-table RootCallRtgTable
```

# first-inbound-na-table

To configure the name of the first inbound policy table to be processed when performing the number analysis stage of a policy, use the **first-inbound-na-table** command in the Routing policy table configuration mode. To unconfigure the name of the first inbound policy table, use the **no** form of this command.

**first-inbound-na-table** *table-name*

**no first-inbound-na-table**

Syntax Description	<i>table-name</i>	The number analysis table that should be processed first.
--------------------	-------------------	---

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	Routing policy table (config-sbc-sbe-rtgpolicy)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. This <b>first-number-analysis-table</b> command was renamed as the <b>first-inbound-na-table</b> command.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
------------------	--

Examples	The following example shows how to configure the table RootNaTable as the first inbound number analysis table in configuration set 1 on mySbc:
----------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# first-inbound-na-table RootNaTable
```

Related Commands	Command	Description
	<b>call-policy-set</b>	Creates a new policy set on the Session Border Controller (SBC).
	<b>call-policy set default</b>	Configures a default policy set on the signaling border element (SBE) entity.
	<b>first-outbound-na-table</b>	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.

<b>Command</b>	<b>Description</b>
<b>show sbc sbe call-policy-set</b>	Lists the details of the policy sets configured on the SBC.
<b>show sbc sbe call-policy-set default</b>	Lists the summary of the default policy set configured on the SBC.



# first-outbound-na-table

To configure the name of the first outbound policy table to be processed when performing the number analysis stage of a policy, use the **first-outbound-na-table** command in the Routing policy table configuration mode. To deconfigure the name of the first outbound policy table, use the **no** form of this command.

**first-outbound-na-table** *table-name*

**no first-outbound-na-table**

<b>Syntax Description</b>	<i>table-name</i> The number analysis table that should be processed first.
---------------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Routing policy table (config-sbc-sbe-rtgpolicy)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the table RootOutTable as the first outbound number analysis table in configuration set 1 on mySbc:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# first-outbound-na-table RootOutTable
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>call-policy-set</b>
	<b>call-policy set default</b>	Configures a default policy set on the signaling border element (SBE) entity.
	<b>first-inbound-na-table</b>	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.

<b>Command</b>	<b>Description</b>
<b>show sbc sbe call-policy-set</b>	Lists the details of the policy sets configured on the SBC.
<b>show sbc sbe call-policy-set default</b>	Lists the summary of the default policy set configured on the SBC.

# first-reg-routing-table

To configure the name of the first policy table to process when performing the routing stage of policy for subscriber-registration events, use the **first-reg-routing-table** command in routing policy table configuration mode. To deconfigure the name of the first policy table, use the **no** form of this command.

**first-reg-routing-table** *table-name*

**no first-reg-routing-table**

<b>Syntax Description</b>	<i>table-name</i>	Specifies the routing table that should be processed first.
---------------------------	-------------------	---

**Command Default** No default behavior or values are available.

**Command Modes** Routing policy table (config-sbc-sbe-rtgpolicy)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the table RootRegRtgTable as the first routing table for subscriber-registration events in configuration set 1 on mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# first-reg-routing-table RootRegRtgTable
```

# flipped-interval (XML Billing)

To configure the maximum interval at which to flip a billing XML file, use the **flipped-interval** command in the SBE billing XML configuration mode. To reset the flip interval to its default value of 3 minutes, use the **no** form of this command.

**flipped-interval** *seconds*

**no flipped-interval**

<b>Syntax Description</b>	<i>seconds</i>	Time after which the CDRs being stored in the existing XML file is stopped and flipped to a new XML billing file. The interval at which to switch from one XML file to another XML file can be specified in seconds ranging from 60 to 86400. The default interval is 180 seconds.
---------------------------	----------------	--

<b>Command Default</b>	By default, the flip interval is 3 minutes (180 seconds).	
------------------------	---	--

<b>Command Modes</b>	SBE billing XML configuration (config-sbc-sbe-billing-xml)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

<b>Usage Guidelines</b>	The XML billing files are stored under the CDR path configured by the administrator. An XML billing file is generated for CDRs at regular intervals and not exceeding the defined flip size. To switch the XML billing file from one XML file to another, use the <b>flipped-interval</b> <i>seconds</i> command from the SBE billing xml configuration mode. The default interval to flip an XML billing file is 3 minutes.
-------------------------	--

<b>Examples</b>	<p>The following example shows how to set the flip interval to 5 minutes (300 seconds):</p> <pre>Router(config)# <b>sbc sbcbilling</b> Router(config-sbc)# <b>sce</b> Router(config-sbc-sce)# <b>billing</b> Router(config-sbc-sce-billing)# <b>xml method</b> Router(config-sbc-sce-billing)# <b>xml 1</b> Router(config-sbc-sce-billing-xml)# <b>flipped-interval 300</b></pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>xml (billing)</b>	Configures the method index for XML billing.
	<b>method xml</b>	Configures the billing method as XML for the Billing Manager.
	<b>ldr-check</b>	Configures the time at which long duration records are checked.

## flipped-size (XML Billing)

To configure the maximum file-size, that if exceeds, leads to the flipping of the billing XML file, use the **flipped-size** command in the SBE billing XML configuration mode. To reset the flip-size to its default value of 10 MB, use the **no** form of this command.

**flipped-size** *size*

**no flipped-size**

<b>Syntax Description</b>	<i>size</i>	The file size, which, if exceeds, leads to the CDRs stored in the existing XML file being stopped and flipped to a new XML billing file. The flip size can be specified in Kilo Bytes (KB) ranging from 5120 to 512000. The default file size is 10 MB or 10240 KB.								
<b>Command Default</b>	By default, the maximum size of billing file after which the billing file is flipped to a new file, is 10 MB.									
<b>Command Modes</b>	SBE billing XML configuration (config-sbc-sbe-billing-xml)									
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>3.2S</td> <td>This command was introduced on the Cisco ASR 1000 Series Routers.</td> </tr> </tbody> </table>	Release	Modification	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.					
Release	Modification									
3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.									
<b>Usage Guidelines</b>	The XML billing files are stored in the CDR path configured by the administrator. An XML billing file is generated for the CDR at regular intervals not exceeding the defined flip-size. To switch the XML billing file from one XML file to another after the flip size is exceeded, execute the <b>flipped-size</b> <i>size</i> command from the SBE billing XML configuration mode. The default file size to flip an XML billing file is 10 MB.									
<b>Examples</b>	<p>The following example shows how to set the flip size to 512000:</p> <pre>Router(config)# sbc sbcbilling Router(config-sbc)# sbe Router(config-sbc-sbe)# billing Router(config-sbc-sbe-billing)# xml method Router(config-sbc-sbe-billing)# xml 1 Router(config-sbc-sbe-billing-xml)# flipped-size 512000</pre>									
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>xml (billing)</b></td> <td>Configures the method index for XML billing.</td> </tr> <tr> <td><b>method xml</b></td> <td>Configures the billing method as XML for the Billing Manager.</td> </tr> <tr> <td><b>ldr-check</b></td> <td>Configures the time at which long duration records are checked.</td> </tr> </tbody> </table>	Command	Description	<b>xml (billing)</b>	Configures the method index for XML billing.	<b>method xml</b>	Configures the billing method as XML for the Billing Manager.	<b>ldr-check</b>	Configures the time at which long duration records are checked.	
Command	Description									
<b>xml (billing)</b>	Configures the method index for XML billing.									
<b>method xml</b>	Configures the billing method as XML for the Billing Manager.									
<b>ldr-check</b>	Configures the time at which long duration records are checked.									

# fntp (codec variant)

To define the format-specific parameters for a variant, use the **fntp** command in the Codec variant configuration mode. To remove the defined format-specific parameters, use the **no** form of this command.

**fntp** *fntp-string*

**no fntp**

<b>Syntax Description</b>	<i>fntp-string</i>	The format-specific parameter string in the <i>name=value</i> format.
---------------------------	--------------------	---

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Codec variant configuration (config-sbc-sbe-codec-var-codec)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

To view the default format-specific parameters values associated with variants, use the **show sbc sbe codecs variant** command.

**Examples**

The following example shows how to define the format-specific parameters for a variant in the Codec variant configuration mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant codec G723-H-1
Router(config-sbc-sbe-codec-var-codec)# fntp bitrate=6.3
```

## fntp (session border controller)

To configure the default value of the format-specific parameters for Session Description Protocol (SDP), use the **fntp** command in the Codec system configuration mode. To remove the default value of the format-specific parameters, use the **no** form of this command.

**fntp** *fntp-string*

**no fntp**

<b>Syntax Description</b>	<i>fntp-string</i>	The format-specific parameter string for SDP, in the <i>name=value</i> format.
---------------------------	--------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Codec system configuration (config-sbc-sbe-codec-def)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	<p>When a codec is converted from a standard to a variant representation, the default format-specific parameters, if any, are stripped out of the resulting SDP. However, when the format-specific parameters under codec variant in a codec variant contains parameters that match the default format-specific parameters for the variant's standard codec, those parameters are deemed matched in SDP if either one of the following is true:</p> <ul style="list-style-type: none"> <li>The exact '<i>&lt;name&gt;=&lt;value&gt;</i>' parameter has been received.</li> <li>No parameters that start with '<i>&lt;name&gt;=</i>' have been received.</li> </ul> <p>To view the default format-specific parameters values associated with standard codecs, use the <b>show sbc sbe codecs</b> command.</p> <p>To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.</p>
-------------------------	---

<b>Examples</b>	<p>The following example shows how to configure the default value of the format-specific parameters for SDP using the <b>fntp</b> command in the Codec system configuration mode:</p>
-----------------	---

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system G723 id 4
Router(config-sbc-sbe-codec-def)# fntp annexa=yes
```

# force-signaling-peer

To force the Session Initiation Protocol (SIP) messages for either only out-of-dialog requests (that is, dialog-creating requests) or both in-dialog and out-of-dialog requests to go to a configured signaling peer, use the **force-signaling-peer** command in adjacency SIP configuration mode. To disable this feature, use the **no** form of this command.

**force-signaling-peer [all]**

**no force-signaling-peer [all]**

<b>Syntax Description</b>	<b>all</b>	Forces the hop to a configured signaling peer for both in-dialog requests and out-of-dialog requests.
---------------------------	------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.1S	The <b>all</b> keyword was added.	

<b>Usage Guidelines</b>	While configuring redundant peer addresses, you must include the <b>all</b> keyword in the command. This is to force SIP messages for both in-call requests and out-of-call requests to go to the configured signaling peer.
-------------------------	--

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

<b>Examples</b>	The following example shows how to force SIP messages to go to a configured signaling peer in the context of both in-dialog and out-of-dialog requests:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# force-signaling-peer all
Router(config-sbc-sbe-adj-sip)# exit
```

<b>Related Commands</b>	<b>redundant peer</b>	Configures an alternative signaling peer for an adjacency.
-------------------------	-----------------------	--



---

<b>signaling-peer-priority</b>	Configures the priority of a signaling peer on a SIP adjacency.
<b>signaling-peer-switch</b>	Configures a SIP adjacency to switch the signaling peer to an available destination.

---

# g107a-factor

To set the Advantage (A) factor, use the **g107a-factor** command in the adjacency H.323 configuration mode or adjacency SIP configuration mode. The Advantage factor is one of the parameters used in the calculation of the MOS-CQE score. To remove the Advantage factor setting, use the **no** form of this command.

**g107a-factor** *factor-number*

**no g107a-factor**

## Syntax Description

<i>factor-number</i>	Value of the Advantage factor. The range is from 0 to 20.
----------------------	---

## Command Default

By default, the value of *factor-number* is 0.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

The following example shows how to configure the Advantage factor by using the **g107a-factor** command in the adjacency H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 adj1
Router(config-sbc-sbe-adj-h323)# g107a-factor 10
```

## Related Commands

Command	Description
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
<b>current15minutes</b>	Specifies that QoS statistics must be calculated for 15-minute intervals.
<b>current5minutes</b>	Specifies that QoS statistics must be calculated for 5-minute intervals.
<b>currentday</b>	Specifies that statistics must be calculated for 24-hour intervals.
<b>currenthour</b>	Specifies that QoS statistics must be calculated for 60-minute intervals.

<b>Command</b>	<b>Description</b>
<b>currentindefinite</b>	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
<b>g107 bpl</b>	Sets a value for the Packet-Loss Robustness (Bpl) factor.
<b>g107 ie</b>	Sets a value for the Equipment Impairment (Ie) factor.
<b>local-jitter-ratio</b>	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
<b>show sbc sbe adjacencies</b>	Displays details of the adjacencies configured on the SBE.
<b>show sbc sbe call-stats</b>	Displays the statistics pertaining to all the calls on a the SBE.
<b>snmp-server enable traps sbc</b>	Enables SBC notification types.
<b>statistics</b>	Specifies the QoS statistic for which alert levels must be set.

# g107 bpl

To set the Packet-Loss Robustness (Bpl) factor, use the **g107 bpl** command in the codec definition mode. The Packet-Loss Robustness factor is one of the parameters used in the calculation of the MOS-CQE score. To remove the Packet-Loss Robustness factor setting, use the **no** form of this command.

**g107 bpl** *factor-number*

**no g107 bpl**

## Syntax Description

<i>factor-number</i>	Value of the Packet-Loss Robustness factor. The range is from 1 to 40.
----------------------	--

## Command Default

By default, the value of *factor-number* is 1.

## Command Modes

Codec definition mode (config-sbc-sbe-codec-def)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

The following example shows how to configure the Packet-Loss Robustness factor by using the **g107 bpl** command in the adjacency H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system PCMU id 0
Router(config-sbc-sbe-codec-def)# g107 bpl 30
```

## Related Commands

Command	Description
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
<b>current15minutes</b>	Specifies that QoS statistics must be calculated for 15-minute intervals.
<b>current5minutes</b>	Specifies that QoS statistics must be calculated for 5-minute intervals.
<b>currentday</b>	Specifies that statistics must be calculated for 24-hour intervals.
<b>currenthour</b>	Specifies that QoS statistics must be calculated for 60-minute intervals.

<b>Command</b>	<b>Description</b>
<b>currentindefinite</b>	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
<b>g107 ie</b>	Sets a value for the Equipment Impairment (Ie) factor.
<b>g107a-factor</b>	Sets a value for the Advantage (A) factor.
<b>local-jitter-ratio</b>	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
<b>show sbc sbe adjacencies</b>	Displays details of the adjacencies configured on the SBE.
<b>show sbc sbe call-stats</b>	Displays the statistics pertaining to all the calls on a the SBE.
<b>snmp-server enable traps sbc</b>	Enables SBC notification types.
<b>statistics</b>	Specifies the QoS statistic for which alert levels must be set.

# g107 ie

To set the Equipment Impairment (Ie) factor, use the **g107 ie** command in the codec definition mode. The Equipment Impairment factor is one of the parameters used in the calculation of the MOS-CQE score. To remove the Equipment Impairment factor setting, use the **no** form of this command.

**g107 ie** *factor-number*

**no g107 ie**

## Syntax Description

<i>factor-number</i>	Value of the Equipment Impairment factor. The range is from 0 to 50.
----------------------	--

## Command Default

By default, the value of *factor-number* is 0.

## Command Modes

Codec definition mode (config-sbc-sbe-codec-def)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

The following example shows how to configure the Equipment Impairment factor by using the **g107 ie** command in the adjacency H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system PCMU id 0
Router(config-sbc-sbe-codec-def)# g107 ie 20
```

## Related Commands

Command	Description
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
<b>current15minutes</b>	Specifies that QoS statistics must be calculated for 15-minute intervals.
<b>current5minutes</b>	Specifies that QoS statistics must be calculated for 5-minute intervals.
<b>currentday</b>	Specifies that statistics must be calculated for 24-hour intervals.
<b>currenthour</b>	Specifies that QoS statistics must be calculated for 60-minute intervals.

<b>Command</b>	<b>Description</b>
<b>currentindefinite</b>	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
<b>g107 bpl</b>	Sets a value for the Packet-Loss Robustness (Bpl) factor.
<b>g107a-factor</b>	Sets a value for the Advantage (A) factor.
<b>local-jitter-ratio</b>	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
<b>show sbc sbe adjacencies</b>	Displays details of the adjacencies configured on the SBE.
<b>show sbc sbe call-stats</b>	Displays the statistics pertaining to all the calls on a the SBE.
<b>snmp-server enable traps sbc</b>	Enables SBC notification types.
<b>statistics</b>	Specifies the QoS statistic for which alert levels must be set.

# generic-stream callee

To configure the generic media stream list settings for a callee, use the **generic-stream callee** command in the CAC table entry configuration mode. To deconfigure the generic media stream list settings, use the **no** form of this command.

**generic-stream callee** *generic-stream-list*

**no generic-stream callee**

## Syntax Description

<i>generic-stream-list</i>	The name of the generic stream list. This generic stream list should be defined during the configuration of the stream list.
----------------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the generic media stream list settings for a callee using the **generic-stream callee** command in the CAC table entry mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# stream-list my-stream
Router(config-sbc-sbe-stream-list)# exit
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# cac-table 2
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# generic-stream callee my-stream
```



# generic-stream caller

To configure the generic media stream list settings for a caller, use the **generic-stream caller** command in the CAC table entry configuration mode. To deconfigure the generic media stream list settings, use the **no** form of this command.

**generic-stream caller** *generic-stream-list*

**no generic-stream caller**

<b>Syntax Description</b>	<i>generic-stream-list</i>	The name of the generic stream list. This generic stream list should be defined during the configuration of the stream list.
---------------------------	----------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.
-------------------------	---

<b>Examples</b>	The following example shows how to configure the generic media stream list settings for a caller using the <b>generic-stream caller</b> command in the CAC table entry mode:
-----------------	--

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# stream-list my-stream
Router(config-sbc-sbe-stream-list)# exit
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# cac-table 2
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# generic-stream caller my-stream
```

# generic-stream media-type

To configure the media type for a generic stream, use the **generic-stream media-type** command in the Stream list configuration mode. To deconfigure the media type for a generic stream, use the **no** form of this command.

```
generic-stream media-type { application | message } transport udp protocol protocol-name
```

```
no generic-stream media-type { application | message } transport udp protocol protocol-name
```

## Syntax Description

<b>application</b>	Specifies <b>application</b> as media type for the generic stream.
<b>message</b>	Specifies <b>message</b> as media type for the generic stream.
<b>transport</b>	Configures the transport protocol for the generic stream.
<b>udp</b>	Specifies the UDP protocol for the generic stream.
<b>protocol</b>	Specifies the protocol name for the generic stream.
<i>protocol-name</i>	The protocol name for the generic stream. The protocol name is case sensitive.

## Command Default

No default behavior or values are available.

## Command Modes

Stream list configuration (config-sbc-sbe-stream-list)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure **application** as the media type for the generic stream using the **generic-stream media-type** command in the Stream list configuration mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# stream-list my-stream
Router(config-sbc-sbe-stream-list)# generic-stream media-type application transport udp protocol BFCP
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show sbc sbe stream-list</b>	Displays the stream lists that are present on the SBE.
<b>stream-list</b>	Configures a stream list.

# generic-stream branch

To configure the generic media stream list settings for a caller or a callee, use the **generic-stream branch** command in the CAC table entry configuration mode. To unconfigure the generic media stream list settings, use the **no** form of this command.

**generic-stream branch** *generic-stream-list*

**no generic-stream branch**

## Syntax Description

<i>generic-stream-list</i>	Name of the generic stream list. This list must be defined during the configuration of the stream list.  The <i>generic-stream-list</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
----------------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the generic media stream list settings by using the **generic-stream branch** command:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# stream-list my-stream
Router(config-sbc-sbe-stream-list)# exit
Router(config-sbc-sbe)# cac-policy-set 2
Router(config-sbc-sbe-cacpolicy)# cac-table 2
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit src-adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# generic-stream branch my-stream
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>generic-stream callee</b>	Configures the generic media stream list settings for a callee.
<b>generic-stream caller</b>	Configures the generic media stream list settings for a caller.

# global

To enter the mode for configuring blacklisting to apply to all addresses, use the **global** command in the SBE blacklist configuration mode.

*global*

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBE blacklist configuration (config-sbc-sbe-blacklist)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to enter the mode for configuring blacklisting to apply to all addresses:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# global
Router(config-sbc-sbe-blacklist-global)#
```

Related Commands	Command	Description
	<b>blacklist</b>	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	<b>ipv4 (blacklist)</b>	Enters the mode for applying blacklisting options to a single IP address.
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source.
	<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
	<b>trigger-period</b>	Defines the period over which events are considered.
	<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.



# group (session border controller)

To configure an adjacency to an adjacency group, use the **group** command in the appropriate adjacency mode. To remove the adjacency from the specified group, use the **no** form of this command.

**group** *word*

**no group** *word*

## Syntax Description

<i>word</i>	Indicates the group name for the adjacency. The maximum size is 32 characters.
-------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **group** command assigns a SIP adjacency named sipGW to adjacency group named InternetEth0:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip sipGW
Router(config-sbc-sbe-adj-sip)# group InternetEth0
```

The following example shows how the **group** command assigns an H.323 adjacency named H323ToIsp42 to an adjacency group named Isp42.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 H323ToIsp42
Router(config-sbc-sbe-adj-h323)# group Isp42
```







## h225 address

To configure the sourceAddress and destinationAddress fields of an H.225 message in the H.323 adjacency, use the **h225 address** command in the H.323 adjacency configuration mode. To return to the default value, use the **no** form of this command.

```
h225 address {block | usage {e164 | h323id}}
```

```
no h225 address {block | usage}
```

Syntax Description		
<b>block</b>	Specifies that the sourceAddress and destinationAddress in a H.225 message are not passed through.	
<b>usage</b>	Specifies the interpretation of the H.225 sourceAddress and destinationAddress fields in an adjacency when Q.931 callingPartyNumber or calledPartyNumber is not present.	
<b>e164</b>	Specifies the e164 format for the addresses. All the other formats are ignored.	
<b>h323id</b>	If the field begins with a numeric prefix, such as [0123456789*.] of 6 or greater characters, it is used as either the calling party number or the called party number, and the rest of the ID is ignored.	

**Command Default** By default, the sourceAddress and destinationAddress in a H.225 message are not blocked. The H.225 sourceAddress and destinationAddress fields are interpreted in the *H.323-ID* format.

**Command Modes** Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the SBC to block the sourceAddress and destinationAddress fields in H.225 messages received on the adjacency by using the **h225 address block** command in the H.323 adjacency configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# h225 address block
```

The following example shows how to configure the H.225 sourceAddress and destinationAddress fields so that they are interpreted in the e164 format:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# h225 address usage e164
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>h225 timeout</b>	Configures the H.225 timeout interval.

---

## h225 address (session border controller)

To configure the sourceAddress and destinationAddress of H.225 message in the H.323 adjacency, use the **h225 address** command in the H.323 adjacency configuration mode. To return to the default value, use the **no** form of this command.

```
h225 address {block | usage {e164 | h323id}}
```

```
no h225 address {block | usage}
```

Syntax Description		
<b>block</b>	Specifies that the sourceAddress and destinationAddress in a H.225 message are not passed through.	
<b>usage</b>	Specifies the interpretation of the H.225 sourceAddress and destinationAddress fields in an adjacency when Q.931 callingPartyNumber or calledPartyNumber is not present.	
<b>e164</b>	Specifies the e164 format for the addresses. All the other formats are ignored.	
<b>h323id</b>	If the field begins with a numeric prefix, such as [0123456789*.] of 6 or greater characters, it is used as either the calling party number or the called party number, and the rest of the ID is ignored.	

**Command Default** *By default, the sourceAddress and destinationAddress in a H.225 message are not blocked. The H.225 sourceAddress and destinationAddress fields are interpreted in the H.323-ID format.*

**Command Modes** Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the SBC to block the sourceAddress and destinationAddress fields in H.225 messages received on the adjacency by using the **h225 address block** command in the H.323 adjacency configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# h225 address block
```

The following example shows how to configure the H.225 sourceAddress and destinationAddress fields so that they are interpreted in the e164 format:

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# h323  
Router(config-sbc-sbe-h323)# h225 address usage e164
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>h225 timeout</b>	Configures the H.225 timeout interval.

# h225 timeout

To configure the H.225 timeout interval, use the **h225 timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**h225 timeout** {**setup** | **proceeding** | **establishment**} *value*

**no h225 timeout** {**setup** | **proceeding** | **establishment**} *value*

Syntax Description	
<b>setup</b>	Specifies the setup state. Default value for this state is 4 seconds.
<b>proceeding</b>	Specifies the proceeding state. Default value for this state is 10 seconds.
<b>establishment</b>	Specifies the establishment state. Default value for this state is 180 seconds.
<i>value</i>	Specifies the timeout period in seconds. For setup and proceeding timeout periods, valid values are from 1 to 30. For establishment timeout, valid values are from 30 to 300.

**Command Default** *No default behavior or values are available.*

**Command Modes** Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
H.323 configuration (config-sbc-sbe-h323)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **h225 timeout** command configures an H.225 timeout interval in adjacency H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# h225 timeout setup 30
Router(config-sbc-sbe-adj-h323)# h225 timeout proceeding 30
Router(config-sbc-sbe-adj-h323)# h225 timeout establishment 30
```

The following example shows how the **h225 timeout** command configures an H.225 timeout interval in H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# h225 timeout setup 30
Router(config-sbc-sbe-h323)# h225 timeout proceeding 30
Router(config-sbc-sbe-h323)# h225 timeout establishment 30
```



# h245-address-pass

To specify when an H.245 address is passed to the caller when the caller does not support tunneling, use the **h245-address-pass** command in the adjacency H.323 configuration mode. The **no** form of this command shows default behavior, where H.323 supplies the H.245 address on a Q.931 call proceeding, and all subsequent messages to the caller until the H.245 connection is opened.

## **h245-address-pass wait-connect**

**no h245-address-pass wait-connect**

Syntax Description	wait-connect	Pass H.245 address to caller until call is connected. H.323 supplies only the H.245 address on the Q.931 connect
--------------------	--------------	--

**Command Default** Default value is the no form of the command.

**Command Modes** Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	Updated the command for the wait-connect option.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the H.323 adjacency to allow delay passing the H.245 address to caller:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 2651XM-5
Router(config-sbc-sbe-adj-h323)# h245-address-pass wait-connect
Router(config-sbc-sbe-adj-h323)# exit
```

Related Commands	Command	Description
	<b>h245-tunnel disable</b>	Disables H.245 tunneling on a per-adjacency basis.

# h245-tunnel disable

To disable H.245 tunneling on a per-adjacency basis, use the **h245-tunnel disable** command in adjacency H.323 configuration mode. To enable tunneling, use the **no** form of this command.

**h245-tunnel disable**

**no h245-tunnel disable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** *No default behavior or values are available.*

**Command Modes** Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **h245-tunnel disable** command disables H.245 tunneling on an H.323 adjacency named H323ToIsp42:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 H323ToIsp42
Router(config-sbc-sbe-adj-h323)# h245-tunnel disable
```

# h248-profile-version

To configure the vDBE H.248 profile version to interoperate with media gateway controller (SBE), use the **h248-profile-version** command in the vDBE H.248 profile configuration mode. To return to the default value, use the **no** form of this command.

**h248-profile-version** {*profile-version*}

**no h248-profile-version**

<b>Syntax Description</b>	<i>profile-version</i>	Version number of the H.248 profile. The values are from 1 to 3. The value of 3 stands for gate control. The value of 1 stands for etsi-bgf.
---------------------------	------------------------	--

<b>Command Default</b>	Default value is 3.
------------------------	---------------------

<b>Command Modes</b>	vDBE H.248 profile configuration (config-sbc-dbe-vdbe-h248-profile)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. To use this command, you must be in the correct configuration mode and submode. The “Examples” section shows the hierarchy of modes and submodes required to run the command.
-------------------------	--

Use the **h248-profile-version** command after you have defined the name of the profile using the **h248-profile** command.

<b>Examples</b>	The following example shows how to configure the vDBE H.248 profile version to interoperate with the media gateway controller (SBE):
-----------------	--

```
Router# configure terminal
Router(config-sbc)# sbc mysbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# h248-profile etsi-bgf
Router(config-sbc-dbe-vdbe-h248-profile)# h248-profile-version 1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>h248-profile</b>	Configures the vDBE H.248 profile name to interoperate with the media gateway controller (SBE).

<b>Command</b>	<b>Description</b>
<b>show sbc dbe h248-profile</b>	Displays the information on the specified profile, including transport, H.248 version, and active packages.
<b>vdbe</b>	Enters Virtual Data Border Element (vDBE) configuration mode.

# h248-profile

To configure a Virtual Data Border Element (VDBE) H.248 profile name to interoperate with the data border element (DBE), use the **h248-profile** command in the vDBE configuration mode. To return to the default value, use the **no** form of this command.

```
h248-profile {etsi-bgf | gate-ctrl} version version-number
```

```
no h248-profile
```

## Syntax Description

<b>etsi-bgf</b>	Configures the Ia profile for ETSI_BGF.
<b>gate-ctrl</b>	Configures the Cisco profile for SBC_GateControl.
<b>version</b>	Configures the profile version.
<i>version-number</i>	The profile's version number. The default version number for <b>etsi-bgf</b> is 2 and <b>gate-ctrl</b> is 3.

## Command Default

Default value is gatecontrol.

## Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.1S	The <b>version</b> keyword and the <i>version-number</i> argument were added to configure the profile version.

## Usage Guidelines

To use this command, you must be in a user group that is associated with a task group that includes the proper task IDs. To use this command, you must also be in the correct configuration mode and submode. The Examples section that follows shows the hierarchy of the modes and submodes required to run the command.

After the DBE is configured to use the H.248 profile name, the applicable profile name is advertised with the Service Change messages.

## Examples

The following example shows how to configure the vDBE H.248 Ia profile to interoperate with the DBE:

```
Router# configure terminal
Router(config-sbc)# sbc mysbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# h248-profile etsi-bgf version 2
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>h248-version</b>	Defines the version of an H.248 protocol that the DBE uses when it forms associations with an H.248 controller.
<b>bandwidth-fields mandatory</b>	Sets the bandwidth description of SDP as mandatory.
<b>vdbe</b>	Enters VDBE configuration mode.

# h248-version (session border controller)

To define the version of an H.248 protocol that the data border element (DBE) uses when it forms associations with an H.248 controller, use the **h248-version** command in VDBE configuration mode. To leave the default as version 2 of the H.248 protocol, use the **no** form of this command.

**h248-version** *version-number*

**no h248-version** *version-number*

## Syntax Description

version-number	Specifies the version number. The DBE can accept H.248.1 version 2 or version 3. The default is H.248.1 version 2.
----------------	--

## Command Default

H.248.1 version 2 is used.

## Command Modes

VDBE configuration mode (config-sbc-dbe-vdbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for distributed SBC.

## Usage Guidelines

This command configures the DBE to support H.248.1v3, thus allowing the DBE to interoperate with an SBE or media gateway controller (MGC) which requires H.248.1 version 3. The DBE can accept H.248.1 version 2 or version 3.

The DBE rejects attempts to negotiate with the MGC to a lower version once the DBE is configured to support version 3.

## Examples

The following example creates a DBE service on an SBC called “mySbc” and configures the DBE to use version 3 of the H.248.1 protocol, for a distributed SBC:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# end
```

## Related Commands

Command	Description
<b>h248-napt-package</b>	Defines which H.248 package, either IP NAT Traversal package (ipnapt) or NAT Traversal package (ntr), the DBE uses for signaling Network Address Translation (NAT) features.

# h248 allow-all-mg

To configure the H.248 signaling stack to allow connections from all Media Gateways, use the **h248 allow-all-mg** command in the SBE configuration mode. Use the **no** form of this command to deconfigure the H.248 signaling stack from allowing connections from all media gateways.

**h248 allow-all-mg**

**no h-248 allow-all-mg**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Default is the **no** form of this command

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following command configures the H.248 signaling stack to allow any Media Gateway to connect to the SBE:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h248 allow-all-mg
Router(config-sbc-sbe)#
```



# h323 (session border controller)

To enter the H.323 configuration mode, use the **h323** command in SBE configuration mode.

**h323**

**Syntax Description** This command has no arguments or keywords.

**Command Default** *No default behavior or values are available.*

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was not supported in Cisco IOS XE Release 2.4 on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to enter the H.323 configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)#
```

Related Commands	Command	Description
	<b>hunting-trigger</b>	Configures failure return codes to trigger hunting.
	<b>ras retry</b>	Configures an H.323 Registration, Admission, and Status (RAS) retry count for an RAS transaction type.
	<b>ras rrq</b>	Configures the registration request (RRQ).
	<b>ras timeout</b>	Configures an H.323 RAS timeout interval.
	<b>adjacency timeout</b>	Configures the adjacency retry timeout interval.

# header-editor

To set a specified header editor for inbound and outbound signaling on the signaling border element (SBE) session initiation protocol (SIP) adjacency, use the **header-editor** command in the Adjacency SIP configuration mode. To remove a header editor, use the **no** form of this command.

```
header-editor {inbound | outbound} {editor-name | default}
```

```
no header-editor {inbound | outbound} {editor-name | default}
```

## Syntax Description

<b>inbound</b>	Sets the inbound SIP header editor.
<b>outbound</b>	Sets the outbound SIP header editor.
<i>editor-name</i>	Name of the header editor to be set for inbound or outbound signaling on the adjacency.  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
<b>default</b>	Sets the header editor to the default settings.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how the **header-editor** command sets header editors for inbound and outbound signaling on the SIPP SBE SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# header-editor inbound editor1
Router(config-sbc-sbe-adj-sip)# header-editor outbound default
Router(config-sbc-sbe-adj-sip)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip header-editor</b>	Configures a header editor.

# header-editor (method)

To add a header editor to act on a method, use the **header-editor** command in the signaling border element (SBE) SIP method element configuration mode. To remove a header editor, use the **no** form of this command.

**header-editor** *editor-name*

**no header-editor**

## Syntax Description

<i>editor-name</i>	Name of the header editor. It can be upto 30 characters.
--------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE SIP Method Element configuration (config-sbc-sbe-mep-mth-ele)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how the **header-editor** command adds a header editor to act on a method:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# sip method-editor MethodEditor1
Router(config-sbc-sbe-mep-mth)# method Method2
Router(config-sbc-sbe-mep-mth-ele)# header-editor HeaderEditor1
```

Command	Description
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.

## header-name

To configure various headers, use the **header-name** command in the adjacency SIP configuration mode. To deconfigure the headers, use the **no** form of this command.

```
header-name {contact {add [tls-param] | contact-param {passthrough | strip}} | expires
suppress | from {passthrough} | p-asserted-id {assert | header-value {word}} | record-route
{passthrough} | route {destination-address {word} | port port number} | supported
{header-value {timer {insert}}} | to {passthrough} |
via {passthrough {inbound | outbound}}}
```

```
no header-name {contact {add [tls-param] | contact-param {passthrough | strip}} | expires
suppress | from {passthrough} | p-asserted-id {assert | header-value {word}} | record-route
{passthrough} | route {destination-address {word} | port port number} | supported
{header-value {timer {insert}}} | to {passthrough} |
via {passthrough {inbound | outbound}}}
```

### Syntax Description

<b>contact</b>	Configures settings affecting the Contact: header in non-REGISTER requests.
<b>add</b>	Adds a specific parameter to the header.
<b>tls-param</b>	Specifies a 'transport=tls' parameter to SBC-originated Contact and Record-Route headers when using Transport Layer Security (TLS).  This is only relevant for a trusted-encrypted or untrusted-encrypted adjacency.
<b>contact-param</b>	Configures settings affecting the contact header parameters.
<b>passthrough</b>	Passthrough header parameters from contact headers. This is the default value.
<b>strip</b>	Specifies strip header parameters from contact headers.
<b>expires suppress</b>	Specifies whether to include Expires header in the outgoing INVITE requests.
<b>from</b>	Configures settings affecting the From: header in non-REGISTER requests.
<b>passthrough</b>	Passthrough header in non-REGISTER requests.
<b>p-asserted-id</b>	Configures settings affecting the P-Asserted-Identity: header.
<b>assert</b>	Determines whether the SBC must assert a registered subscriber's identity on any outbound signal from this adjacency, by converting a P-Preferred-Identity header to a P-Asserted-Identity header on an outbound INVITE request or an OOD request. This field can be used to override the inherit profile.
<b>header-value</b>	Specifies the value of the P-Asserted-Identity header on the outgoing SIP message, for the messages received on this adjacency.
<b>word</b>	Specifies the header value.
<b>record-route</b>	Specifies type of SIP header to configure.
<b>passthrough</b>	Passthrough header in non-REGISTER requests.
<b>route</b>	Configures settings affecting the Route: header.
<b>destination-address</b>	Configures the route header destination, which is either the IP address or the domain name.
<b>word</b>	Specifies the IP address or the domain name.
<b>port</b>	Configures the route header port.
<i>port-number</i>	Specifies the port of the route header port.
<b>supported</b>	Configures settings affecting the Supported: header.

<b>header-value</b>	Configures settings affecting the Supported header-value:header.
<b>timer</b>	Configures settings affecting the Supported timer: header.
<b>insert</b>	Inserts a Supported: timer header.
<b>to</b>	Configures settings affecting the To: header in non-REGISTER requests.
<b>passthrough</b>	Passthrough header in non-REGISTER requests.
<b>via</b>	Configures settings affecting the Via: header.
<b>passthrough</b>	Allows the Via header passthrough.
<b>inbound</b>	Allows the Inbound Via Header passthrough.
<b>outbound</b>	Allows the Outbound Via Header passthrough.

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	The keyword expires suppress was added.
	Cisco IOS XE Release 3.2	This command was modified. The <b>contact-param</b> keyword was added.
	Cisco IOS XE Release 3.6	This command was modified. The <b>Via</b> keyword was added.

**Usage Guidelines** This command is used in configuring Aggregate Registration.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **header-name** command is used to configure the passthrough header for non-REGISTER requests:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# header-name from passthrough
Router(config-sbe-adj-sip)# header-name to passthrough
```

The following example shows how the **header-name** command is used to suppress the expires header in the outgoing INVITE messages:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip mySIP
Router(config-sbe-adj-sip)# header-name expires suppress
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>request-line request-uri rewrite</b>	Requests the SBC to rewrite the Request-URI to a different user and hostname before sending a request to a registered subscriber.

# header-name p-asserted-id

To specify the value for the P-Asserted-Identity on the outgoing SIP message, use the **header-name p-asserted-id** command in SBC SBE Adjacency SIP mode. Use the **no** form of this command to remove the P-Asserted-Identity.

**header-name p-asserted-id** [*header-value* [*header-value*] | **assert**]

**no header-name p-asserted-id** [*header-value* [*header-value*] | **assert**]

## Syntax Description

<i>header-value</i>	A value for the P-Asserted-Identity header as defined by RFC 3325.
<b>assert</b>	Enable the P-Asserted-Identity on the outgoing SIP messages.

## Command Default

No default behavior or values are available.

## Command Modes

SBC SBE Adjacency SIP (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The header is added to all requests and responses except ACK, CANCEL, INFO, PRACK, REGISTER and UPDATE.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to specify the header value for the P-Asserted-Identity for adjacency CORE. In the following example, sip:1234@cisco.com is specified as the header-value:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip CORE
Router(config-sbc-sbe-adj-sip)# header-name p-asserted-id header-value sip:1234@cisco.com
Router(config-sbc-sbe-adj-sip)# header-name p-asserted-id assert
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# exit
Router(config-sbc)# exit
Router(config)# exit
```



The following show command output provides details of the above configuration:

```

Router# show sbc test sbe adjacencies CORE detail
SBC Service "test"
Adjacency CORE (SIP)
  Status: Detached
  Signaling address: 44.33.107.8:default
  Signaling-peer: :5060 (Default)
  Force next hop: No
  Account:
  Group: None
  In header profile: Default
  Out header profile: Default
  In method profile: Default
  Out method profile: Default
  In body profile: None
  Out body profile: None
  In UA option prof: Default
  Out UA option prof: Default
  In proxy opt prof: Default
  Out proxy opt prof: Default
  Priority set name: None
  Local-id: None
  Rewrite REGISTER: Off
  Register contact username: Rewrite
  Target address: None
  NAT Status: Auto Detect
  Reg-min-expiry: 3000 seconds
  Fast-register: Enabled
  Fast-register-int: 30 seconds
  Register aggregate: Disabled
  Registration Required: Enabled
  Register Out Interval: 0 seconds
  Parse username params: Disabled
  Supported timer insert: Disabled
  Suppress Expires: Disabled
p-asserted-id header-value: sip:1234@cisco.com
p-asserted-id assert: Enabled
  Authenticated mode: None
  Authenticated realm: None
  Auth. nonce life time: 300 seconds
  IMS visited NetID: None
  Inherit profile: Default
  Force next hop: No
  Home network Id: None
  UnEncrypt key data: None
  SIPI passthrough: No
  Passthrough headers:
  Media passthrough: No
  Incoming 100rel strip: No
  Incoming 100rel supp: No
  Out 100rel supp add: No
  Out 100rel req add: No
  Parse TGID parms: No
  IP-FQDN inbound:
  IP-FQDN outbound:
  FQDN-IP inbound:
  FQDN-IP outbound:
  Outbound Flood Rate: None
  Hunting Triggers: Global Triggers
  Add transport=tls param: Disabled
  Redirect mode: Pass-through
  Security: Untrusted-Unencrypted
  TLS mutual authentication: No

```

```
Ping:                               Disabled
Ping Interval:                       32 seconds
Ping Life Time:                       32 seconds
Ping Peer Fail Count:                 3
Ping Trap sending:                    Enabled
Ping Peer Status:                     Not Tested
Rewrite Request-uri:                  Disabled
Registration Monitor:                 Disabled
DTMF SIP NOTIFY Relay:                Enabled
DTMF SIP NOTIFY Interval:             2000
DTMF SIP default duration:            200
DTMF Preferred Method:                 SIP NOTIFY
Realm                                 :      None
Statistics setting:                   Summary
```

Router#

# header-name supported header-value timer insert

To insert a “Supported:timer” header, use the *header-name supported header-value timer insert* command in SBC SBE Adjacency SIP mode. Use the **no** form of this command to disable inserting the header.

*header-name supported header-value timer insert*

*no header-name supported header-value timer insert*

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBC SBE Adjacency SIP (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the SIP adjacency CORE to insert a supported timer header:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip CORE
Router(config-sbc-sbe-adj-sip)# header-name supported header-value timer insert
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# exit
Router(config-sbc)# exit
Router(config)# exit
```

The following show command output provides details on the above configuration. Note the value of the supported timer insert field:

```
Router# show sbc test sbe adjacencies CORE detail
SBC Service "test"
  Adjacency CORE (SIP)
    Status: Detached
    Signaling address: 44.33.107.8:default
    Signaling-peer: :5060 (Default)
    Force next hop: No
```

```

Account:
Group:                None
In header profile:    Default
Out header profile:   Default
In method profile:    Default
Out method profile:   Default
In body profile:      None
Out body profile:     None
In UA option prof:    Default
Out UA option prof:   Default
In proxy opt prof:    Default
Out proxy opt prof:   Default
Priority set name:     None
Local-id:             None
Rewrite REGISTER:    Off
Register contact username: Rewrite
Target address:       None
NAT Status:           Auto Detect
Reg-min-expiry:       3000 seconds
Fast-register:        Enabled
Fast-register-int:    30 seconds
Register aggregate:   Disabled
Registration Required: Enabled
Register Out Interval: 0 seconds
Parse username params: Disabled
Supported timer insert: Enabled
Suppress Expires:     Disabled
p-asserted-id header-value: sip:1234@cisco.com
p-assert-id assert:   Enabled
Authenticated mode:   None
Authenticated realm:  None
Auth. nonce life time: 300 seconds
IMS visited NetID:    None
Inherit profile:      Default
Force next hop:       No
Home network Id:      None
UnEncrypt key data:   None
SIPI passthrough:     No
Passthrough headers:
Media passthrough:    No
Incoming 100rel strip: No
Incoming 100rel supp: No
Out 100rel supp add:  No
Out 100rel req add:   No
Parse TGID parms:    No
IP-FQDN inbound:
IP-FQDN outbound:
FQDN-IP inbound:
FQDN-IP outbound:
Outbound Flood Rate:  None
Hunting Triggers:     Global Triggers
Add transport=tls param: Disabled
Redirect mode:         Pass-through
Security:              Untrusted-Unencrypted
TLS mutual authentication: No
Ping:                  Disabled
Ping Interval:         32 seconds
Ping Life Time:        32 seconds
Ping Peer Fail Count:  3
Ping Trap sending:     Enabled
Ping Peer Status:      Not Tested
Rewrite Request-uri:   Disabled
Registration Monitor:  Disabled
DTMF SIP NOTIFY Relay: Enabled

```

```
DTMF SIP NOTIFY Interval: 2000
DTMF SIP default duration: 200
DTMF Preferred Method: SIP NOTIFY
Realm : None
Statistics setting: Summary
```

# header-name via passthrough

To configure the session border controller (SBC) to allow the Via headers on inbound requests or outbound requests for a specified adjacency to pass through, use the **header-name via passthrough** command in the adjacency SIP configuration mode. To disable passthrough of Via headers on inbound requests or outbound requests, use the **no** form of this command.

**header-name via passthrough {inbound | outbound}**

**no header-name via passthrough {inbound | outbound}**

## Syntax Description

<b>inbound</b>	Specifies that the Via headers on inbound requests for a specified adjacency must be allowed to pass through.
<b>outbound</b>	Specifies that the Via headers on outbound requests for a specified adjacency must be allowed to pass through.

## Command Default

The SBC removes the existing Via headers and adds its own Via header.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
3.6S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to use the **header-name via passthrough** command to allow the Via headers on inbound requests and outbound requests for a specified adjacency to pass through:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe) # adjacency sip adj1
Router(config-sbc-sbe-adj-sip) # header-name via passthrough inbound
Router(config-sbc-sbe-adj-sip) # header-name via passthrough outbound
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>header-name</b>	Configures the contact header and passthrough header in non-REGISTER requests.
<b>header-name p-asserted-id</b>	Specifies the value for the P-Asserted-Identity header on outgoing SIP messages.
<b>header-name supported header-value timer insert</b>	Inserts the Supported:timer header in SIP messages.

# header-prio header-name

To configure the priority of a header that is used to derive a source, destination, or diverted-by address, use the **header-prio header-name** command in the appropriate SIP header address configuration mode. To remove the priority from a header, use the **no** form of this command.

**header-prio** *priority-level* **header-name** *header-name* [**request-uri**]

**no header-prio** *priority-level* **header-name** *header-name* [**request-uri**]

## Syntax Description

<i>priority-level</i>	Specifies the priority number to assign to the header. Priority levels are 1 to 10.
<i>header-name</i>	Name of the existing header, that is used to derive the source, destination, or diverted-by address, to which the <i>priority-level</i> is assigned.
<b>request-uri</b>	(Optional) Specifies that the Request URI is to be used for extraction of the destination address. (Available only in destination address mode.)

## Command Default

No default behavior or values are available.

## Command Modes

SIP header destination address configuration (config-sbc-sbe-sip-hdr-dst)  
 SIP header source address configuration (config-sbc-sbe-sip-hdr-src)  
 SIP header diverted-by address configuration (config-sbc-sbe-sip-hdr-div)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of modes required to run the command.

This command can be used multiple times to set the priorities of multiple headers.

## Examples

The following example shows how to configure the priority of a header that uses the Request URI to derive a destination address:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile HP1
Router(config-sbc-sbe-sip-hdr) dst-address
Router(config-sbc-sbe-sip-hdr-dst)# header-prio 1 header-name request-uri
Router(config-sbc-sbe-sip-hdr-dst)#
```

The following example shows how to configure a list of headers to derive a destination address:



```

ASR-1002# configure terminal
ASR-1002(config)# sbc mySBC
ASR-1002(config-sbc)# sbe
ASR-1002(config-sbc-sbe)# sip header-profile Hprof1
ASR-1002(config-sbc-sbe-sip-hdr)# dst-address
ASR-1002(config-sbc-sbe-sip-hdr-dst)# header-prio 1 header-name P-Called-ID
ASR-1002(config-sbc-sbe-sip-hdr-dst)# header-prio 2 header-name To
ASR-1002(config-sbc-sbe-sip-hdr-dst)# header-prio 2 header-name Request-uri
ASR-1002(config-sbc-sbe-sip-hdr-dst)# end

```

The following example shows how to configure a list of headers to derive a source address:

```

ASR-1002# configure terminal
ASR-1002(config)# sbc mySBC
ASR-1002(config-sbc)# sbe
ASR-1002(config-sbc-sbe)# sip header-profile Hprof1
ASR-1002(config-sbc-sbe-sip-hdr)# src-address
ASR-1002(config-sbc-sbe-sip-hdr-src)# header-prio 1 header-name Remote-Party-ID
ASR-1002(config-sbc-sbe-sip-hdr-src)# header-prio 2 header-name P-Preferred-Identity
ASR-1002(config-sbc-sbe-sip-hdr-src)# header-prio 2 header-name From
ASR-1002(config-sbc-sbe-sip-hdr-src)# end
ASR-1002#

```

The following example shows how to configure a list of headers to derive a source address of a diverted call:

```

ASR-1002# configure terminal
ASR-1002(config)# sbc mySBC
ASR-1002(config-sbc)# sbe
ASR-1002(config-sbc-sbe)# sip header-profile Hprof1
ASR-1002(config-sbc-sbe-sip-hdr)# div-address
ASR-1002(config-sbc-sbe-sip-hdr-div)# header-prio 1 header-name Diversion
ASR-1002(config-sbc-sbe-sip-hdr-div)# end
ASR-1002#

```

The following is an example of the show command output after the header list for destination address, source address, and diversion address is configured on an SBC:

```

ASR-1002# show sbc mine sbe sip header-profile Hprof1
Header profile "Hprof1"
Description:
Type:      Whitelist
dst-address: (inbound only)
            header-prio 1 header-name P-Called-ID
            header-prio 2 header-name To
            header-prio 3 header-name Request-uri
src-address: (inbound only)
            header-prio 1 header-name Remote-Party-ID
            header-prio 2 header-name P-Preferred-Identity
            header-prio 3 header-name From
div-address (inbound only)
            header-prio 1 Diversion
store-rules:
            No store-rule entries found.
request-line:
            No request-line entries found.
headers:
            test
            entry 1
            description:
            action add-first-header value "cisco"
            condition is-request eq true
            Not in use with any adjacencies
            Not in use with any method-profile

```

Related Commands	Command	Description
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
	<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
	<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
	<b>header-prio header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
	<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
	<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
	<b>req-timeout</b>	Configures the ENUM request timeout period.
	<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
	<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
	<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
	<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
	<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

# header-prio header-name (editor)

To configure the priority of a header that is used to derive a source, destination, or diverted-by address, use the **header-prio header-name** command in the appropriate session initiation protocol (SIP) Header Address configuration mode. To remove the priority from a header, use the **no** form of this command.

**header-prio** *priority-level* **header-name** *header-name* [**request-uri**]

**no header-prio** *priority-level*

## Syntax Description

<i>priority-level</i>	Priority number to be assigned to the header. Priority levels are 1 to 10.
<i>header-name</i>	Name of the existing header that is used to derive the source, destination, or diverted-by address to which the <i>priority-level</i> is assigned.
<b>request-uri</b>	(Optional) Specifies that the Request URI is to be used for the extraction of the destination address. (Available only in Destination address mode.)

## Command Default

No default behavior or values are available.

## Command Modes

SIP header destination address configuration (config-sbc-sbe-sip-hdr-dst)  
 SIP header source address configuration (config-sbc-sbe-sip-hdr-src)  
 SIP header diverted-by address configuration (config-sbc-sbe-sip-hdr-div)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

This command can be used multiple times to set the priorities of multiple headers.

## Examples

The following example shows how to configure the priority of a header that uses the Request URI to derive a destination address:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor HP1
Router(config-sbc-sbe-mep-hdr) dst-address
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 1 header-name request-uri
Router(config-sbc-sbe-mep-hdr-dst)#
```

The following example shows how to configure a list of headers to derive a destination address:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Hprof1
Router(config-sbc-sbe-mep-hdr)# dst-address
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 1 header-name P-Called-ID
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 2 header-name To
Router(config-sbc-sbe-mep-hdr-dst)# header-prio 2 header-name Request-uri
Router(config-sbc-sbe-mep-hdr-dst)# end
```

The following example shows how to configure a list of headers to derive a source address:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Hprof1
Router(config-sbc-sbe-mep-hdr)# src-address
Router(config-sbc-sbe-mep-hdr-src)# header-prio 1 header-name Remote-Party-ID
Router(config-sbc-sbe-mep-hdr-src)# header-prio 2 header-name P-Preferred-Identity
Router(config-sbc-sbe-mep-hdr-src)# header-prio 2 header-name From
Router(config-sbc-sbe-mep-hdr-src)# end
Router#
```

The following example shows how to configure a list of headers to derive the source address of a diverted call:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Hprof1
Router(config-sbc-sbe-mep-hdr)# div-address
Router(config-sbc-sbe-mep-hdr-div)# header-prio 1 header-name Diversion
Router(config-sbc-sbe-mep-hdr-div)# end
Router#
```

#### Related Commands

Command	Description
<b>div-address</b>	Enables entry into the Diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enables entry into the Destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>src-address</b>	Enables entry into the Source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>sip header-editor</b>	Configures a header editor.

# header-profile

To set a specified header profile for inbound and outbound signaling on a specified SBE SIP adjacency, use the **header-profile** command in adjacency sip configuration mode.

**header-profile {inbound | outbound} profile-name**

<b>Syntax Description</b>	<b>inbound   outbound</b>	Sets the inbound and outbound SIP header profiles.
	<i>profile-name</i>	Specifies the name of the header profile to be set for inbound or outbound signaling on a specified adjacency.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.  <b>Note</b> If you enter the name <b>default</b> , the default header profile is set for inbound or outbound signaling.

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency sip configuration (config-sbc-sbe-adj-sip)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **header-profile** command sets header profiles for inbound and outbound signaling on an SBE SIP adjacency test:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# header-profile inbound profile1
Router(config-sbc-sbe-adj-sip)# header-profile outbound profile2
Router(config-sbc-sbe-adj-sip)#
```

# header (editor)

To add a header to a SIP message editor, use the **header** command in the SIP Header Editor configuration mode. To remove a header, use the **no** form of this command.

**header** *header-name* [**entry** *entry-number*]

**no header** *header-name* [**entry** *entry-number*]

## Syntax Description

<i>header-name</i>	Name of the header to be added to the header editor. Valid names are 1 to 32 characters in length (inclusive) and case-sensitive.
<b>entry</b>	Specifies the filtered entry number. By default, it is 1.
<i>entry-number</i>	Entry number that can range from 1 to 99.

## Command Default

By default, the entry number is 1.

## Command Modes

SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how the **header** command adds a header, test, to the Myeditor header editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Myeditor
Router(config-sbc-sbe-sip-hdr)# header test
```

## Related Commands

Command	Description
<b>blacklist</b>	Configures a SIP header or method blacklist editor on a SIP message.
<b>description</b>	Configures descriptive text for a SIP header.
<b>sip header-editor</b>	Configures a header editor.

# header (session border controller)

To add a header with a specified name to a SIP message profile, use the **header** command in SIP header-profile configuration mode. To remove the method from the profile, use the **no** form of this command.

**header** *header-name*

**no header** *header-name*

<b>Syntax Description</b>	<i>header-name</i>	Specifies the name of the header added to the header profile. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.
---------------------------	--------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SIP header configuration (config-sbc-sbe-sip-hdr)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>header</b> command adds the header “test” to the header profile Myprofile:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile Myprofile
Router(config-sbc-sbe-sip-hdr)# header test
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>blacklist</b>
	<b>description</b>	Configures descriptive text for a SIP header.

# heart-beat terminate

To configure the interval during which only one heartbeat request from an H.248 terminal device can pass through the Border Access Controller (BAC), and terminate the other heartbeat requests sent during this interval, use the **heart-beat terminate** command in the H248 BAC adjacency configuration mode. To return to the default value, use the **no** form of this command.

**heart-beat terminate** *terminate-interval*

**no heart-beat terminate** *terminate-interval*

<b>Syntax Description</b>	<i>terminate-interval</i> Interval during which heartbeat requests are terminated, in seconds. The range is from 0 to 3600. The default value is 60.
---------------------------	--

<b>Command Default</b>	The default terminate interval is 60 seconds.
------------------------	---

<b>Command Modes</b>	H248 BAC adjacency configuration (config-h248-bac-adj)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To disable the heartbeat termination function, set the <i>terminate-interval</i> to 0 seconds. If the <i>terminate-interval</i> is 0 seconds, then all the heartbeat requests are passed through the BAC and none are terminated.
-------------------------	---

This command can be configured only in the access adjacency submode and not in the core adjacency submode.

<b>Examples</b>	The following example shows how the <b>heart-beat terminate</b> command is used to configure the terminate interval:
-----------------	--

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# heart-beat terminate 80
```



# hold-media-timeout

To configure the time an SBE will wait after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down, use the **hold-media-timeout** command in SBE configuration mode. To set the number to its default, use the **no** form of this command.

*hold-media-timeout timeout*

<b>Syntax Description</b>	<i>timeout</i>	Specifies the time in milliseconds an SBE will wait after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down.
---------------------------	----------------	--

<b>Command Default</b>	The default value is 0 milliseconds.
------------------------	--------------------------------------

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following command configures the SBE to wait two hours after receiving the last media packet on an on-hold call before cleaning up the call resources:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# hold-media-timeout 7200
Router(config-sbc-sbe)#
```

# hunt-on-reject

To set the trigger on hunting, use the **hunt-on-reject** command in the signaling border element (SBE) SIP body element configuration mode. To stop the trigger, use the **no** form of this command.

**hunt-on-reject**

**no hunt-on-reject**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBE SIP body element configuration (config-sbc-sbe-mep-bdy-ele)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to create a body editor named bodyeditor1, describe the body type that is to act on the messages with the *application/ISUP* Content Type header, and set the trigger on hunting:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-editor bodyeditor1
Router(config-sbc-sbe-mep-bdy)# body application/ISUP
Router(config-sbc-sbe-mep-bdy-ele)# hunt-on-reject
Router(config-sbc-sbe-mep-bdy-ele)#
```

Related Commands	Command	Description
	<b>body</b>	Names a body type or content header type for a non-SDP message body that is a part of a body editor.
	<b>body-editor</b>	Associates a body editor at a SIP adjacency level to an adjacency in the SIP adjacency mode.
	<b>sip body-editor</b>	Creates a body editor to filter the non-SDP bodies from the incoming and outgoing SIP messages.

# hunting-mode

To configure the form of H.323 hunting to perform if hunting is triggered, use the **hunting-mode** command in one of its supported modes: H.323 (global H.323 scope) and adjacency h323 (destination H.323 adjacency). The **no** form of the command resets to the default of alternate end points.

*hunting-mode {altEndps | multiARQ}*

*no hunting-mode*

## Syntax Description

<i>altEndps</i>	Specifies alternate end points hunting. When H.323 has a list of alternate endpoints for a call, H.323 tries each endpoint in turn before reporting a routing failure.
<i>multiARQ</i>	Specifies multiARQ hunting. This is a non-standard H.323 mechanism for hunting for other routes or destination adjacencies. It is based on issuing multiple Admission Requests (ARQs) to a Gatekeeper for a single call.

## Command Default

Default is alternate end points (altEndps) if user does not configure a hunting-mode or configures **no hunting-mode**. It does not disable hunting completely.

## Command Modes

H.323 configuration (config-sbc-sbe-h323)  
 Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The SBC hunts for other routes or destination adjacencies in the event of a failure. Hunting re-routes the call in response to a specific user-configured event or error code. The hunting mode is typically set after the hunting-trigger is configured.

The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure H.323 to perform multiARQ hunting and to retry routing if it receives a noBandwidth or securityDenied error:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# h323
Router (config-sbc-sbe-h323)# hunting-trigger noBandwidth securityDenied
Router (config-sbc-sbe-h323)# hunting-mode multiARQ
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>hunting-trigger</b>	Configures failure return codes to trigger hunting.

# hunting-trigger

To configure failure return codes to trigger hunting, use the **hunting-trigger** command in one of its supported modes: SIP (global SIP scope), H.323 (global H.323 scope), adjacency SIP (destination SIP adjacency), and adjacency h323 (destination H.323 adjacency). The **no** form of the command clears all error codes.

If you enter **no hunting-trigger x y**, then just codes x and y are removed from the configured list.

*hunting-trigger {error-codes | disable} error-codes*

*no hunting-trigger {error-codes | disable} error-codes*

## Syntax Description

<i>error-codes</i> (SIP and adjacency modes)	Signifies a space-separated list of SIP numeric error codes.
error-codes (h323 and adjacency h323 modes)	Specifies one of the following values: <ul style="list-style-type: none"> <li>noBandwidth—H.225 no bandwidth response.</li> <li>unreachableDestination—H.225 unreachable destination response.</li> <li>destinationRejection—H.225 destination rejection response.</li> <li>noPermission—H.225 no permission response.</li> <li>gatewayResources—H.225 gateway Resources response.</li> <li>badFormatAddress—H.225 bad format address response.</li> <li>securityDenied— H.225 security denied response.</li> <li><b>connectFailed</b>—Internal response.</li> <li><b>noRetry</b>—Specifies that routing should never be retried for this adjacency no matter what failure return code is received.</li> </ul>

## Command Default

*No default behavior or values are available.*

## Command Modes

SBE SIP configuration (config-sbc-sbe)  
H.323 configuration (config-sbc-sbe-h323)  
Adjacency SIP configuration (config-sbc-sbe-adj-sip)  
Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

If both adjacency level and SBE level hunting triggers are configured, the adjacency level takes priority.

If you enter **hunting-trigger x** followed by **hunting-trigger y**, the value of **x** is replaced with **y**.

To set both **x** and **y** to be hunting triggers, you must enter **hunting-trigger x y**.

The Examples section shows the hierarchy of modes required to run the command.

In the adjacency SIP or H.323 adjacency modes, if you specify the special hunting-trigger value of **disable**, routes are never retried to this adjacency, even if the error code is on the global retry list.

To configure more than one H.323 hunting trigger, you must enter the commands as separate lines, such as in the following example:

```

sbc mySBC
sbe
  adjacency h323 h1
    hunting-trigger badFormatAddress
    hunting-trigger connectFailed

```

## Examples

### SIP mode

The following example shows how to configure SIP to retry routing if it receives a 415 (media unsupported) or 480 (temporarily unavailable) error:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# sip hunting-trigger 416 480

```

### H.323 mode

The following example shows how to configure H.323 to retry routing if it receives a noBandwidth or securityDenied error. Note that for multiple error codes, each hunting trigger must be configured on a separate line:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# h323
Router (config-sbc-sbe-h323)# hunting-trigger noBandwidth
Router (config-sbc-sbe-h323)# hunting-trigger securityDenied

```

### SIP adjacency mode

The following example shows how to configure SIP to retry routing to the SIP adjacency SipAdj1 if it receives a 415 (media unsupported) or 480 (temporarily unavailable) error:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# hunting-trigger 415 480

```

### H.323 adjacency mode

The following example shows how to configure H.323 to retry routing to the H.323 adjacency h323Adj1 if it receives a noBandwidth or securityDenied error. Note that for multiple error codes, each hunting trigger must be configured on a separate line:

```

Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323Adj1
Router (config-sbc-sbe-adj-h323)# hunting-trigger noBandwidth

```

```
Router (config-sbc-sbe-adj-h323) # hunting-trigger securityDenied
```

# import-map

To configure flexible policy handling by a BGP route server, use the **import-map** command in route server context address family configuration mode. To remove the route server's flexible policy handling, use the **no** form of this command.

**import-map** *route-map-name*

**no import-map** *route-map-name*

## Syntax Description

<i>route-map-name</i>	Name of the route map that controls which routes will be added to the route server client virtual table.
-----------------------	--

## Command Default

No import map exists and no flexible policy handling by a route server exists.

## Command Modes

Route server context address family configuration (config-router-rsctx-af)

## Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.

## Usage Guidelines

Use this command if your BGP route server needs to support flexible policies.

In order to configure flexible policy handling, you must create a route server context, which includes an import map. The import map references a standard route map. You may match on nexthop, AS path, communities, and extended communities.



### Note

Do not confuse the **import-map** command with the **import map** command in VRF configuration submode, which configures an import route map for a VPN routing and forwarding (VRF) instance.

## Examples

In the following example, the local router is a BGP route server. Its neighbors at 10.10.10.12 and 10.10.10.13 are its route server clients. A route server context named ONLY\_AS27\_CONTEXT is created and applied to the neighbor at 10.10.10.13. The context uses an import map that references a route map named only\_AS27\_routemap. The route map matches routes permitted by access list 27. Access list 27 permits routes that have 27 in the autonomous system path.

```
router bgp 65000
  route-server-context ONLY_AS27_CONTEXT
    address-family ipv4 unicast
      import-map only_AS27_routemap
    exit-address-family
  exit-route-server-context
  !
  neighbor 10.10.10.12 remote-as 12
  neighbor 10.10.10.12 description Peer12
  neighbor 10.10.10.13 remote-as 13
```



```

neighbor 10.10.10.13 description Peer13
neighbor 10.10.10.21 remote-as 21
neighbor 10.10.10.27 remote-as 27
!
address-family ipv4
  neighbor 10.10.10.12 activate
  neighbor 10.10.10.12 route-server-client
  neighbor 10.10.10.13 activate
  neighbor 10.10.10.13 route-server-client context ONLY_AS27_CONTEXT
  neighbor 10.10.10.21 activate
  neighbor 10.10.10.27 activate
exit-address-family
!
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
  match as-path 27
!

```

### Related Commands

Command	Description
<b>description (route server context)</b>	Describes a route server context for a user-friendly way to see the purpose of the route server context.
<b>route-map</b>	Enables policy routing.
<b>route-server-context</b>	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

# ims media-service

To configure a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources, use the **ims media-service** command in CAC table entry configuration mode. To return to the default condition where only Rx is used, use the no form of this command.

**ims media-service**

**no ims media-service**

**Syntax Description** This command has no arguments or keywords.

**Command Default** When media service is not configured, only Rx is in use.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

By default, only Rx is in use, and media and 3rd-party transcoding resources cannot be used. When IMS media service is configured, Rx is used as well as media resources and 3rd party transcoding resources.



**Note**

Media bypass takes precedence over IMS media service configuration.

**Examples** The following example shows how to configure a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# ims media-service
```

Related Commands	Command	Description
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.
	<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
	<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
	<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
	<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
	<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
	<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
	<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
	<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
	<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
	<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# ims pani

To configure the P-Access-Network-Info (PANI) header process preference for an adjacency, use the **ims pani** command in adjacency SIP configuration mode. To remove a PANI header process preference from an adjacency, use the no form of this command.

**ims pani** [**received** | **rx** | **received rx** | **rx received**]

**no ims pani** [**received** | **rx** | **received rx** | **rx received**]

## Syntax Description

<b>received</b>	Specifies that information in the PANI header of a received message has preference over information from the Rx interface. The received message PANI is passed through.
<b>rx</b>	Specifies that information from the Rx interface has preference and overrides the information in the PANI header of a received message.
<b>received rx</b>	Specifies that if a received message contains a PANI header, it is passed through. Otherwise, a PANI header is added to the received message, using information from the Rx interface.
<b>rx received</b>	Specifies that information from the Rx interface has preference if there is any. Otherwise, the PANI header of the received message is passed through.

## Command Default

If no keywords are specified, the default is **rx received**.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

This command may be used when the adjacency is active, but it will only apply to new calls. It will not effect existing calls.

## Examples

The following example shows how to configure the PANI header process preference for an adjacency:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
```

```
Router(config-sbc-sbe-adj-sip)# ims pani
```

Related Commands	Command	Description
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.
	<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
	<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
	<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
	<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
	<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
	<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
	<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
	<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
	<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
	<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# ims realm

To configure an IMS realm for use by either an IMS Rx interface or an IMS Rf interface, use the **ims realm** command in adjacency SIP configuration mode. To remove an IMS realm, use the no form of this command.

**ims realm** *realm-name*

**no ims realm** *realm-name*

## Syntax Description

<i>realm-name</i>	Specifies a case sensitive, unique name for the realm. The maximum length is 63 characters.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.1S	This command was updated to support an IMS Rf interface.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure an IMS realm for use by an IMS Rx interface:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# ims realm Realm_1
```

## Related Commands

Command	Description
<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
<b>origin-realm</b>	Configures the domain name of an IMS local realm.
<b>origin-host</b>	Configures the domain name of an IMS local host.
<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.

<b>Command</b>	<b>Description</b>
<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# ims rf

To enable the IP Multimedia Subsystem (IMS) Rf interface for an access adjacency on the Cisco Session Border Controller (SBC), use the **ims rf** command in the SBC SBE adjacency SIP configuration mode. To disable the IMS Rf interface for an access adjacency, use the **no** form of this command.

**ims rf**

**no ims rf**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** SBC SBE adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command cannot be modified unless the operational state of the access adjacency is down.

**Examples** The following example shows how to disable the IMS Rf interface for an access adjacency on the SBC:

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# no ims rf
```



# ims rx

To configure an IMS Rx interface for access adjacency, use the **ims rx** command in adjacency SIP configuration mode. To remove an IMS Rx interface, use the no form of this command.

```
ims rx [pcrf pcrf-name]
```

```
no ims rx [pcrf pcrf-name]
```

## Syntax Description

<b>pcrf</b> <i>pcrf-name</i>	(Optional) Specifies the name of (and provides the contact point to) the Policy and Charging Rule Function (PCRF) operating in Rx mode. The PCRF configures the destination-host AVP used for Diameter messages. The PCRF name must be a case sensitive, unique, fully qualified domain name (FQDN). The maximum is length 128 characters.
------------------------------	--

## Command Default

When PCRF is not specified, Rx messages are routed by realm.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

This command can only be used when the operational state of the adjacency is down.

## Examples

The following example shows how to configure an IMS Rx interface for access adjacency:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip)# ims rx
```

## Related Commands

Command	Description
<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
<b>origin-realm</b>	Configures the domain name of an IMS local realm.

<b>Command</b>	<b>Description</b>
<b>origin-host</b>	Configures the domain name of an IMS local host.
<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# ims rx preliminary-aar-forbid

To prevent preliminary AAR messages from being sent in an IMS Rx session, use the **ims rx preliminary-aar-forbid** command in CAC table entry configuration mode. To return to the default condition where preliminary AAR messages are sent, use the no form of this command.

**ims rx preliminary-aar-forbid**

**no ims rx preliminary-aar-forbid**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Preliminary AAR messages are sent.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to prevent preliminary AAR messages from being sent in an IMS Rx session:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# ims rx preliminary-aar-forbid
```

Related Commands	Command	Description
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.

<b>Command</b>	<b>Description</b>
<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# inbound secure

To configure the incoming calls from an H.323 adjacency as secure calls, use the **inbound secure** command in the H.323 Adjacency configuration mode. To restore the insecure status to the incoming calls, use the **no** form of this command.

**inbound secure**

**no inbound secure**

## Syntax Description

This command has no arguments or keywords.

## Command Default

By default, all the incoming calls are insecure calls.

## Command Modes

H.323 Adjacency configuration mode (config-sbc-sbe-adj-h323)

## Command History

Release	Modification
3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

To ensure that the calls coming from an H323 adjacency are treated as secure calls, define the incoming calls from an H.323 adjacency as secure calls using the **inbound secure** command in the H.323 Adjacency configuration mode. By default, all incoming calls are insecure calls.

To configure the incoming secure calls as not secured, use the **no inbound secure** command from H.323 adjacency configuration mode.



### Note

If an H.323 adjacency is configured as untrusted, you cannot configure an incoming calls as secure calls.

## Examples

The following example shows how to configure incoming calls from an H.323 adjacency as secure calls:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h.323 trust-h323-adj
Router(config-sbc-sbe-adj-h323)# inbound secure
```

## Related Commands

Command	Description
<b>trunk trusted</b>	Configures an H.323 adjacency as trusted.

# inherit profile

To configure a global inherit profile for the SIP adjacency, use the **inherit profile** command in adjacency SIP configuration mode. To deconfigure the global inherit profile, use the **no** form of this command.

**inherit profile** {**preset-access** | **preset-core** | **preset-ibcf-ext-untrusted** | **preset-ibcf-external** | **preset-ibcf-internal** | **preset-p-cscf-access** | **preset-p-cscf-core** | **preset-peering** | **preset-standard-non-ims**}

**no inherit profile**

## Syntax Description

<b>preset-access</b>	Specifies a preset access profile for an adjacency that faces an access device on a User-Network Interface (UNI) location.
<b>preset-core</b>	Specifies a preset core profile for an adjacency that faces a core device on a UNI location. This is the default.
<b>preset-ibcf-ext-untrusted</b>	Specifies a preset IBCF external untrusted profile.
<b>preset-ibcf-external</b>	Specifies a preset IBCF external profile.
<b>preset-ibcf-internal</b>	Specifies a preset IBCF internal profile.
<b>preset-p-cscf-access</b>	Specifies a preset P-CSCF-access profile.
<b>preset-p-cscf-core</b>	Specifies a preset P-CSCF-core profile.
<b>preset-peering</b>	Specifies a preset peering profile for an adjacency that faces a peer device on a Network-Network Interface (NNI) location.
<b>preset-standard-non-ims</b>	Specifies a preset standard-non-IMS profile.

## Command Default

The default inherit profile setting is **preset-core**.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	The command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

This adjacency-specific configuration overrides any global configuration of the adjacency that was configured using the **sip inherit profile** command.

---

**Examples**

The following example shows how the **inherit profile** command is used to configure a P-CSCF-access inherit profile on a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-access
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>adjacency</b>	Configures an adjacency for an SBC.

# interwork cost

To specify the resource cost for an audio stream using inband DTMF interworking or to specify the resource cost for an audio or video stream using SRTP encryption and decryption, use the **transcode cost** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

**interwork** {**inband-dtmf** | **srtp**} **cost** *number*

**no interwork** {**inband-dtmf** | **srtp**} **cost**

## Syntax Description

<b>inband-dtmf</b>	Specifies that the resource cost is to be set for an audio stream that is using inband DTMF interworking.
<b>srtp</b>	Specifies that the resource cost is to be set for an audio or video stream that is using SRTP encryption and decryption.
<i>number</i>	Resource cost. The range is from 1 to 4294967295.

## Command Default

The default resource cost for an audio stream using inband DTMF interworking is 4. Similarly, the default resource cost for an audio or video stream using SRTP encryption and decryption is 15. When you use the **no** form of this command, the resource cost is changed to the default value.

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **interwork cost** command is used to set the resource cost for an audio stream using inband DTMF interworking to 8. This command is also used to set the resource cost for an audio or video stream using SRTP encryption and decryption to 20.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway policy type default
Router(config-sbc-sbe-media-pol)# interwork inband-dtmf cost 8
Router(config-sbc-sbe-media-pol)# interwork srtp cost 20
```



Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# interwork maximum

To specify the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time, use the **interwork maximum** command in the SBE media policy configuration mode. To remove the maximum limit, use the **no** form of this command.

**interwork {inband-dtmf | srtp} maximum *number***

**no interwork {inband-dtmf | srtp} maximum**

## Syntax Description

<i>number</i>	Maximum number of media streams that can use the interworking service specified in the command.
---------------	---

## Command Default

*The default maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time is 4294967295. When you use the **no** form of this command, any maximum limit set earlier is changed to this default value.*

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the **interwork maximum** command is used to set the maximum number of calls that use the SRTP interworking service at any point of time to 500:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
Router(config-sbc-sbe-media-pol)# type cac-policy
Router(config-sbc-sbe-media-pol)# interwork srtp maximum 500
```

Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# invite-timeout

To configure the time that SBC waits for a final response to an outbound SIP invite request, use the **invite-timeout** command in IP timer configuration mode. To return to the default value, use the **no** form of this command.

*invite-timeout* {interval-value}

no *invite-timeout*

<b>Syntax Description</b>	<i>interval-value</i>	Time, in seconds, SBC waits before timing out an outbound invite request.
---------------------------	-----------------------	---

<b>Command Default</b>	The default wait interval is 180 seconds. If no response is received during that time, an internal 408 request timeout response is generated and is sent to the caller.	
------------------------	---	--

<b>Command Modes</b>	SIP timer (config-sbc-sbe-sip-tmr)	
----------------------	------------------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.	
-------------------------	--	--

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.

<b>Examples</b>	The following example shows how to configure the SBC to time out invite transactions after 60 seconds:	
-----------------	--	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# invite-timeout 60
Router(config-sbc-sbe-sip-tmr)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>udp-response-linger-period</b>	Configures the time period that SBC retains negative UDP responses to invite requests.

# ipsec maximum

To specify the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, use the **ipsec maximum** command in the SBE CAC table CAC policy configuration mode. To remove this configuration, use the **no** form of this command.

**ipsec maximum** {registers | calls} *number*

**no ipsec maximum** {registers | calls}

## Syntax Description

<i>number</i>	Specifies one of the following: <ul style="list-style-type: none"> <li>Maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link</li> <li>Maximum number of calls that can use IPsec-protected signaling</li> </ul>
---------------	---

## Command Default

The default maximum number of media streams that can use IPsec encryption and decryption on their signaling link or that can use IPsec-protected signaling, at any point of time, is 4294967295. When you use the no form of this command, any maximum limit set earlier is changed to this default value.

## Command Modes

SBE CAC table CAC policy configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the **ipsec maximum** command is used to set the maximum number of media streams that can use IPsec encryption and decryption on their signaling link to 200. In addition, the command is used to set the maximum number of media streams that can use IPsec-protected signaling to 80.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table t1
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media limits mp1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# ipsec maximum registers 200
Router(config-sbc-sbe-cacpolicy-cactable-entry)# ipsec maximum calls 80
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
<b>media-gateway policy type</b>	Configures a media gateway policy.
<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
<b>media-policy</b>	Configures a media policy.
<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
<b>show sbc sbe media-policy</b>	Displays the details of media policies.
<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# ipv4

To create an IPv4 address within a DBE media address pool, use the **ipv4** command in media address configuration mode. To delete an IPv4 address within a DBE media address pool, use the **no** form of this command.

**ipv4** *ipv4\_address* [**vrf** *vrf-name*]

**no ipv4** *ipv4\_address* [**vrf** *vrf-name*]

Syntax Description	
<i>ipv4_address</i>	Specifies the IPv4 media address.
<i>vrf vrf-name</i>	(Optional) Specifies the VRF name.

**Command Default** No default behavior or values are available.

**Command Modes** Media address (config-sbc-dbe-media-address)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure address 10.0.1.1 for use both for non-VPN media and for media to or from vpn3:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address
Router(config-sbc-dbe-media-address)# media-address ipv4 10.0.1.1
Router(config-sbc-dbe-media-address)# media-address ipv4 10.0.1.1 vrf vpn3
```

# ipv4 (blacklist)

To enter the mode for applying blacklisting options to a single IP address or for configuring the default event limits for the source addresses in a given VPN (where the IP address is under the VPN), use the **ipv4** command in the SBE blacklist configuration mode. Use the no form of the command to remove the blacklist entry for an address.

*ipv4 ip address*

<b>Syntax Description</b>	<i>IP address</i>	Specifies the IPv4 H.248 control address.
---------------------------	-------------------	---

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	SBE blacklist configuration (config-sbc-sbe-blacklist)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.	
-------------------------	--	--

<b>Examples</b>	The following example shows how to enter the mode for applying blacklisting options to a single IP address:	
-----------------	---	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 1.1.1.1
Router(config-sbc-sbe-blacklist-ipv4)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>blacklist</b>
	<b>ipv4 (blacklist)</b>	Enters the mode for applying blacklisting options to a single IP address.
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source.
	<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.



<b>Command</b>	<b>Description</b>
<b>trigger-period</b>	Defines the period over which events are considered.
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.

# ipv4 (SBE H.248)

To configure an SBE to use a given IPv4 H.248 control address, use the **ipv4** command in H.248 control address configuration mode. To delete a given IPv4 H.248 control address, use the **no** form of this command.

**ipv4** *IP address*

**no ipv4** *IP address*

<b>Syntax Description</b>	<i>IP address</i> Specifies the IPv4 H.248 control address.
---------------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	H.248 control address (config-sbc-sbe-ctrl-h248)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

**Examples** The following example shows how to configure an SBE to use a given IPv4 H.248 control address:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 index 0
Router(config-sbc-sbe-ctrl-h248)# ipv4 1.1.1.1
Router(config-sbc-sbe-ctrl-h248)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>control address h248 index</b>	Selects index value and enters H.248 control address mode.
	<b>port (SBE H.248)</b>	Configures an SBE to use a given IPv4 H.248 port.
	<b>transport (SBE H.248)</b>	Configures an SBE to use a certain transport for H.248 communications.

# ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

```
ip access-list {{standard | extended}} {access-list-name | access-list-number} |
  helper egress check
```

```
no ip access-list {{standard | extended}} {access-list-name | access-list-number} |
  helper egress check
```

Syntax Description		
<b>standard</b>		Specifies a standard IP access list.
<b>extended</b>		Specifies an extended IP access list. Required for object-group ACLs.
<i>access-list-name</i>		Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
<i>access-list-number</i>		Number of the access list. <ul style="list-style-type: none"> <li>• A standard IP access list is in the ranges 1–99 or 1300–1999.</li> <li>• An extended IP access list is in the ranges 100–199 or 2000–2699.</li> </ul>
<b>helper egress check</b>		Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address.

**Command Default** No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.4(20)T	This command was modified. Object-group ACLs are now accepted when the <b>deny</b> and <b>permit</b> commands are used in standard IP access-list configuration mode or extended IP access-list configuration mode.
	Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.
	15.0(1)M	This command was modified. The <b>helper</b> , <b>egress</b> , and <b>check</b> keywords were added.

---

**Usage Guidelines**

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Named access lists are not compatible with Cisco IOS software releases prior to Release 11.2.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

---

**Examples**

The following example defines a standard access list named Internetfilter:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in my\_network\_object\_group if the protocol ports match the ports specified in my\_service\_object\_group:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list helper egress check
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>deny</b>	Sets conditions in a named IP access list or in an object-group ACL that will deny packets.
	<b>ip access-group</b>	Applies an ACL or an object-group ACL to an interface or a service policy map.
	<b>object-group network</b>	Defines network object groups for use in object-group ACLs.
	<b>object-group service</b>	Defines service object groups for use in object-group ACLs.
	<b>permit</b>	Sets conditions in a named IP access list or in an object-group ACL that will permit packets.
	<b>show ip access-list</b>	Displays the contents of IP access lists or object-group ACLs.
	<b>show object-group</b>	Displays information about object groups that are configured.

# ip host

To resolve host names to IP addresses in evaluation cases where a DNS server is not available, use the **ip host** command in Global configuration mode. To return to the default value, use the **no** form of this command.

*ip host hostname ip\_address*

*no ip host hostname ip\_address*

## Syntax Description

<i>hostname</i>	Specifies the host name. The following guidelines apply: <ul style="list-style-type: none"> <li>The <i>hostname</i> can include upto 63 characters.</li> <li>Host names must start with a letter and can end with a letter or a digit.</li> </ul>
<i>ip_address</i>	Specifies the IP address.

## Command Default

The default wait interval is 180 seconds. If no response is received during that time, an internal 408 request timeout response is generated and is sent to the caller.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.



### Caution

The **ip host** command provides a mechanism to resolve host names to IP addresses in evaluation cases where a DNS server is not available. Properly designed networks rely on DNS infrastructure to manage the mapping of host names to IP addresses in a scalable and consistent network-wide manner. Use of the **ip host** command in conjunction with a DNS server may result in an undesirable result when the local configuration conflicts with the global DNS mapping.

## Examples

The following example shows how to configure the SBC to time out invite transactions after 60 seconds:

```
Router# configure terminal
Router(config)# ip host host_1 172.18.51.20
```



# ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

```
ip multicast-routing [vrf vrf-name] [distributed]
```

```
no ip multicast-routing [vrf vrf-name]
```

## Cisco IOS XE Release 3.3S

```
ip multicast-routing {[vrf vrf-name] distributed}
```

```
no ip multicast-routing {[vrf vrf-name] distributed}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.	
<b>distributed</b>	(Optional) Enables Multicast Distributed Switching (MDS).	

**Command Default** IP multicast routing is disabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	10.0	This command was introduced.
	11.2(11)GS	The <b>distributed</b> keyword was added.
	12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the <b>no</b> form of this command now disables IP multicast routing on the Multicast Multilayer Switching (MMLS) Route Processor (RP) and purges all multicast MLS cache entries on the MMLS-SE.
	12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
	12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S. This command without the <b>distributed</b> keyword was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.3S	This command was modified. Either the <b>distributed</b> keyword or the <b>vrf</b> <i>vrf-name</i> <b>distributed</b> keyword and argument combination is required with this command in Cisco IOS Release 3.3S.



**Usage Guidelines**

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets. The optional **distributed** keyword for this command is not supported in Cisco IOS XE Release 3.2S. Either the **distributed** keyword or the **vrf vrf-name distributed** keyword and argument combination for this command is required in Cisco IOS XE Release 3.3S and later releases.

**Note**

For IP multicast, after enabling IP multicast routing, PIM must be configured on all interfaces. Disabling IP multicast routing does not remove PIM; PIM still must be explicitly removed from the interface configurations.

**Examples**

The following example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Router(config)# no ip multicast-routing
```

The following example shows how to enable MDS in Cisco IOS XE Release 3.3S a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1 distributed
```

**Related Commands**

Command	Description
<b>ip pim</b>	Enables PIM on an interface.

# ip multicast rpf mofrr

To enable a Provider Edge (PE) router to perform Reverse Path Forwarding (RPF) lookups using multicast only fast re-route (MoFRR) on an IP address of the exit router in the global table or a specific VPN, use the **ip multicast rpf mofrr** command in global configuration mode. To disable this functionality, use the **no** form of this command.

```
ip multicast [vrf vrf-name] rpf mofrr {access-list-number | access-list-name} [sticky]
```

```
no ip multicast [vrf vrf-name] rpf mofrr {access-list-number | access-list-name} [sticky]
```

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Enables a PE router to perform an RPF lookup using MoFRR on the exit router for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
<i>access-list-name</i>	Name of the IP access list or object group access control list (OGACL). Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
<i>access-list-number</i>	Number of the access control list (ACL). MoFRR is enabled for the mroute matching the ACL. <ul style="list-style-type: none"> <li>An extended IP access list is in the range 100 to 199 or 2000 to 2699.</li> </ul> <p><b>Note</b> MoFRR accepts extended ACLs only. It does not accept standard ACLs.</p>
<b>sticky</b>	(Optional) Ensures that the primary RPF does not change even if a better primary comes along. It changes only if for some reason the current primary RPF is unreachable. The <b>sticky</b> keyword ensures that there is no RPF flapping happening on mroutes if the unicast routes are fluctuating for some reason.

## Command Default

The RPF MoFRR functionality is disabled.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

## Usage Guidelines

Use the **ip multicast rpf mofrr** command to enable a PE router to perform RPF lookups using MoFRR on an IP address of the exit router in the global table or a specific VPN. MoFRR uses standard Protocol Independent Multicast (PIM) join messages to set up a primary and a secondary multicast forwarding path by establishing a primary and a secondary RPF interface on each router that receives a PIM join

message. Data is received from both the primary and backup paths. If the router detects a forwarding error in the primary path, it switches RPF to the secondary path and immediately has packets available to forward out to each outgoing interface.

MoFRR accepts extended ACLs only. It does not accept standard ACLs.

---

**Examples**

The following example shows how to enable a PE router to perform RPF lookups using MoFRR for the mroute matching the ACL numbered 150:

```
ip multicast rpf mofrr 150
```

---

**Related Commands**

Command	Description
<b>show ip mroute</b>	Displays information about the multicast routing (mroute) table.
<b>show ip rpf</b>	Displays the information that IP multicast routing uses to perform the RPF check for a multicast source.

---

# ip multicast rpf select topology

To associate a multicast topology with a multicast group with a specific mroute entry, use the **ip multicast rpf select topology** command in global configuration mode. To disable the functionality, use the **no** form of this command.

```
ip multicast rpf select topology { multicast | unicast } topology-name access-list-number
```

```
no ip multicast rpf select topology { multicast | unicast } topology-name access-list-number
```

## Syntax Description

<b>multicast</b>	Associates a multicast topology with an (S,G) mroute entry.
<b>unicast</b>	Associates a unicast topology with an (S,G) mroute entry.
<i>topology-name</i>	Name of the topology instance.
<i>access-list-number</i>	Number of the access list.

## Command Default

The topology is not associated with an (S,G) mroute entry.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

## Usage Guidelines

The **ip multicast rpf select topology** command associates a multicast topology with an (S,G) mroute entry. One (S,G) mroute entry can be associated with multiple topologies. During RPF lookup, PIM MT-ID will be used (smaller ID has higher priority) to select a topology.

One access list could be associated with multiple (S,G) mroute entries. The sequence number in the access list is used to determine the order of (S,G) mroute entry lookup within the access list.

One topology can be associated with only one access list.

## Examples

The following example shows how to associate a multicast topology with an (S,G) mroute entry:

```
ip multicast rpf select topology multicast topology live-A 111
```

## Related Commands

Command	Description
<b>debug ip multicast topology</b>	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
<b>ip multicast topology</b>	Configures topology selection for multicast streams.
<b>show ip multicast topology</b>	Displays IP multicast topology information.

# ip multicast topology

To configure topology selection for multicast streams, use the **ip multicast topology** command in global configuration mode. To disable the functionality, use the **no** form of this command.

```
ip multicast topology { multicast | unicast } topology-name tid topology-number
```

```
no ip multicast topology { multicast | unicast } topology-name tid topology-number
```

## Syntax Description

<b>multicast</b>	Configures a multicast topology instance.
<b>unicast</b>	Configures a unicast topology instance.
<i>topology-name</i>	Name of the topology instance.
<b>tid</b> <i>topology-number</i>	Specifies the number of the topology identifier.

## Command Default

All multicast streams are associated with the multicast base topology.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

## Usage Guidelines

The **ip multicast topology** command configures topology selection for multicast streams, which is usually only required for first hop and last hop routers (and may not be required for transit routers in between). The stream, specified by an extended IP access list, can be source based, group based, or a combination of both. The sequence number in the access list will decide the order of the (S,G) mroute entries.

## Examples

The following example shows how to configure topology selection for multicast streams:

```
ip multicast topology multicast live-A 111
```

## Related Commands

Command	Description
<b>debug ip multicast topology</b>	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
<b>ip multicast rpf select topology</b>	Associates a multicast topology with a multicast group with a specific mroute entry.
<b>show ip multicast topology</b>	Displays IP multicast topology information.

# ip precedence

To configure an IP precedence with which to mark IP packets belonging to the given QoS profile, use the **ip precedence** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

**ip precedence** *value*

**no ip precedence**

## Syntax Description

*value* Specifies the IP precedence with which to mark packets. Range is 0 to 7.

## Command Default

*value*: 0

## Command Modes

Qos sig configuration (config-sbc-sbe-qos-sig)  
 QoS video configuration (config-sbc-sbe-qos-video)  
 QoS voice configuration (config-sbc-sbe-qos-voice)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the QoS profile to mark IP packets with a precedence of 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos sig residential
Router(config-sbc-sbe-qos-sig)# ip precedence 1
Router(config-sbc-sbe-qos-sig)#
```

# ip service reflect

To match and rewrite multicast packets routed onto a Vif1 interface, use the **ip service reflect** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**ip service reflect** *input-interface* **destination** *destination-address* **to** *new-destination-address*  
**mask-len** *number* **source** *new-source-address*

**no ip service reflect** *input-interface* **destination** *destination-address* **to** *new-destination-address*  
**mask-len** *number* **source** *new-source-address*

Syntax Description		
<i>input-interface</i>		Interface type and number.
<b>destination</b>		Identifies packets with the specified destination address.
<i>destination-address</i>		Destination IP address in the packets, in A.B.C.D format.
<b>to</b>		Modifies the destination IP address in reflected packets to a new IP address.
<i>new-destination-address</i>		New destination address to be used, in A.B.C.D format.
<b>mask-len</b> <i>number</i>		Specifies the mask length of the destination address to match. The <i>number</i> argument is a value from 0 to 32.
<b>source</b>		Modifies the source address in reflected packets. The source address must be on the same subnet as the Vif1 interface.
<i>new-source-address</i>		New source address to be used, in A.B.C.D format.

**Command Default** The multicast service reflection feature is disabled.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	12.4(4)T	This command was introduced.
	12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
	Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

**Usage Guidelines** Use the **ip service reflect** command to match and rewrite multicast packets routed onto a Vif1 interface. The matched and rewritten packet is sent back into Cisco multicast packet routing, where it is handled like any other packet arriving from an interface.

More than one multicast service reflection operation can be configured to match the same packet, allowing you to replicate the same received traffic to multiple destination addresses.

---

**Examples**

The following example shows how to translate any multicast packet with a destination address of 239.1.1.0/24 to a destination of 239.2.2.0/24 with a new source address of 10.1.1.2. For example, a packet with a source and destination of (10.10.10.10, 239.1.1.15) would be translated to (10.1.1.2, 239.2.2.15).

```
Router(config)# interface Vif1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip service reflect Ethernet 0/0 destination 239.1.1.0 to 239.2.2.0
mask-len 24 source 10.1.1.2
Router(config-if)# ip igmp static-group 239.1.1.0
Router(config-if)# ip igmp static-group 239.1.1.1
```



# ip TOS (session border controller)

To configure an IP ToS (type of service) with which to mark IP packets belonging to the QoS profile, use the **ip TOS** command in the appropriate configuration mode. To return the QoS profile to setting the default IP ToS, use the **no** form of this command.

**ip TOS** *value*

**no ip TOS**

## Syntax Description

value	Specifies the IP ToS with which to mark packets. This may be a value of 0 (normal service) or a bit field consisting of one or more of the following bits: <ul style="list-style-type: none"> <li>8: Minimize delay.</li> <li>4: Maximize throughput.</li> <li>2: Maximize reliability.</li> <li>1: Minimize monetary cost.</li> </ul>
-------	--

## Command Default

The default IP ToS is 0 (normal service).

## Command Modes

Qos sig configuration (config-sbc-sbe-qos-sig)  
 QoS video configuration (config-sbc-sbe-qos-video)  
 QoS voice configuration (config-sbc-sbe-qos-voice)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure an IP TOS:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos sig residential
Router(config-sbc-sbe-qos-sig)# ip tos 12
Router(config-sbc-sbe-qos-sig)#
```

# ip wccp outbound-acl-check

To check the outbound access control list (ACL) for Web Cache Communication Protocol (WCCP), use the **ip wccp outbound-acl-check** command in global configuration mode. To disable the outbound check, use the **no** form of this command.

**ip wccp outbound-acl-check**

**no ip wccp outbound-acl-check**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Check of the outbound ACL services is not enabled.

**Command Modes** Global configuration (config)

## Command History

Release	Modification
12.3(14)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

## Usage Guidelines

This command performs the same function as the **ip wccp check acl outbound** command.

## Examples

The following example shows how to configure a router to check the outbound ACL for WCCP:

```
Router(config)# ip wccp outbound-acl-check
```

## Related Commands

Command	Description
<b>ip wccp</b>	Enables support of the WCCP service for participation in a service group.
<b>ip wccp check acl outbound</b>	Checks the outbound ACL for WCCP.
<b>ip wccp check services all</b>	Enables all WCCP services.
<b>ip wccp version</b>	Specifies which version of WCCP to use on a router.

## ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

```
ip wccp [vrf vrf-name] {web-cache | service-number} redirect {in | out}
```

```
no ip wccp [vrf vrf-name] {web-cache | service-number} redirect {in | out}
```

Syntax Description		
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.	
<b>web-cache</b>	Enables the web cache service.	
<i>service-number</i>	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 254.  If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.	
<b>in</b>	Specifies packet redirection on an inbound interface.	
<b>out</b>	Specifies packet redirection on an outbound interface.	

**Command Default** Redirection checking on the interface is disabled.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.0(11)S	The <b>in</b> keyword was added.
	12.1(3)T	The <b>in</b> keyword was added.
	12.2(17d)SXB	Support for this command on the Cisco 7600 series router Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
	12.2(18)SXD1	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 720.
	12.2(18)SXF	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 32.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. <b>Note</b> The <b>out</b> keyword is not supported in Cisco IOS XE Release 2.2.
	15.0(1)M	This command was modified. The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

Release	Modification
12.2(33)SRE	This command was modified. The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
Cisco IOS XE Release 3.1S	This command was modified. The <b>vrf</b> keyword and <i>vrf-name</i> argument were added. Support for the <b>out</b> keyword was added.

### Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

The **ip wccp redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ip wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.



#### Tips

Be careful not to confuse the **ip wccp redirect {out | in}** interface configuration command with the **ip wccp redirect exclude in** interface configuration command.



#### Note

This command has the potential to affect the **ip wccp redirect exclude in** command. (These commands have opposite functions.) If you have **ip wccp redirect exclude in** set on an interface and you subsequently configure the **ip wccp redirect in** command, the “exclude in” command will be overridden. The opposite is also true: configuring the “exclude in” command will override the “redirect in” command.

### Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when fast/CEF switching is enabled:

```
Router(config)# interface multilink2
Router(config-if)# ip address 10.21.21.1 255.255.255.0
Router(config-if)# ip access-group IDS_Multilink2_in_1 in
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ip nat outside
Router(config-if)# ip inspect FSB-WALL out
Router(config-if)# max-reserved-bandwidth 100
Router(config-if)# service-policy output fsb-policy
Router(config-if)# no ip route-cache
Router(config-if)# load-interval 30
Router(config-if)# tx-ring-limit 3
Router(config-if)# tx-queue-limit 3
Router(config-if)# ids-service-module monitoring
```

```
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 2
Router(config-if)# crypto map abc1
```

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 is redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

#### Related Commands

Command	Description
<b>ip wccp redirect exclude in</b>	Enables redirection exclusion on an interface.
<b>show ip interface</b>	Displays the usability status of interfaces that are configured for IP.
<b>show ip wccp</b>	Displays the WCCP global configuration and statistics.

## ip wccp source-interface

To specify the interface that Web Cache Communication Protocol (WCCP) uses as the preferred router ID and generic routing encapsulation (GRE) source address, use the **ip wccp source-interface** command in global configuration mode. To enable the WCCP default behavior for router ID selection, use the **no** form of this command.

```
ip wccp [vrf vrf-name] source-interface source-interface
```

```
no ip wccp [vrf vrf-name] source-interface
```

### Syntax Description

<b>vrf vrf-name</b>	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
<b>source-interface</b>	The type and number of the source interface.

### Command Default

If this command is not configured, WCCP selects a loopback interface with the highest IP address as the router ID.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

### Usage Guidelines

Use this command to set the interface from which WCCP may derive the router ID and GRE source address. The router ID must be a reachable IPv4 address.

The interface identified by the *source-interface* argument must be assigned an IPv4 address and be operational before WCCP uses the address as the router ID. If the configured source interface cannot be used to derive the WCCP router ID, a Cisco IOS error message similar to the following is displayed:

```
%WCCP-3-SIFIGNORED: source-interface interface ignored (reason)
```

The *reason* field in the error output indicates why the interface has been ignored and can include the following:

- **VRF mismatch**—The VRF domain associated with the interface does not match the VRF domain associated with the WCCP command.
- **interface does not exist**—The interface has been deleted.
- **no address**—The interface does not have a valid IPv4 address.
- **line protocol down**—The interface is not fully operational.

This command provides control only of the router ID and GRE source address. This command does not influence the source address used by WCCP control protocol (“Here I Am” and Removal Query messages). The WCCP control protocol is not bound to a specific interface and the source address is always selected based on the destination address of an individual packet.

**Examples**

The following example shows how to select Gigabit Ethernet interface 0/0/0 as the WCCP source interface:

```
Router(config)# ip wccp source-interface gigabitethernet0/0/0
```

**Related Commands**

Command	Description
<b>ip wccp</b>	Enables support of the specified WCCP service for participation in a service group.
<b>show ip wccp</b>	Displays the WCCP global configuration and statistics.
<b>show ip wccp global counters</b>	Displays global WCCP information for packets that are processed in software.
<b>show platform software wccp</b>	Displays platform specific configuration and statistics related WCCP information on Cisco ASR 1000 Series Routers.

# ip wccp version

To specify the version of Web Cache Communication Protocol (WCCP), use the **ip wccp version** command in global configuration mode.

```
ip wccp version {1 | 2}
```

Syntax Description	1	2
	Specifies Web Cache Communication Protocol Version 1 (WCCPv1).	Specifies Web Cache Communication Protocol Version 2 (WCCPv2).

**Command Default** WCCPv2

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. Only WCCP version 2 is supported in Cisco IOS XE Release 2.2.

**Usage Guidelines** Configuring this command does not have any impact on Cisco ASR 1000 Series Routers because these routers support only WCCPv2. WCCPv2 is enabled by default on Cisco ASR 1000 series routers when a service group is configured or a service group is attached to an interface.

**Examples** In the following example, the user changes the WCCP version from the default of WCCPv2 to WCCPv1, starting in privileged EXEC mode:

```
Router(config)# ip wccp version 1
```

```
Router# show ip wccp
```

```
% WCCP version 2 is not enabled
```

Related Commands	Command	Description
	<b>ip wccp</b>	Enables support of the WCCP service for participation in a service group.
	<b>show ip wccp</b>	Displays the WCCP global configuration and statistics.



# key (session border controller)

To configure the authentication key of the accounting and authentication servers, use the **key** command in the appropriate server configuration mode. To disable any previously set authentication key, use the **no** form of this command.

**key** *key*

**no key**

<b>Syntax Description</b>	<i>key</i> Specifies the authentication key. This is only valid if authentication is turned on.
---------------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Server accounting (config-sbc-sbe-acc-ser) Server authentication (config-sbc-sbe-auth)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the <i>acctsvr</i> accounting server with the <i>HJ5689</i> authentication key and <i>acctsvr2</i> accounting server with the <i>cisco</i> authentication key on mySbc for RADIUS client instance radius1:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting radius1
Router(config-sbc-sbe-acc)# server acctsvr
Router(config-sbc-sbe-acc-ser)# key HJ5689
Router(config-sbc-sbe-acc-ser)# exit
Router(config-sbc-sbe-acc)# server acctsvr2
Router(config-sbc-sbe-acc-ser)# key cisco
Router(config-sbc-sbe-acc-ser)# exit
Router(config-sbc-sbe-acc)# exit
Router(config-sbc-sbe)# exit
```

# Idr-check

To configure the time of day (local time) to run the Long Duration Check (LDR), use the **ldr-check** command in SBE billing configuration mode. To return to 00:00, use the **no** form of this command.

**ldr-check** {*HH MM*}

**no ldr-check**

<b>Syntax Description</b>	<i>HH:MM</i> Time in hours and minutes using a 24-hour clock. The range of the <i>HH</i> argument is 0 to 23. The range of the <i>MM</i> argument is 0 to 59.
---------------------------	---

<b>Command Default</b>	<i>HH MM</i> : 00 00
------------------------	----------------------

<b>Command Modes</b>	SBE billing configuration (config-sbc-sbe-billing)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.

**Examples**

The following example shows how to configure the remote long-duration-call check to occur at 10.30 p.m., to specify the time each day when SBC should check for any call whose duration is over 24 hours:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# ldr-check 22 30
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
	<b>billing</b>	Configures billing.
	<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.

<b>Command</b>	<b>Description</b>
<b>method packetcable-em</b>	Enables the packet-cable billing method.
<b>packetcable-em transport radius</b>	Configures a packet-cable billing instance.
<b>show sbc sbe billing remote</b>	Displays the local and billing configurations.

# Idr-check (XML billing)

To configure the time at which to check all calls over 24-hour-long, use the **ldr-check** *hour min* command in the SBE billing XML configuration mode. To disable the configuration, use the **no** form of this command.

**ldr-check** *hour min*

**no ldr-check**

Syntax Description	hour	Number to indicate the hour at which calls that are more than 24-hours-long will be checked. The hour format should be set using the 24-hour clock.
	min	Number to indicate the minutes at which long duration records will be checked.

**Command Default** By default, the LDR checks are done at 00:00 hours.

**Command Modes** SBE billing XML configuration (config-sbc-sbe-billing-xml)

Command History	Release	Modification
	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

**Usage Guidelines** It is important to take a note of calls that are more than 24-hours-long. To report long duration calls that are more than 24 hours, use the **ldr-check** *hour min* command from SBE billing XML configuration mode. The initial value is inherited from the value in the Billing-MGR table. The hour and minute values must be set using the 24-hour clock. The **no** form of the command does not require any parameter. The default duration at which LDR checks are performed is 00 hour and 00 minutes.

**Examples** The following example shows how to configure the time 23 hour and 30 minutes to check long duration calls:

```
Router(config)# sbc sbcbilling
Router(config-sbc)# sce
Router(config-sbc-sce)# billing
Router(config-sbc-sce-billing)# xml method
Router(config-sbc-sce-billing)# xml 1
Router(config-sbc-sce-billing-xml)# ldr-check 23 30
```

Related Commands	Command	Description
	<b>xml (billing)</b>	Configures the method index for XML billing.
	<b>method xml</b>	Configures the billing method as XML.
	<b>cdr path</b>	Configures the time at which long duration records are checked.

# load-order

To specify the load order of a script in a script set, use the **load-order** command in the SBE script-set script configuration mode.

**load-order** *load-order-number*

<b>Syntax Description</b>	<i>load-order-number</i>	Order in which the script must be loaded. The range is from 1 to 4294967295.
---------------------------	--------------------------	--

<b>Command Default</b>	The default load order number of the first script set that you configure without using the <b>load-order</b> command, is 100. For scripts that are subsequently added without using the <b>load-order</b> command, the default order index number is set in multiples of 100, that is, 200, 300, 400, and so on.	
------------------------	--	--

<b>Command Modes</b>	SBE script-set script configuration (config-sbc-sbe-scrpset-script)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command. Note that scripts are loaded in ascending order of the order index number. For example, a script with the order index number 4 is loaded before a script with the order index number 6.
-------------------------	---

<b>Examples</b>	In the following example, the <b>load-order</b> command is used to specify 2 as the load order:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# script-set 10 lua
Router(config-sbc-sbe-script-set)# script mySBCScript
Router(config-sbc-sbe-scrpset-script)# load-order 2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>active-script-set</b>	Activates a script set,
	<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
	<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
	<b>editor</b>	Specifies the order in which a particular editor must be applied.

<b>Command</b>	<b>Description</b>
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# local-address ipv4

To configure the local IPv4 address that appears in the CDR, use the **local-address ipv4** command in SBE billing configuration mode. To deconfigure the local IPV4 address, use the **no** form of this command.

**local-address ipv4** {A.B.C.D.}

**no local-address ipv4**

## Syntax Description

A.B.C.D. Local IPv4 address to be configured.

## Command Default

No default behavior or values are available.

## Command Modes

SBE billing configuration

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.



### Note

This field cannot be reconfigured when billing is active.

## Examples

The following example shows how to configure the local-address to 10.20.1.1 for the billing:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing remote
Router(config-sbc-sbe-billing)# local-address ipv4 10.20.1.1
```

## Related Commands

Command	Description
<b>billing</b>	Configures billing.
<b>ldr-check</b>	Configures the time of day (local time) to run the Long Duration Check (LDR).

<b>Command</b>	<b>Description</b>
<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
<b>method packetcable-em</b>	Enables the packet-cable billing method.
<b>packetcable-em transport radius</b>	Configures a packet-cable billing instance.
<b>show sbc sbe billing remote</b>	Displays the local and billing configurations.



# local-address ipv4 (packet-cable)

To configure the local address of the packet-cable billing instance, use the **local-address ipv4** command in the packetcable-em configuration mode. To disable the local address, use the **no** form of this command.

**local-address ipv4 A.B.C.D.**

**no local-address ipv4**

## Syntax Description

**A.B.C.D.** Local IPv4 address to be configured.

## Command Default

0.0.0.0

## Command Modes

Packet-cable em configuration (config-sbc-sbe-billing-packetcable-em)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If no address is configured, the SBC uses any local address.

## Examples

The following example shows how to enter the billing mode for mySbc:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
(config-sbc-sbe-billing)# packetcable-em 4 transport radius test
(config-sbc-sbe-billing-packetcable-em)# local-address ipv4 10.10.10.10
```

## Related Commands

Command	Description
<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
<b>attach</b>	activate the billing for a RADIUS client
<b>batch-size</b>	Configures the batching or grouping of RADIUS messages sent to a RADIUS server.
<b>batch-time</b>	Configures the maximum number of milliseconds for which any record is held in the batch before the batch is sent
<b>deact-mode</b>	Configures the deactivate mode for the billing method.

<b>Command</b>	<b>Description</b>
<b>ldr-check</b>	Configures the time of day (local time) to run the Long Duration Check (LDR).
<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
<b>local-address ipv4 (packet-cable)</b>	Configures the local address of the packet-cable billing instance.
<b>method packetcable-em</b>	Enables the packet-cable billing method.
<b>packetcable-em transport radius</b>	Configures a packet-cable billing instance.
<b>show sbc sbe billing remote</b>	Displays the local and billing configurations.

# local-id host

To configure the local identify name on a SIP adjacency, use the **local-id** command in adjacency SIP configuration mode. To remove this configuration, use the **no** form of this command.

**local-id host** *name*

**no local-id host**

<b>Syntax Description</b>	<p><i>name</i> Specifies the local identity name to present on outbound SIP messages.</p> <p>The following guidelines apply:</p> <ul style="list-style-type: none"> <li>• Upto 30 alphanumeric characters are allowed.</li> <li>• Except for the underscore sign (<code>_</code>), it is recommended that you do not use any special character.</li> <li>• The <i>name</i> can be a DNS name.</li> </ul> <p>The <i>name</i> must not contain a port.</p>
---------------------------	--

<b>Command Default</b>	When the name field is not set, the local signaling address is used in SIP messages.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to set the SIP local identity of SIP adjacency SipToIsp42 to mcarthur:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# local-id host mcarthur
```

# local-jitter-ratio

To specify the percentage of calls that must be used to calculate the local jitter ratio, use the **local-jitter-ratio** command in the adjacency H.323 configuration mode or adjacency SIP configuration mode. To remove this configuration, use the **no** form of this command.

**local-jitter-ratio** *call-percentage*

**no local-jitter-ratio**

## Syntax Description

<i>call-percentage</i>	Percentage of calls. The range is from 0 to 1000. For example, if you enter 305 as the value of <i>call-percentage</i> , the SBC uses 30.5 percent of the calls for measuring local jitter.
------------------------	---

## Command Default

By default, the value of *call-percentage* is 0 because jitter determination is a performance drain on the MPF. When the value is 0, measurements of the jitter ratio and the MOS-CQE are not available for the adjacency.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **local-jitter-ratio** command is used to specify that 20.5 percent of the calls must be used to calculate the local jitter ratio:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 adj1
Router(config-sbc-sbe-adj-h323)# local-jitter-ratio 305
```

## Related Commands

Command	Description
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
<b>current15minutes</b>	Specifies that QoS statistics must be calculated for 15-minute intervals.

<b>Command</b>	<b>Description</b>
<b>current5minutes</b>	Specifies that QoS statistics must be calculated for 5-minute intervals.
<b>currentday</b>	Specifies that statistics must be calculated for 24-hour intervals.
<b>currenthour</b>	Specifies that QoS statistics must be calculated for 60-minute intervals.
<b>currentindefinite</b>	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
<b>g107 bpl</b>	Sets a value for the Packet-Loss Robustness (Bpl) factor.
<b>g107 ie</b>	Sets a value for the Equipment Impairment (Ie) factor.
<b>g107a-factor</b>	Sets a value for the Advantage (A) factor.
<b>show sbc sbe adjacencies</b>	Displays details of the adjacencies configured on the SBE.
<b>show sbc sbe call-stats</b>	Displays the statistics pertaining to all the calls on a the SBE.
<b>snmp-server enable traps sbc</b>	Enables SBC notification types.
<b>statistics</b>	Specifies the QoS statistic for which alert levels must be set.

# local-port (session border controller)

To configure a data border element (DBE) to use a specific local port when connecting to the default media gateway controller (MGC), use the **local-port** command in either SBC configuration mode or VDBE configuration mode. To disable this configuration, use the **no** form of this command.

**local-port** {*abcd*}

**no local-port** {*abcd*}

## Syntax Description

*abcd* This is the number of the local port the DBE uses.

## Command Default

Default is to use local port 2944. Note that use-any-local-port should not be used when there is a redundant Session Border Controller (SBC). If it is, the connection to the MGC may be lost with an SBC switch over.

## Command Modes

VDBE configuration (config-sbc-dbe-vdbe) for distributed SBC

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for distributed SBC.

## Usage Guidelines

The Examples section shows the hierarchy of modes required to run the command.

The local port cannot be modified after any controller has been configured on the DBE. You must delete the controller before you can modify or configure the local port.

## Examples

The following example creates a DBE service on a distributed SBC called mySbc and configures the DBE to use the local port number 5090:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# local-port 5090
Router(config-sbc-dbe-vdbe)# end
```

The following example creates a DBE service on a unified SBC called mySbc and configures the DBE to use the local port number 5090:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc)# vdbe
Router(config-sbc-vdbe)# local-port 5090
Router(config-sbc-vdbe)# end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>use-any-local-port</b>	Configures a DBE to use any available local port when connecting to the default MGC.

# location-id (session border controller)

To configure the location ID for a DBE service of the Session Border Controller (SBC), use the **location-id** command in SBC-DBE configuration mode. To set the location ID to the default, use the **no** form of this command.

**location-id** *location-id*

**no location-id** *location-id*

Syntax Description	
location-id	The location ID of the DBE. The location ID range is from -1 to 65535.

Command Default	
	The default location-id is -1

Command Modes	
	SBC-DBE configuration (config-sbc-dbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	
	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The **no** form of the command does not take an argument and sets the location-id to the default, which is 0xFFFFFFFF (-1).

A location ID is configured on each DBE. The SBE may associate endpoints with a particular location ID and then use the location IDs to route calls between different DBEs.

Use the **dbe** command to enter into SBC-DBE configuration mode prior to entering the **location-id** command.

Examples	
	The following example creates a DBE service on an SBC called mySbc, enters into SBC-DBE configuration mode, and sets the location ID for a DBE to be 1:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# location-id 1
Router(config-sbc-dbe)# exit
```

Related Commands	Command	Description
	<b>dbe</b>	Creates the DBE service on a SBC and enters into DBE-SBE configuration mode.



# max-call-rate-per-scope

To configure the maximum call rate for an entry in an admission control table and specify the averaging period to be used in rate calculation, use the **max-call-rate-per-scope** command in the CAC table configuration mode. To unconfigure the maximum call rate for an entry in an admission control table and to remove the averaging period, use the **no** form of this command.

**max-call-rate-per-scope** *limit* [**averaging-period** *period-num*]

**no max-call-rate-per-scope** *limit* [**averaging-period** *period-num*]

<b>Syntax Description</b>	<i>limit</i>	A positive integer specifying the maximum number of subscriber registrations per minute to permit at the relevant scope. Only one parameter should be supplied for each command. The range is from 0 to 2147483647.
	<b>averaging-period</b>	Specifies the averaging period to be used in rate calculation. By default, 1 is selected.
	<i>period-num</i>	The rate based on the specified averaging period. The range is from 1 to 2.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The <b>max-call-rate</b> command was renamed as the <b>max-call-rate-per-scope</b> command. The <b>averaging-period</b> keyword and the <i>period-num</i> argument were also added

**Usage Guidelines** Only one parameter should be supplied for each command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to configure the maximum call rate for an entry CAC table 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry) # max-call-rate-per-scope 10
averaging-period 2
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.
<b>max-num-calls</b>	Configures the maximum number of calls pertaining to an entry in an admission control table.
<b>max-regs</b>	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
<b>max-reg-rate-per-scope</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.

# max-connections

To configure the maximum number of SIP connections that will be made to each remote address, use the **max-channels** command in SBE configuration mode. To set this to an unlimited number of connections, use the **no** form of this command.

**max-connections** *number-of-connections*

**no max-connections** *number-of-connections*

## Syntax Description

**number-of-connections** The maximum number of connections.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command configures the maximum number of connections to each remote address to 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip max-connections 1
```

## Related Commands

Command	Description
<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
<b>max-call-rate-per-scope</b>	Configures the maximum call rate for an entry in an admission control table.
<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.
<b>max-num-calls</b>	Configures the maximum number of calls of an entry in an admission control table.
<b>max-regs</b>	Configures the maximum number of subscriber registrations of an entry in an admission control table.

<b>Command</b>	<b>Description</b>
<b>max-regs-rate-per-scope</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.

# max-in-call-msg-rate

To configure the maximum in-call rate and specify the averaging period to be used in rate calculation, use the **max-in-call-msg-rate** command in the CAC table entry configuration mode. To deconfigure the maximum in-call rate and remove the specified averaging period, use the **no** form of this command.

**max-in-call-msg-rate** limit [**averaging-period** *period-num*]

**no max-in-call-msg-rate** limit [**averaging-period** *period-num*]

Syntax Description		
	limit	The maximum number of in-call messages per minute. The range is from 0 to 2147483647.
	<b>averaging-period</b>	Specifies the averaging period to be used in the rate calculation. By default, 1 is selected.
	<i>period-num</i>	The rate based on the specified averaging period. Valid range is from 1 to 2.

**Command Default** No limit.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The <b>max-in-call-rate</b> command was renamed as <b>max-in-call-msg-rate</b> . The <b>averaging-period</b> keyword and the <i>period-num</i> argument were also added

**Usage Guidelines** In-call messages include all the messages within the context of a call, including provisional responses during call setup and call renegotiation messages, but not including call setup or tear-down messages. When configuring the maximum rate of in-call messages in Call Admission Control (CAC), note that the following messages are not rate-limited:

- SIP INVITE requests: 200 responses and ACK messages
- SIP PRACK messages and response
- SIP BYE messages and responses
- Any SIP message with nonduplicate SDP on
- For H.323 calls: Q.931 SETUP, Q.931 CONNECT, and Q.931 RELEASE messages

The Cisco Unified Border Element (SP Edition) will reject the in-call messages when the rate exceeds the rate that is specified in the CAC.

The averaging period must be configured using the **cac-policy-set** command before the averaging period is specified in this command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

### Examples

The following command shows how to configure the maximum number of connections to each remote address to 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 200
Router(config-sbc-sbe)# cac-policy-set averaging-period 2 500
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-in-call-msg-rate 500 averaging-period 2
```

### Related Commands

Command	Description
<b>max-out-call-msg-rate</b>	Configures the maximum out-call rate in an admission control table and specifies the averaging period to be used in rate calculation.
<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
<b>max-call-rate-per-scope</b>	Configures the maximum call rate for an entry in an admission control table and specifies the averaging period to be used in the rate calculation.
<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.
<b>max-num-calls</b>	Configures the maximum number of calls pertaining to an entry in an admission control table.
<b>max-regs</b>	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
<b>max-regs-rate-per-scope</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.

# max-num-calls

To configure the maximum number of calls of an entry in an admission control table, use the **max-num-calls** command in CAC table configuration mode. To delete the maximum number of calls in the given entry in the admission control table, use the **no** form of this command.

**max-num-calls** *mnc*

**no max-num-calls** *mnc*

<b>Syntax Description</b>	<i>mnc</i>	Positive integer specifying the maximum number of calls to permit at the relevant scope.
---------------------------	------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC table configuration (config-sbc-sbe-cacpolicy-cactable)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the maximum number of calls for an entry in the new admission control table MyCacTable:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-num-calls 50
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
	<b>max-call-rate-per-scope</b>	Configures the maximum call rate for an entry in an admission control table.
	<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.

<b>Command</b>	<b>Description</b>
<b>max-connections</b>	Configures the maximum number of SIP connections that will be made to each remote address.
<b>max-regs</b>	Configures the maximum number of subscriber registrations of an entry in an admission control table.
<b>max-regs-rate-per-scope</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.



# max-out-call-msg-rate

To configure the maximum out-call rate and specify the averaging period to be used in rate calculation, use the **max-out-call-msg-rate** command in the CAC table entry configuration mode. To disable the maximum out-call rate and remove the specified averaging period, use the **no** form of this command.

**max-out-call-msg-rate** limit [**averaging-period** *period-num*]

**no max-out-call-msg-rate** *limit* [**averaging-period** *period-num*]

Syntax Description		
	limit	The maximum number of call-out messages per minute. The range is from 0 to 2147483647.
	<b>averaging-period</b>	Specifies the averaging period to be used in rate calculation. By default, 1 is selected.
	<i>period-num</i>	The rate based on the specified averaging period. The range is from 1 to 2.

**Command Default** No limit.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The <b>max-out-call-rate</b> command was renamed as <b>max-out-call-msg-rate</b> . The <b>averaging-period</b> keyword and the <i>period-num</i> argument were also added

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

The averaging period must be configured using the **cac-policy-set** command before the averaging period is specified in this command.

**Examples** The following command shows how to configure the maximum number of connections to each remote address to 1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 200
Router(config-sbc-sbe)# cac-policy-set averaging-period 2 500
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
```

```
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-out-call-msg-rate 500
averaging-period 2
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>max-in-call-msg-rate</b>	Configures the maximum in-call rate in an admission control table and specifies the averaging period to be used in rate calculation.
<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
<b>max-call-rate-per-scope</b>	Configures the maximum call rate for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.
<b>max-num-calls</b>	Configures the maximum number of calls pertaining to an entry in an admission control table.
<b>max-regs</b>	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
<b>max-regs-rate-per-scope</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.

# max-recursive-depth

To configure the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR), use the **max-recursive-depth** command in ENUM configuration mode. To return the maximum number of recursive ENUM look-ups to the default value, use the no form of this command.

**max-recursive-depth** *number*

**no max-recursive-depth** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of look-ups. The range is 1 to 2147483647.
---------------------------	---------------	---

<b>Command Default</b>	The default 5.
------------------------	----------------

<b>Command Modes</b>	ENUM configuration (config-sbc-sbe-enum)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
-----------------	--

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# max-recursive-depth 100
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
	<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.

<b>Command</b>	<b>Description</b>
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe</b> <b>call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum</b> <b>entry</b>	Displays the contents of an ENUM client entry.

# max-regs-rate-per-scope

To configure the maximum call number of subscriber registrations for an entry in an admission control table and specify the averaging period to be used in rate calculation, use the **max-regs-rate-per-scope** command in the CAC table configuration mode. To delete the maximum number of subscriber registrations in a given entry in the admission control table and to remove the averaging period, use the **no** form of this command.

**max-regs-rate-per-scope** *limit* [**averaging-period** *period-num*]

**no max-regs-rate-per-scope** *limit* [**averaging-period** *period-num*]

## Syntax Description

<i>limit</i>	A positive integer specifying the maximum number of subscriber registrations per minute to permit at the relevant scope. Only one parameter should be supplied for each command. The range is from 0 to 2147483647.
<b>averaging-period</b>	Specifies the averaging period to be used in rate calculation. By default, 1 is selected.
<i>period-num</i>	The rate based on the specified averaging period. The range is from 1 to 2.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The <b>max-regs-rate</b> was renamed as <b>max-regs-rate-per-scope</b> . The <b>averaging-period</b> keyword and the <i>period-num</i> argument were also added

## Usage Guidelines

Only one parameter should be supplied for each command.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

The averaging period must be configured using the **cac-policy-set** command before the averaging period is specified in this command.

## Examples

The following example shows how to configure the maximum registration rate for an entry in the new admission control table MyCacTable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set averaging-period 1 200
```

```

Router(config-sbc-sbe)# cac-policy-set averaging-period 2 500
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-regs-rate-per-scope 300
averaging-period 2

```

**Related Commands**

Command	Description
<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
<b>max-call-rate-per-scope</b>	Configures the maximum call rate for an entry in an admission control table and specifies the averaging period to be used in rate calculation.
<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.
<b>max-num-calls</b>	Configures the maximum number of calls pertaining to an entry in an admission control table.
<b>max-regs</b>	Configures the maximum number of subscriber registrations pertaining to an entry in an admission control table.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.

# max-regs

To configure the maximum number of subscriber registrations of an entry in an admission control table, use the **max-regs** command in CAC table configuration mode. To delete the maximum number of subscriber registrations in the given entry in the admission control table, use the **no** form of this command.

```
max-regs mr
```

```
no max-regs mr
```

<b>Syntax Description</b>	<i>mrr</i>	Positive integer specifying the maximum number of subscriber registrations to permit at the relevant scope.
---------------------------	------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC table configuration (config-sbc-sbe-cacpolicy-cactable)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the maximum number of subscriber registrations for an entry in the new admission control table MyCacTable:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-regs 500
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
	<b>max-call-rate-per-scope</b>	Configures the maximum call rate for an entry in an admission control table.

<b>Command</b>	<b>Description</b>
<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.
<b>max-connections</b>	Configures the maximum number of SIP connections that will be made to each remote address.
<b>max-num-calls</b>	Configures the maximum number of calls of an entry in an admission control table.
<b>max-regs-rate-per-scope</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.



# max-responses

To configure the maximum number of ENUM records returned to the routing module, use the **max-response** command in ENUM configuration mode. To return the number of records returned to the default value, use the no form of this command.

**max-responses** *number*

**no max-responses** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of ENUM records. The range is 0 to 2147483647.
---------------------------	---------------	---

This command has no arguments or keywords.

<b>Command Default</b>	The default is zero (0).
------------------------	--------------------------

<b>Command Modes</b>	ENUM configuration (config-sbc-sbe-enum)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the maximum number of ENUM records returned to the routing module:
-----------------	---

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# max-responses 100
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).

<b>Command</b>	<b>Description</b>
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

# max-updates

To configure the maximum call updates for an entry in an admission control table, use the **max-updates** command in CAC table configuration mode. To delete the maximum call updates in the given entry in the admission control table, use the **no** form of this command.

**max-updates** *mu*

**no max-updates** *mu*

<b>Syntax Description</b>	<i>mu</i>	Positive integer specifying the maximum number of updates to call media to permit at the relevant scope.
---------------------------	-----------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	CAC table configuration (config-sbc-sbe-cacpolicy-cactable)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the maximum number of call updates for an entry in the new admission control table MyCacTable:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-updates 500
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
	<b>max-call-rate-per-scope</b>	Configures the maximum call rate for an entry in an admission control table.

<b>Command</b>	<b>Description</b>
<b>max-channels</b>	Configures the maximum number of channels for an entry in an admission control table.
<b>max-connections</b>	Configures the maximum number of SIP connections that will be made to each remote address.
<b>max-num-calls</b>	Configures the maximum number of calls of an entry in an admission control table.
<b>max-regs</b>	Configures the maximum number of subscriber registrations of an entry in an admission control table.
<b>max-regs-rate-per-scope</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table.

# media

To enable the media bypass feature or the media down detect feature on a Border Access Controller (BAC) adjacency, use the **media** command in the H248 BAC adjacency configuration mode. To disable the media bypass feature or the media down detect feature on a BAC adjacency, use the **no** form of this command.

```
media {bypass | down}
```

```
no media {bypass | down}
```

Syntax Description	Command	Description
	<b>bypass</b>	Enables the media bypass feature on a BAC adjacency.
	<b>down</b>	Enables the media down detect feature on a BAC adjacency.

**Command Default** None

**Command Modes** H248 BAC adjacency configuration (config-h248-bac-adj)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to enable the media bypass feature on a BAC adjacency:

```
Router> enable
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access vrfex
Router(config-h248-bac-adj)# media bypass
```

## media-address

To add an IPv4 or IPv6 address to the set of addresses that can be used by the data border element (DBE) as a local media address, use the **media-address** command in either the SBC configuration mode or the SBC-DBE configuration mode. To remove an IPv4 or IPv6 address from the set of local media addresses, use the **no** form of this command.

```
media-address {ipv4 | ipv6} {addr} [nat-mode twice-nat | vrf vrf-name | managed-by {dbe | mgc}]
```

```
no media-address {ipv4 | ipv6} {addr} [nat-mode twice-nat | vrf vrf-name | managed-by {dbe | mgc}]
```

Syntax Description		
<i>A.B.C.D</i>	Local IP address on a Session Border Controller (SBC) interface, which can be used for media arriving on the DBE.	
<i>nat-mode twice-nat</i>	(Optional) Allows local addresses to be reserved for Twice-NAT pinholes.	
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies that the IP address is associated with a specific VPN routing and forwarding (VRF) instance. If the VRF is not specified, the address is assumed to be an address on the global VPN.	
<i>managed-by</i>	(Optional) Specifies whether the DBE or the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.	
<b>dbe</b>	(Optional) Specifies that only the DBE is allowed to select these addresses as local addresses for flows.	
<b>mgc</b>	(Optional) Specifies that only the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.	

**Command Default** No default behavior or values are available.

**Command Modes** SBC configuration (config-sbc) for unified SBC  
SBC-DBE configuration (config-sbc-dbe) for distributed SBC  
Voice service VoIP for TDM gateways and CUBE(config-voi-serv)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	This command was modified. The <i>nat-mode twice-nat</i> keyword was introduced.
	Cisco IOS XE Release 2.4	This command was modified for unified SBC.
	Cisco IOS XE Release 3.2S	This command was modified. The IPv6 support was added.
	Cisco IOS XE Release 3.9S	This command was modified to be supported under voice service VoIP configuration.

## Usage Guidelines

Use the **media-address** command to configure a local media address for the traffic arriving on the DBE for each IP address that you specified under the SBC virtual interface with the **ip address** command.

After you have configured a local media address, it cannot be modified while the DBE service is active. You must first deactivate the DBE with the **no activate** command.

Media address is a pool of IP addresses on the DBE for the media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All the vDBEs within the DBE draw media addresses from this pool.

## Examples

The following example for a unified SBC shows how the IP address 10.0.1.1, which is configured on an SBC interface, is used when media traffic arrives on the DBE from the global VPN:

```
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc)# media-address ipv4 10.0.1.1
Router(cfg-sbc-media-address)# end
```

The following example for a distributed SBC shows that the IPv4 address 10.0.1.1, which is configured on an SBC interface, is the local address used when media traffic arrives on the DBE, and is reserved for Twice-NAT pinholes:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv4 10.0.1.1 managed-by mgc nat-mode twice-nat
Router(config-sbc-dbe-media-address)# end
```

The following example for a distributed SBC shows that the IP address 10.0.1.1, which is an address configured on an SBC interface, is used when media traffic arrives on the DBE from the global VPN:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv4 10.0.1.1
Router(config-sbc-dbe-media-address)# end
```

The following example for a distributed SBC tries to delete the media address 1.1.1.1 before deactivating the DBE, and receives an error message:

```
Router(config-sbc-dbe)# no media-address ipv4 1.1.1.1
SBC: Unable to delete a media address whilst the DBE is active.
SBC: Please deactivate the DBE and try again.
```

The following example configures port ranges for a media-address range:

```
Router(config)# voice service voip
Router (conf-voi-serv)# media-address range 1.3.6.3 1.3.6.4
Router (conf-voi-serv)# port-range 32766 32766
```

## Related Commands

Command	Description
<b>media-address pool</b>	Creates a pool of sequential IPv4 and IPv6 media addresses that can be used by the DBE as local media addresses.
<b>ip address</b>	Configures the IPv4 address and the subnet mask on an SBC interface.
<b>sbc dbe</b>	Creates the DBE service on an SBC and enters into the SBC-DBE configuration mode.
<b>activate</b>	Initiates the DBE service of the SBC.





# media-address ipv4

To add an IPv4 H.248 Border Access Controller (BAC) address to the set of addresses that the BAC can use as local media address, use the **media-address ipv4** command in the H248 BAC configuration mode. To remove an IPv4 address from the set of local media addresses, use the **no** form of this command.

**media-address ipv4** *ipv4-address* **realm** *realm-number* **vrf** *vrf-name*

**no media-address ipv4** *ipv4-address* **realm** *realm-number* **vrf** *vrf-name*

## Syntax Description

<b>ipv4</b>	Configures an IPv4 H.248 BAC media address.
<i>ipv4-address</i>	IPv4 address assigned to an H.248 association.
<b>realm</b>	Configures the realm for an IPv4 H.248 BAC media address.
<i>realm-number</i>	Specifies the realm number.
<b>vrf</b>	Configures a VPN routing and forwarding (VRF) instance.
<i>vrf_name</i>	Name of the VRF for the H.248 adjacency.

## Command Default

None

## Command Modes

H248 BAC configuration (config-h248-bac)

## Command History

Release	Modification
Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

A realm group can contain multiple media addresses. When you configure a realm group under an adjacency, the IP address and port for the media stream of this adjacency is allocated from the media addresses in this realm group.

The **media-address ipv4** command includes the **port-range** *port-range* subcommand that configures the port range of the media address.

## Examples

The following example shows how the **media-address ipv4** command is used to configure an H.248 media address instance:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# media-address ipv4 192.168.0.2 realm 5 vrf cisco
Router(config-h248-bac-media-addr)# port-range 20000 30000
```

## Related Commands

Command	Description
<b>realm (H.248 BAC)</b>	Configures an IP realm of the BAC under an adjacency.



# media-address pool

To create a pool of sequential IPv4 or IPv6 media addresses that can be used by the data border element (DBE) as local media addresses, use the **media-address pool** command in the appropriate configuration mode. This pool of addresses is added to the set of local media addresses that can be used by the DBE. To remove this pool of IPv4 addresses from the set of local media addresses, use the **no** form of this command.

```
media-address pool {ipv4 | ipv6} {start-addr} {end-addr} [nat-mode twice-nat | vrf vrf-name | managed-by {dbe | mgc}]
```

```
no media-address pool {ipv4 | ipv6} {start-addr} {end-addr} [nat-mode twice-nat | vrf vrf-name | managed-by {dbe | mgc}]
```

## Syntax Description

<i>start-addr</i>	Starting the IPv4 or IPv6 media address in a range of addresses. An IPv4 or IPv6 media address is a local IP address on a Session Border Controller (SBC) interface that can be used when media traffic arrives on the DBE.
<i>end-addr</i>	Ending an IPv4 or IPv6 media address in a range of addresses. The ending IPv4 or IPv6 address must be numerically greater than the starting address.
<b>nat-mode twice-nat</b>	(Optional) Allows local addresses to be reserved for the Twice-NAT pinholes.
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies that the IP addresses are associated with a specific VPN routing and forwarding (VRF) instance. If the VRF instance is not specified, the address is assumed to be an address on the global VPN.
<b>managed-by</b>	(Optional) Specifies whether the DBE or the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.
<b>dbe</b>	(Optional) Specifies that only the DBE is allowed to select these addresses as local addresses for flows.
<b>mgc</b>	(Optional) Specifies that only the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.

## Command Default

If a pool of IPv4 or IPv6 media addresses is specified, but the optional parameters are not specified, the following default values are used:

- Addresses in the pool are members of the global VRF.
- Only the DBE is allowed to select these addresses as local addresses for flows.

## Command Modes

SBC configuration (config-sbc): for unified SBC

SBC-DBE configuration (config-sbc-dbe): for distributed SBC

Voice service VoIP(config-voi-serv): for TDM gateways and CUBE

**Command History**

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	This command was modified. The <b>nat-mode twice-nat</b> keyword was introduced.
Cisco IOS XE Release 2.4	This command was modified for unified SBC.
Cisco IOS XE Release 3.2S	This command was modified. The IPv6 support was added.
Cisco IOS XE Release 3.9S	This command was modified to be supported under the voice service VoIP configuration.

**Usage Guidelines**

Depending on whether you are running an unified SBC or a distributed SBC, use this command in the appropriate configuration mode.

The media address pool size is limited to 1024 IPv4 addresses. If more IPv4 addresses are required, we recommend that you create multiple SBC interfaces, and then configure the address pools from the subnets on those interfaces.

After you configure a local media address, it cannot be modified while the DBE service is active. Deactivate the DBE with the **no activate** command before modifying the media-address pool ipv4 specification.

A media address is a part of a pool of IP addresses on the DBE that are used for the media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All the virtual data border elements (vDBEs) within the DBE draw media addresses from this pool.

**Examples**

The following example for a unified SBC shows how to create a DBE service on an SBC called “global” and how to configure addresses from 10.0.2.1 to 10.0.2.10 in the global VRF:

```
Router(config)# sbc global
Router(config-sbc)# media-address pool ipv4 10.0.2.1 10.0.2.10
Router(cfg-sbc-media-address-pool)# end
```

The following example for a distributed SBC shows how to add IPv4 addresses from 10.0.2.1 to 10.0.2.10 to the media address pool as local addresses reserved for the Twice-NAT pinholes:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.1 10.0.2.10 nat-mode twice-nat
Router(config-sbc-dbe-media-address-pool)# end
```

The following example for a distributed SBC shows how to create a DBE service on an SBC called “mySbc,” and enters into the SBC-DBE configuration mode, and how to configure addresses from 10.0.2.1 to 10.0.2.10 in the global VRF:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.1 10.0.2.10
Router(config-sbc-dbe-media-address-pool)# end
```

The following example for a distributed SBC shows how to create a DBE service on an SBC called “mySbc,” and enters into the SBC-DBE configuration mode, and how to configure addresses from 10.0.2.20 to 10.0.2.25 in vpn3:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.20 10.0.2.25 vrf vpn3
Router(config-sbc-dbe-media-address-pool)# exit
```

The following example for a distributed SBC tries to delete the media address 10.0.2.1 before deactivating the DBE, and receives an error message:

```
Router(config-sbc-dbe)# no media-address ipv4 10.0.2.1
SBC: Unable to delete a media address whilst the DBE is active.
SBC: Please deactivate the DBE and try again.
```

### Related Commands

Command	Description
<b>activate</b>	Initiates the DBE service of the SBC.
<b>media-address</b>	Adds an IPv4 address to the set of addresses that can be used by the DBE as a local media address.

# media-gateway

To configure a media gateway, use the **media-gateway** command in SBE configuration mode. To remove a media gateway configuration, use the **no** form of this command.

**media-gateway ipv4** *A.B.C.D*

**no media-gateway ipv4** *A.B.C.D*

## Syntax Description

*ipv4 A.B.C.D* Specifies the IPv4 media gateway address.

## Command Default

*No default behavior or values are available.*

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to access media gateway mode from where you configure a media gateway.

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway ipv4 10.0.0.1
Router(config-sbc-sbe-mg)#
```

## Related Commands

Command	Description
<b>codecs</b>	Configures the codecs supported by the media gateway.
<b>show sbc sbe media-gateway-associations</b>	Displays a list of known media gateways with an active association.
<b>transcoder</b>	Configures the media gateway as a transcoder.

# media-gateway policy type

To configure a media gateway policy, use the **media-gateway policy type** command in the SBE configuration mode. To remove the policy, use the **no** form of this command.

```
media-gateway policy type {default | local | {remote {ipv4 | ipv6} ip-address [port
port-number]}}
```

```
no media-gateway policy type {default | local | {remote {ipv4 | ipv6} ip-address [port
port-number]}}
```

## Syntax Description

<b>default</b>	Specifies that the media gateway policy must be applied to all media gateways configured on the SBC. A default media gateway policy is applied on a media gateway (local or remote) when no other media policy is applied on the media gateway.
<b>local</b>	Specifies that the media gateway policy must be applied to the media gateway that is locally configured on the SBC.
<b>remote</b>	Specifies that the media gateway policy must be applied to a remote media gateway.
<b>ipv4</b>	Specifies that the remote media gateway has an IPv4 IP address.
<b>ipv6</b>	Specifies that the remote media gateway has an IPv6 IP address.
<i>ip-address</i>	IP address of the remote media gateway. The IP address can be in the IPv4 format or IPv6 format.
<b>port</b>	Specifies the port number of the remote media gateway.
<i>port-number</i>	Port number of the remote media gateway.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples**

In the following example, the **media-gateway policy type** command is used to configure a remote-type media gateway policy on the media gateway at 192.0.2.26:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway policy type remote ipv4 192.0.2.26 6886
```

**Related Commands**

Command	Description
<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
<b>media-gateway policy type</b>	Configures a media gateway policy.
<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
<b>media-policy</b>	Configures a media policy.
<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
<b>show sbc sbe media-policy</b>	Displays the details of media policies.
<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.



# media-late-to-early-iw

To configure late-to-early media interworking (iw), use the *media-late-to-early-iw* command in Adjacency SIP configuration mode. To deconfigure late-to-early media interworking (iw), use the **no** form of this command.

```
media-late-to-early-iw {incoming | outgoing}
```

```
no media-late-to-early-iw {incoming | outgoing}
```

## Syntax Description

<i>incoming</i>	Enable late-to-early media iw for calls from caller on this adjacency.
<i>outgoing</i>	Enable late-to-early media iw for calls to callee on this adjacency.

## Command Default

*No default behavior or values are available.*

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure late-to-early media iw for calls from caller on this adjacency.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# media-late-to-early-iw incoming
```

## Related Commands

Command	Description
<b>adjacency</b>	Configures an adjacency for an SBC service.

# media-line

To add a media description line to an entry in an SDP media profile, use the **media-line** command in SBC SBE SIP SDP media profile entry configuration mode. To delete a line, use the **no** form of this command.

```
media-line index "media-description"
```

```
no media-line index
```

## Syntax Description

<i>index</i>	Specifies the SDP line number in an SDP media profile. Must be an integer.
" <i>media-description</i> "	The <i>media_description</i> argument must be enclosed in quotes (" "). The value inside the quotes must be syntactically valid SDP as defined in RFC 2327. The following rules apply: <ul style="list-style-type: none"> <li>An SDP entry must contain exactly one m-line. The m-line must appear first in the entry. The m-line port must be zero. SBC replaces the zero with the appropriate port.</li> <li>An SDP entry must not contain a c-line.</li> </ul> <p>The Cisco command line interface handles the contents of <i>media_description</i> as a string value. It does not check the syntax of the configured information. If the syntax is incorrect, outbound offers by the SBC are rejected.</p>

## Command Default

No default behavior or values are available.

## Command Modes

SBC SBE SIP SDP media profile entry configuration (config-sbc-sbe-sip-sdp-media-ele)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Use the **media-line** command to add media description lines into an entry of an SDP media profile.

## Examples

The following example shows how to create lines in an SDP media profile entry :

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip sdp-media-profile Mediaprofile
Router(config-sbc-sbe-sip-sdp-media)# entry 1
Router(config-sbc-sbe-sip-sdp-media-ele)# media-line 1 "m=audio 0 RTP/AVP 31"
Router(config-sbc-sbe-sip-sdp-media-ele)# media-line 2 "a=aaa:testing"
```

```
Router(config-sbc-sbe-sip-sdp-media-ele)# Ctrl Z
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>entry</b>	Creates an entry in a table or SDP media profile.
<b>sdp-media-profile</b>	Creates or modifies a customized SDP media profile.
<b>show sbc sbe sip sdp-media-profile</b>	Shows all SDP media profiles in an SBC service or details for a specified profile.

# media-policy

To configure a media policy, use the **media-policy** command in the SBE configuration mode. To remove the media policy configuration, use the **no** form of this command.

**media-policy** *policy-name*

**no media-policy** *policy-name*

## Syntax Description

<i>policy-name</i>	Name of the media policy.  The <i>policy-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
--------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the **media-policy** command is used to create the my\_media\_policy media policy:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
```

Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# media-timeout (session border controller)

To set the maximum time a DBE waits after receiving the last media packet on a call and before cleaning up the call resources, use the **media-timeout** command in SBC-DBE configuration mode. To reset the **timeout** value to the default value of 30 seconds, use the **no** form of this command.

**media-timeout** *{timeout}* **first-packet**

no media-timeout timeout

## Syntax Description

timeout This is the timeout value in seconds.

## Command Default

The default is 30 seconds if **media-timeout** is not configured.

## Command Modes

SBC-DBE configuration (config-sbc-dbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	The <b>first-packet</b> keyword was added.

## Usage Guidelines

This command sets the maximum time the DBE waits after receiving the last media packet on a call before the DBE determines that the call has ceased and begins to clear up the call resources and to signal the signaling border element (SBE) to do the same. This command is used when the SBE is not able to clear up the calls itself. The normal method for clearing a call is for the SBE to explicitly signal the DBE.

You can halt detection of the media timeout event with the **first-packet** keyword of the **media-timeout** command. The **first-packet** keyword instructs the DBE to wait until it has received the first packet since the call has been established before starting the media timeout timer to start counting the number of seconds for which it has not seen an SBC packet. By the DBE waiting, SBC packets can continue to be forwarded because there is no media timeout yet. After waiting for the first packet and counting the configured number of seconds, then the DBE generates an alert to the SBE.

Use the **sbc dbe** command to enter into SBC-DBE configuration mode before using the **media-timeout** command.

## Examples

The following example configures the DBE to wait 10 seconds after receiving the last media packet and before cleaning up the call resources:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-timeout 10
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	dbe	Enters into SBC-DBE configuration mode.

# media address preserve

To ensure that media pinholes are preserved for deleted streams so that if a stream is re-enabled, the Cisco Unified Border Element (SP Edition) will re-use the same pinhole, use the **media address preserve** command in CAC table entry configuration mode. To preserve media addresses allocated during the initial call negotiation process, use the **init-negotiation** keyword. To allow a media pinhole for a deleted stream to be deleted, use the **no** form of this command.

**media address preserve**

**media address preserve init-negotiation**

**no media address preserve**

## Syntax Description

<b>init-negotiation</b>	Enable or disable Media Address Preservation during initial call negotiaiton.
-------------------------	---

## Command Default

If the **media address preserve** command is not configured or the **no media address preserve** command is used, the media pinhole for a deleted stream will be deleted.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.5.1	Enhancement for Media Address Preservation during initial negotiation introduced.

## Usage Guidelines

The **media address preserve** command configures the Support Renegotiated Call Over NAT feature. This feature is used to avoid de-allocation of a video pinhole in a Network Address Translation (NAT) scenario where Delta Renegotiation mode is in effect and a video transmission is paused. Although the standard Secure Device Provisioning (SDP) protocol when a video transmission is paused is to set the video stream to “a=inactive” (which indicates that SBC should keep the stream allocated), there are known devices that do not set the video stream to “a=inactive” to pause it. Instead, these devices delete the video stream by setting its port to 0. To ensure that the stream remains allocated and the pinhole is preserved even when the SBC receives a port value of 0 during a media stream renegotiation, you can enable the **media address preserve** command on a per-call basis. When the **media address preserve** command is enabled, stream statistics and SDP billing information will be output at call termination, not at Delta Renegotiation.

The **init-negotiation** keyword enables you to preserve media addresses allocated during the initial call negotiation process. This means that a media address/port allocated due to SDP in an initial offer remains allocated for the lifetime of the call.



**Examples**

The following example ensures that media pinholes are preserved for deleted streams so that if a stream is re-enabled, the Cisco Unified Border Element (SP Edition) will re-use the same pinhole. Note that the **media address preserve** command is applied on a per-call basis.

```
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table 1
Router(config-sbc-sbe-cacpolicy)# cac-table 1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media address preserve
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac complete
Router(config-sbc-sbe-cacpolicy)# complete
Router(config-sbc-sbe)# active cac-policy-set 1
```

**Related Commands**

Command	Description
<b>show sbc sbe cac-policy-set table entry</b>	Lists detailed information for a given entry in a CAC policy table, including whether the <b>media address preserve</b> command is enabled. When the <b>media address preserve</b> command is enabled, the “Media Address” field shows a value of “Preserve.”

# media bandwidth-fields ignore

To set the media flag to ignore the b-line and use CODEC to calculate the baseline bandwidth required for the media stream, use the **media bandwidth-fields ignore** command in the CAC table entry configuration mode. To return to the default state, use the **no** form of this command.

**media bandwidth-fields ignore**

**no media bandwidth-fields**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to set the AMB\_CAC\_MEDIA\_FLAG\_IGN\_EXPL\_BW media flag to ignore the b-line and use CODEC to calculate the baseline bandwidth required for the media stream:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table StandardListByAccount
Router(config-sbc-sbe-cacpolicy)# cac-table StandardListByAccount
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media bandwidth-fields ignore
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
```

Related Commands	Command	Description
	show sbc sbe	Displays detailed information for a given entry in a CAC policy table.
	cac-policy-set table entry	

# media bypass

To configure the Multiple SBC Media Bypass feature on a Session Initiation Protocol (SIP) adjacency, use the **media bypass** command in the adjacency SIP configuration mode. To disable the Multiple SBC Media Bypass feature, use the **no** form of this command.

```
media bypass { max-data-len data-length | tag sequence-number tag-name | auto-nat-tag-gen }
```

```
no media bypass { max-data-len | tag sequence-number | auto-nat-tag-gen }
```

## Syntax Description

<b>max-data-len</b>	Specifies the maximum length of the multiple SBC media bypass data that can be transmitted through the outbound signaling messages on an adjacency.
<i>data-length</i>	Maximum multiple SBC media bypass data length, in bytes. The range is from 100 to 2048. The default is 1000.
<b>tag</b>	Specifies the tag that can be used to control the groups to which the endpoints on an adjacency belong to in the Multiple SBC Media Bypass feature.
<i>sequence-number</i>	Sequence number of a media bypass tag in the tag list. The tag list is formed from the set of tags that are arranged according to their sequence number. The range is from 1 to 20.
<i>tag-name</i>	Name of a multiple SBC media bypass tag. The total length of all the tags in an adjacency cannot exceed 255 characters. A tag name can contain letters (alphabets), numerals, special characters, and all printable characters other than commas, semicolons, and spaces.
<b>auto-nat-tag-gen</b>	Configures the Common IP Address Media Bypass feature to generate a media bypass tag for registered endpoints that are behind a NAT device associated with this adjacency.  The default is that the SBC does not generate media bypass tags on the basis of the NAT device behind which the endpoints are located.

## Command Default

The SBC relays media for all the endpoints associated with the adjacency.

## Command Modes

Adjacency SIP configuration mode (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The <b>media-bypass</b> and <b>media-bypass forbid</b> commands were replaced with the <b>media bypass</b> command.
Cisco IOS XE Release 3.6S	This command was modified. The <b>auto-nat-tag-gen</b> keyword was added with the introduction of the Common IP Address Media Bypass feature.

**Usage Guidelines**

On any particular adjacency, you can configure both the **media bypass tag** *sequence-number tag-name* command and the **media bypass auto-nat-tag-gen** command.

To use the **media bypass** command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Note**

Media bypass is not supported for H.323 calls.

**Examples**

The following example shows how to use the **media bypass** command to configure the Multiple SBC Media Bypass feature and to set the maximum length of the multiple SBC media bypass data that can be transmitted on the outbound signaling messages on the adjacency to 150 bytes. The second **media bypass** command in this example is used to set TAG1 as the name of the tag that is used to control the groups that belong to the endpoints on the adjacency.

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# media bypass max-data-len 150
Router(config-sbc-sbe-adj-sip)# media bypass tag 1 TAG1
```

The following example shows how to use the **media bypass** command to configure the Multiple SBC Media Bypass feature and to specify that a media bypass tag must be automatically generated for each endpoint that is behind a NAT device on the adjacency.

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# media bypass auto-nat-tag-gen
```

**Related Commands**

Command	Description
adjacency	Configures an adjacency for the SBC service.

## media bypass type

To configure the Multiple SBC Media Bypass feature for a Call Admission Control (CAC) policy set, use the **media bypass type** command in the CAC table entry configuration mode. To deconfigure the Multiple SBC Media Bypass feature, use the **no** form of this command.

**media bypass type** [all | none | full [hairpin partial] | hairpin [full partial] | partial [full hairpin]]

**no media bypass type**

Syntax Description		
<b>all</b>		Enables all types of media bypass, such as partial, hairpin, and full, for a CAC table entry.
<b>none</b>		Disables all types of media bypass for a CAC table entry.
<b>full</b>		Enables media bypass on the SBC if adjacent and nonadjacent downstream and upstream hops have direct media connectivity, and common tags in the bypass tag list, or the same VPN.
<b>hairpin</b>		Enables media bypass for hairpin calls.
<b>partial</b>		Enables media bypass if the SBC is a member of a group of SBCs that share the same IP realm, and if even one SBC within that group is on the media path.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to configure the Multiple SBC Media Bypass feature to enable all types of media bypass:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table table1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media bypass type all
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>cac-table</b>	Configures the admission control tables.
<b>table-type</b>	Configures a CAC table type to enable the priority of the call to be used as a criterion in the CAC policy.

# media limits

To specify the media policy to be associated with the CAC policy table entry or applied on the media gateway, use the **media limits** command in the SBE CAC table CAC policy configuration mode or the SBE media gateway configuration mode. To remove this configuration, use the **no** form of this command.

**media limits** *policy-name*

**no media limits** *policy-name*

## Syntax Description

<i>policy-name</i>	The <i>policy-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

The configuration mode can be one of the following:

- SBE CAC table CAC policy configuration (config-sbc-sbe-cacpolicy-cactable-entry)
- SBE media gateway configuration (config-sbc-sbe-mg-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the **media limits** command is used to specify that the mp1 policy must be applied as entry 1 in the t1 CAC table.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table t1
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media limits mp1
```

In the following example, the **media limits** command is used to specify that the `audio_limit1` media policy must be applied on the remote media gateway at 192.0.2.82:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy audio_limit1
Router(config-sbc-sbe-media-pol)# type gateway
Router(config-sbc-sbe-media-pol)# transcode audio maximum 15000
Router(config-sbc-sbe-media-pol)# exit
Router(config-sbc-sbe)# media-gateway policy type remote ipv4 192.0.2.82 port 2000
Router(config-sbc-sbe-mg-pol)# media limits audio_limit1
```

#### Related Commands

Command	Description
<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
<b>media-gateway policy type</b>	Configures a media gateway policy.
<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
<b>media-policy</b>	Configures a media policy.
<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
<b>show sbc sbe media-policy</b>	Displays the details of media policies.
<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.



# media police

To configure how SBC handles media streams that exceed bandwidth limits for media calls, use the **media police** command in CAC table entry configuration mode. To return the policing conditions to the default value, use the no form of this command.

**media police strip | reject | degrade**

**no media police strip | reject | degrade**

Syntax Description	strip	reject	degrade
	Sets the following conditions: <ul style="list-style-type: none"> <li>If an individual media stream exceeds the bandwidth limit for a call, that media stream is disabled by setting the port to zero (0).</li> <li>If after the above stage has completed, the sum of the bandwidths of all remaining streams exceeds the bandwidth limit for a call, the request is rejected.</li> </ul>	Sets the following conditions: <p>If an individual media stream exceeds the bandwidth limit for a call, the request is rejected.</p> <p>If the sum of the bandwidths of all media streams exceeds the bandwidth limit for a call, the request is rejected.</p>	If a media stream exceeds the bandwidth limit for a call, the video stream is downgraded to a lower (non-zero) bandwidth that brings the media stream within the bandwidth limit for the call. <p><b>Note</b> Only the video stream is downgraded. Audio streams are not downgraded. If the audio stream exceeds the bandwidth for a call, the media stream cannot be downgraded.</p>

**Command Default** When media police is not configured, the default is to inherit the conditions from the interface, which in most cases is equivalent to the conditions for strip.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The degrade option is not supported on H.323 calls.

Using the degrade option may cause a 2 to 5 percent performance degradation.

**Examples**

The following example shows how to configure SBC to degrade media streams to lower bandwidths when requests exceed bandwidth limits.

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table cac-tbl-1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# media police degrade
Router(config-sbc-sbe-cacpolicy-cactable-entry)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>bandwidth</b>	Configures the maximum and minimum bandwidth limits for media calls.
<b>caller-bandwidth-field</b>	Configures SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the caller.
<b>callee-bandwidth-field</b>	Configures the SBC to convert a specific bandwidth line format into another bandwidth line format in an outbound Session Description Protocol (SDP) sent to the callee.
<b>max-bandwidth-per-scope</b>	Configures the maximum limit for the bandwidth in bps, Kbps, Mbps or Gbps for an entry in an admission control table.

# method-editor

To configure a method editor, use the **method-editor** command in the Adjacency SIP configuration mode. To remove a method editor, use the **no** form of this command.

**method-editor** {inbound | outbound} {editor-name | default}

**no method-editor** {inbound | outbound} {editor-name | default}

Syntax Description		
<b>inbound</b>	Sets the inbound SIP method editor.	
<b>outbound</b>	Sets the outbound SIP method editor.	
<i>editor-name</i>	Name of the method editor to be set for inbound or outbound signaling on the adjacency.	
	The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.	
	<b>Note</b> Except for the underscore character, do not use any special character to specify field names.	
<b>default</b>	Sets the method editor to the default settings.	

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how the **method-editor** command configures an inbound method editor named test1:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-sip)# method-editor inbound test1
```

Related Commands	Command	Description
	<b>sip method-editor</b>	Configures a method editor.



# method-profile

To configure a method profile in the mode of an SBE entity, use the **method-profile** command in Adjacency SIP configuration mode. To remove the method profile, use the **no** form of this command.

**method-profile** {inbound | outbound} *profile-name*

**no method-profile** {inbound | outbound}

Syntax Description	inbound   outbound	Sets the inbound and outbound SIP method profiles.
	<i>profile-name</i>	Specifies the name of the method profile. If you enter the <i>name</i> <b>default</b> , the default profile is configured. This profile is used for all adjacencies that do not have a specific profile configured.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **method-profile** command configures a method profile with the name of test1:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# method-profile test1
```

## method 3GPP-RF

To enable the 3GPP-RF billing method on the Cisco Session Border Controller (SBC), use the **method 3GPP-RF** command in the SBC SBE billing configuration mode. To disable the 3GPP-RF billing method, use the **no** form of this command.

**method 3GPP-RF**

**no method 3GPP-RF**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** SBC SBE billing configuration (config-sbc-sbe-billing)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to enable the 3GPP-RF billing method on the SBC:

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# method 3gpp-rf
```

# method (editor)

To add a method to an method editor, use the **method** command in the session initiation protocol (SIP) Method Editor configuration mode. To remove a method from an editor, use the **no** form of this command.

**method** *method-name*

**no method** *method-name*

<b>Syntax Description</b>	<i>method name</i>	Name of the method to be added to the method editor. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.
---------------------------	--------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SIP Method Editor configuration (config-sbc-sbe-mep-mth)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>method</b> command adds a method, test, to the Myeditor method editor:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-editor Myeditor
Router(config-sbc-sbe-mep-mth)# method test
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sip method-editor</b>	Configures a method editor.

# method packetcable-em

To enable the packet-cable billing method, use the `method packetcable-em` in the SBE billing configuration mode. To disable the packet-cable billing method, use the **no** form of this command.

**method packetcable-em**

**no method packetcable-em**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBE billing configuration (config-sbc-sbe-billing)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** *The following example shows how to enable the packet-cable billing method:*

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
(config-sbc-sbe)# billing
(config-sbc-sbe-billing)# method packetcable-em
```

Related Commands	Command	Description
	<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
	<b>billing</b>	Configures billing.
	ldr-check	Configures the time of day (local time) to run the Long Duration Check (LDR).
	<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.
	packetcable-em <i>transport radius</i>	Configures a packet-cable billing instance.
	show sbc sbe billing remote	Displays the local and billing configurations.





# method (session border controller)

To add a method with a specified name to a SIP message profile, use the **method** command in the SIP method-profile mode. To remove the method from the profile, use the **no** form of this command.

**method** *method-name*

**no method** *method-name*

<b>Syntax Description</b>	<i>method name</i>	Specifies the name of the method added to the method profile. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.
---------------------------	--------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SIP method-profile configuration (config-sbc-sbe-sip-mth)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>method</b> command adds a method test to the method profile Myprofile:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile Myprofile
Router(config-sbc-sbe-sip-mth)# method test
```

# method xml

To configure the Billing Manager such that it enables enabling the XML billing method, use the **method xml** command in the SBE billing configuration mode. To disable the XML billing method, use the **no** form of this command.

**method xml**

**no method xml**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** SBE billing configuration (config-sbc-sbe-billing)

Command History	Release	Modification
	3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

**Usage Guidelines** The XML method has been introduced to provision IP-centric logging information. Because the PacketCable billing method was too telephonic-specific, and uses the BAF format, the XML method has been introduced.

To enable the XML billing method on Billing Manager, you need to execute the **method xml** command from SBE billing configuration mode. To disable, the XML billing method, execute the **no method xml** command.



**Note** If XML billing instances are configured, the **no method xml** command cannot be successfully executed.

**Examples** The following example shows how to enable the XML billing method on the Billing Manager:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# method xml
```

Related Commands	Command	Description
	<b>xml (billing)</b>	Configures the method index for XML billing.
	<b>cdr path</b>	Indicates the path in which to store CDR billing records on the local machine.
	<b>ldr-check</b>	Configures the time at which long duration records are checked.

# minor-alert-size

To configure the number of specified events before a minor alert is triggered, use the **minor-alert-size** command in the blacklist reason mode. To disable the number of specified events, use the no form of this command.

**minor-alert-size** *number-of-events*

**no minor-alert-size**

## Syntax Description

<i>number-of-events</i>	The number of events for alert to be triggered. This can be of any value ranging from 1 to 65535.
-------------------------	---

## Command Default

No default behavior or values.

## Command Modes

Blacklist reason mode (config-sbc-sbe-blacklist-reason)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the number of specified events for a minor alert to be triggered using the **minor-alert-size** command in the blacklist reason mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist)# reason na-policy-rejection
Router(config-sbc-sbe-blacklist-reason)# minor-alert-size 20
```

## Related Commands

Command	Description
<b>critical-alert-size</b>	Configures the number of specified events before a critical alert is triggered.
<b>major-alert-size</b>	Configures the number of specified events before a major alert is triggered.
<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).

<b>Command</b>	<b>Description</b>
<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
snmp-server enable traps sbc blacklist	To enable SNMP SBC Blacklist traps.
<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.

## mode (session border controller)

To enter a mode for configuring the mode of a RADIUS Authentication server or RADIUS accounting server, use the **server mode** command in the server authentication mode. To exit the mode for configuring of RADIUS Authentication server mode, use the **no** form of this command.

**mode** {*local* |*remote*}

**no mode** {*local* |*remote*}

### Syntax Description

<i>server-name</i>	Specifies the name of the server.
<b>local</b>	Specifies local authentication.
<b>remote</b>	Specifies remote authentication.

### Command Default

No default behavior or values are available.

### Command Modes

Server authentication (config-sbc-sbe-auth-ser)

Server accounting (config-sbc-sbe-acc-ser)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how to configure server mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius authentication
Router(config-sbc-sbe-auth)# server panther
Router(config-sbc-sbe-auth-ser)# mode local
Router(config-sbc-sbe-auth-ser)#
```

# monitor event-trace sbc ha (EXEC)

To monitor and control the event trace function of the Session Border Controller (SBC), use the **monitor event-trace sbc ha** command in privileged EXEC mode.

```
monitor event-trace sbc ha {clear | continuous [cancel] | disable | dump [pretty] | enable |
one-shot }
```

Syntax Description	ha	Monitors and controls the event trace messages pertaining to the SBC high availability.
	<b>clear</b>	Clears the existing trace messages pertaining to the SBC.
	continuous	Continuously displays the latest event trace entries.
	cancel	(Optional) Cancels the continuous display of the latest trace entries.
	disable	Turns off event tracing for the SBC.
	dump	Writes the event trace results to the file that has been configured using the <b>monitor event-trace sbc ha</b> command in global configuration mode. The trace messages are saved in binary format.
	pretty	(Optional) Saves the event trace messages in ASCII format.
	enable	Turns on event tracing for the SBC.
	one-shot	Clears existing trace information, if any, from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the <b>monitor event-trace sbc ha</b> command in global configuration mode.

**Command Default** Event tracing in the SBC is not enabled.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced.
	Cisco IOS XE Release 2.3	The <b>sbc_ha</b> keyword was bifurcated into two keywords, <b>sbc</b> and <b>ha</b> .
	Cisco IOS XE Release 2.4	The event tracing default for the <b>monitor event-trace sbc ha</b> command was changed from Enabled to Disabled.
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **monitor event-trace sbc ha** command to control when and how and what kind of event trace data pertaining to the SBC on the Cisco ASR 1000 Series Aggregation Services Routers is collected. Use this command after you have configured the event trace functionality on the Cisco ASR 1000 Series Routers using the **monitor event-trace sbc ha** command in global configuration mode.



**Note** The amount of data collected from the trace depends on the trace message size that has been configured using the **monitor event-trace sbc ha** command in global configuration mode for each instance of a trace.

You can enable or disable SBC event tracing either by using the **monitor event-trace sbc ha** command in privileged EXEC mode or by using the **monitor event-trace sbc** command in global configuration mode. To disable event tracing, you should enter either of these commands with the **disable** keyword. To enable event tracing again, you should enter either of these commands with the **enable** keyword.

Use the **show monitor event-trace sbc ha** command to display trace messages. Use the **monitor event-trace sbc ha dump** command to save the trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace sbc ha dump pretty** command.

To configure the file in which you want to save trace information, use the **monitor event-trace sbc ha dump-file *dump-file-name*** command in global configuration mode. The trace messages are saved in binary format.

**Examples**

The following example shows the privileged EXEC commands that stop event tracing, clear the current contents of memory, and re-enable the trace function for the SBC high availability events. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace sbc ha disable
Router# monitor event-trace sbc ha clear
Router# monitor event-trace sbc ha enable
```

The following example shows how to configure the continuous display of the latest SBC high availability trace entries:

```
Router# monitor event-trace sbc ha continuous
```

The following example shows how to stop the continuous display of the latest trace entries:

```
Router# monitor event-trace sbc ha continuous cancel
```

**Related Commands**

Command	Description
<b>monitor event-trace (EXEC)</b>	Controls the event trace function for the specified Cisco IOS software subsystem component.
<b>monitor event-trace sbc ha (global)</b>	Configures event tracing for the SBC.
<b>show monitor event-trace ha</b>	Displays the event trace messages pertaining to the Cisco IOS software subsystem components.



## monitor event-trace sbc ha (global)

To configure event tracing for the Session Border Controller (SBC), use the **monitor event-trace sbc ha** command in the global configuration mode. To remove event tracing configuration from the SBC, use the **no** form of this command.

```
monitor event-trace sbc ha { disable | dump-file dump-file-name | enable | size number | stacktrace [depth] }
```

```
no monitor event-trace sbc ha { dump-file dump-file-name | size number | stacktrace [depth] }
```

### Syntax Description

<b>ha</b>	Configures event tracing for SBC high availability.
<b>disable</b>	Turns off event tracing for SBC high availability.
<b>dump-file</b> <i>dump-file-name</i>	Specifies the file in which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters. The path can point to the flash memory on the networking device or to a TFTP or FTP server.
<b>enable</b>	Turns on event tracing for the SBC high availability events, if event tracing has been disabled with the <b>monitor event-trace sbc ha disable</b> command.
<b>size</b> <i>number</i>	Sets the number of messages that can be written to memory for a single instance of a trace. Valid values are from 1 to 1000000.  <b>Note</b> Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the <b>show monitor event-trace sbc ha parameters</b> command.  When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
<b>stacktrace</b>	Enables stack trace at tracepoints.  <b>Note</b> Clear the trace buffer with the <b>monitor event-trace sbc ha clear</b> privileged EXEC command before entering the command.
<i>depth</i>	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.

### Command Default

Event tracing for the SBC is not enabled.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.3	The <b>sbc_ha</b> keyword was bifurcated into two keywords, <b>sbc</b> and <b>ha</b> .
Cisco IOS XE Release 2.4	The event tracing default for the <b>monitor event-trace sbc ha</b> command was changed from Enabled to Disabled.
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

Use the **monitor event-trace sbc ha** command to enable or disable event tracing and to configure event trace parameters for the SBC.

The Cisco IOS XE software allows the SBC to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value either by using the **monitor event-trace sbc ha** command in the privileged EXEC mode or by using the **monitor event-trace sbc ha** command in the global configuration mode.

Additionally, default settings do not appear in the configuration file. If the SBC enables event tracing by default, the **monitor event-trace sbc ha enable** command does not appear in the configuration file of the networking device. However, disabling event tracing that has been enabled by default by the subsystem creates a command entry in the configuration file.



**Note**

The amount of data collected from the trace depends on the trace message size that has been configured using the **monitor event-trace sbc ha size** command for each instance of a trace. Some Cisco IOS software subsystem components set the size by default. To display the size parameters, use the **show monitor event-trace sbc ha parameters** command.

To determine whether event tracing is enabled by default for the SBC, use the **show monitor event-trace sbc ha** command to display the trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer with the **monitor event-trace sbc ha clear** privileged EXEC command.

**Examples**

The following example shows how to enable event tracing for the SBC subsystem component in the Cisco IOS XE software, and to configure the size to 10,000 messages. The trace messages file is set to sbc-ha-dump in flash memory.

```
Router(config)# monitor event-trace sbc ha enable
Router(config)# monitor event-trace sbc ha dump-file bootflash:sbc-ha-dump
Router(config)# monitor event-trace sbc ha size 10000
```

**Related Commands**

Command	Description
<b>monitor event-trace (global)</b>	Configures event tracing for a specified Cisco IOS software subsystem component.
<b>monitor event-trace sbc ha (EXEC)</b>	Monitors and controls the event trace function pertaining to the SBC.
<b>show monitor event-trace sbc ha</b>	Displays event trace messages pertaining to the SBC.

# na-carrier-id-table

To enter the configuration mode of a number analysis table within the context of an SBE policy set, use the **na-carrier-id-table** command in the SBE call policy set mode. To remove the number analysis table, use the **no** form of this command.

*na-carrier-id-table table-name*

*no na-carrier-id-table table-name*

<b>Syntax Description</b>	<p><i>table-name</i></p> <p>Name of the number analysis table you are creating, or name of an existing table you are configuring.</p> <p>The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	---

**Command Default** No default behavior or values are available.

**Command Modes** SBE routing policy (config-sbc-sbe-rtgpolicy)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The na-dst-number-attr-table was renamed as na-carrier-id-table.

**Usage Guidelines**

The entries in this table are matched with the carrier ID. If necessary, a new number analysis table is created. Do not change the configuration of the tables in the context of the active policy set.

A number analysis table should not be removed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** *The following command shows how to enter the configuration mode of the na-table number analysis table within the context of an SBE policy set:*

```
Router# configure terminal
Router# mySbc sbe
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-carrier-id-table na-table
Router(config-sbc-sbe-rtgpolicy-natable)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

# na-dst-address-table

To enter the configuration mode of a number analysis table within the context of an SBE policy set, use the **na-dst-address-table** command in the SBE call policy set mode. To remove the number analysis table, use the **no** form of this command.

**na-dst-address-table** *table-name*

**no na-dst-address-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the number analysis table you are creating, or name of an existing table you are configuring.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE call policy set (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The na-dst-number-table was renamed as na-dst-address-table.

## Usage Guidelines

The entries in this table are matched with the complete dialed number. If necessary, a new number analysis table is created. Do not change the configuration of the tables in the context of the active policy set.

A number analysis table should not be removed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

*The following command shows how to create the MyNaTable number analysis table with the table entries matching the complete dialed number:*

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
(config-sbc-sbe)# call-policy-set 1
(config-sbc-sbe-rtgpolicy)# na-dst-address-table MyNaTable
(config-sbc-sbe-rtgpolicy-natable)# exit
```

```
(config-sbc-sbe-rtgpolicy)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	no call-policy-set default	Deconfigures the active routing policy set.
	<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

# na-dst-prefix-table

To enter the mode in which to configure a number analysis table, with numbers that match the prefix of the dialed number within an SBE policy set, use the **na-dst-prefix-table** command in SBE call policy set mode. Use the **no** form of this command to destroy the number analysis table.

**na-dst-prefix-table** *table-name*

**no na-dst-prefix-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the number analysis table you are creating or of an existing table you are configuring.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example illustrates the use of the **na-dst-prefix-table** command to create a number analysis table called *MyNaTable*.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-dst-prefix-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)#
```

## Related Commands



<b>Command</b>	<b>Description</b>
<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

# na-src-account-table

To enter the mode for configuring a number analysis table within an SBE policy set, with entries that match the source account, use the **na-src-account-table** command in the SBE call policy set mode. Use the **no** form of this command to destroy the table.

**na-src-account-table** *table-name*

**no na-src-account-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the number analysis table within an SBE policy set, with entries matching the source account.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.40.00	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following commands enter the mode for the NA table *MyNaTable*, or if it does not already exist, it creates it.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-account-table MyNaTable
```

## Related Commands

Command	Description
<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.

<b>Command</b>	<b>Description</b>
<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

# na-src-address-table

To enter the configuration mode of a source number analysis table within the context of an SBE policy set, use the **na-src-address-table** command in the SBE call policy set mode. To remove the number analysis table, use the **no** form of this command.

**na-src-address-table** *table-name*

**no na-src-address-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the number analysis table you are creating, or name of an existing table you are configuring.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE call policy set (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	This command was modified. The na-src-number-table was renamed as na-src-address-table.

## Usage Guidelines

The entries in this table are matched with the complete number from which the call originated. If necessary, a new number analysis table is created. Do not change the configuration of the tables in the context of the active policy set.

A number analysis table should not be removed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following command shows how to enter the configuration mode of the na-table number analysis table within the context of an SBE policy set:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-address-table MySrcNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# exit
```

```
Router(config-sbc-sbe-rtgpolicy)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	no call-policy-set default	Deconfigures the active routing policy set.
	<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

# na-src-adjacency-table

To enter the mode of configuration of a number analysis table within the context of an SBE policy set, use the *na-src-adjacency-table* command in SBE routing policy mode. The **no** form of this command destroys the number analysis table.

*na-src-adjacency-table table-name*

*no na-src-adjacency-table table-name*

## Syntax Description

<i>table-name</i>	Name of the number analysis table within an SBE policy set, with entries matching the source account.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The entries of this table match against the source adjacency. If necessary, a new number analysis table is created. You may not change the configuration of tables in the context of the active policy set. A number analysis table may not be destroyed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following commands enter the mode for the NA table *MyNaTable* with entries matching against the whole dialed number:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-adjacency-table MyNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.

## na-src-name-anonymous-table

To enter the configuration mode of a number analysis table, to determine whether the display name or presentation number is anonymous, use the **na-src-name-anonymous-table** command in the SBE routing policy configuration mode. Use the **no** form of this command to remove the number analysis table.

*na-src-name-anonymous-table table-name*

*no na-src-name-anonymous-table table-name*

### Syntax Description

*table-name*

Name of the number analysis table you are creating or of an existing table you are configuring.

The *table-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

**Note** Except for the underscore character, do not use any special character to specify field names.

### Command Default

No default behavior or values are available.

### Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

### Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers

### Usage Guidelines

The entries of this table match against the carrier ID. If necessary, a new number analysis table is created. You may not change the configuration of tables in the context of the active policy set.

A number analysis table may not be destroyed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following command enters the mode of configuration of a number analysis table na-table within the context of an SBE policy set.

```
Router# configure terminal
Router# mySbc sbe
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-name-anonymous-table NameTable
Router(config-sbc-sbe-rtgpolicy-natable)#
```



Related Commands	Command	Description
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.
	<b>match-anonymous</b>	Matches the display name or presentation number to Anonymous in the <b>na-src-name-anonymous-table</b> number analysis table.

# na-src-prefix-table

To enter the mode in which to configure a number analysis table, with numbers that match the prefix of the source number within an SBE policy set, use the **na-src-prefix-table** command in SBE call policy set mode. Use the **no** form of this command to destroy the number analysis table.

**na-src-prefix-table** *table-name*

**no na-src-prefix-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the number analysis table you are creating or of an existing table you are configuring.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example illustrates the use of the **na-src-prefix-table** command to create a number analysis table called *MySrcPrefixNaTable*.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# na-src-prefix-table MySrcPrefixNaTable
Router(config-sbc-sbe-rtgpolicy-natable)# entry 1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# action accept
Router(config-sbc-sbe-rtgpolicy-natable-entry)# category CAT-1
Router(config-sbc-sbe-rtgpolicy-natable-entry)# match-prefix 159
Router(config-sbc-sbe-rtgpolicy-natable-entry)# exit
Router(config-sbc-sbe-rtgpolicy-natable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>entry</b>	Enters the mode for configuring an entry in a number analysis table, creating the table, if necessary.
	<b>edit-cic</b>	Manipulates a carrier identification code in number analysis and routing tables.

## nat (session border controller)

To configure a SIP adjacency to assume that all endpoints are behind a NAT device, use the **nat** command in the SIP adjacency mode. To deconfigure this feature on the SIP adjacency, use the **no** form of this command.

**nat {force-on | force-off}**

**no nat {force-on | force-off}**

### Syntax Description

<b>force-on</b>	Sets the SIP adjacency to assume that all endpoints are behind a NAT device.
<b>force-off</b>	Sets the SIP adjacency to assume that the endpoints are not behind a NAT device.

### Command Default

The SBC autodetects whether all the endpoints are behind a NAT device.

### Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how the **nat force-on** command is used to configure the SIP adjacency to assume that all endpoints are behind a NAT device:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# nat force-on
```

# nat force-on

To configure all the endpoints of an access adjacency for the H.248 Border Access Controller (BAC) to be behind a NAT device, use the **nat force-on** command in the H248 BAC access adjacency configuration mode. To configure all the endpoints of an access adjacency for the H.248 BAC not to be behind a NAT device, use the **no** form of this command.

**nat force-on**

**no nat force-on**

**Syntax Description** This command has no arguments or keywords.

**Command Default** All the endpoints of an H.248 BAC access adjacency are not behind a NAT device.

**Command Modes** H248 BAC access adjacency. (config-h248-bac-adj)

Command History	Release	Modification
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **nat force-on** command is used to configure all the endpoints of an access adjacency for the H.248 BAC to be behind a NAT device:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access access1
Router(config-h248-bac-adj)# nat force-on
```

# network-id (session border controller)

To configure the network ID, use the **network-id** command in SBE configuration mode. To **deconfigure the network ID**, use the **no** form of this command.

**network-id** *id*

**no network-id**

<b>Syntax Description</b>	<i>id</i> Specifies the eight-digit network ID. Range is 0 to 99999.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to set the network ID to 88888:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# network-id 88888
```

# network

To configure either an IPv4 or IPv6 network on a redundant peer, use the **network** command in adjacency Session Initiation Protocol (SIP) peer configuration mode. To deconfigure a network, use the **no** form of this command.

**network** {IPv4 address netmask | IPv6 address netmask}

**no network** {IPv4 address netmask | IPv6 address netmask}

## Syntax Description

<i>address</i>	The IPv4 or IPv6 IP address.
<i>netmask</i>	The IPv4 or IPv6 netmask.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP peer configuration (config-sbc-sbe-adj-sip-peer)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

## Examples

The following example shows how the **network** command is used to configure an IPv4 network on a redundant peer on a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# redundant peer 1
Router(config-sbe-adj-sip-peer)# network IPv4 33.33.36.2 255.255.255.0
```

## Related Commands

Command	Description
<b>address</b>	Configures either an IP address or a host name to act as a redundant peer.
<b>port</b>	Configures a port for a redundant peer.
<b>priority</b>	Configures a redundant peer's priority.
<b>redundant peer</b>	Configures an alternative signaling peer for an adjacency.

# option-editor

To set an adjacency to use a specified editor for the whitelisting or blacklisting options, use the **option-editor** command. To remove the option editor, use the **no** form of this command.

**option-editor** [*ua* | *proxy*] [*inbound* | *outbound*] [*editor-name* | *default*]

**no option-editor** [*ua* | *proxy*] [*inbound* | *outbound*] [*editor-name* | *default*]

## Syntax Description

<b>ua</b>	Sets the SIP user agent (UA) option editors.
<b>proxy</b>	Sets the SIP proxy option editors.
<b>inbound</b>	Sets the inbound SIP option editors.
<b>outbound</b>	Sets the outbound SIP option editors.
<b>editor-name</b>	Specifies the name of the editor to use.  The editor-name can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
<b>default</b>	Sets the option editor to the default settings.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

UA editors are applied to the Supported and Require headers. Proxy editors are applied to the Proxy-Require headers.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to set the adjacency to use the specified editor for the whitelisting or blacklisting options:

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# option-editor ua inbound OP1
```



**Related Commands**

<b>Command</b>	<b>Description</b>
sip option-editor	Configures an option editor.

# option-profile

To set the adjacency to use the specified profile for white/blacklisting options, use the **option-profile** command. Use the **no** form of the command to select the default global configuration.

**option-profile** [**ua** | **proxy**] [**inbound** | **outbound**] [*prof-name* | **default**]

**no option-profile** [**ua** | **proxy**] [**inbound** | **outbound**] [*prof-name* | **default**]

## Syntax Description

<b>ua</b>	Sets the SIP ua header profiles.
<b>proxy</b>	Sets the SIP proxy header profiles.
<b>inbound</b>	Sets the inbound SIP header profiles.
<b>outbound</b>	Sets the outbound SIP header profiles.
<b>prof-name</b>	Specifies the name of profile to use.  The <i>prof-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

## Command Default

The global default is used.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

User agent (UA) profiles are applied to Supported and Require headers. Proxy profiles are applied to Proxy-Require headers.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to set the adjacency to use the specified profile for white/blacklisting options:

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)#

Router(config)# sbc test sbe adjacency sip Adj1
Router(config-sbc-sbe-adj-sip)# option-profile ua inbound OP1
Router(config-sbc-sbe-adj-sip)# exit
```



# options

To configure the codec that will support voice inband DTMF, use the **options** command in codec definition mode. Use the **no** form of this command to remove an existing option from this codec.

**options** {none | transrate | transcode | inband-dtmf}

**no options** {none | transrate | transcode | inband-dtmf}

## Syntax Description

options	Name of option. The values for the options are: <ul style="list-style-type: none"> <li>• none</li> <li>• transrate</li> <li>• transcode</li> <li>• inband-dtmf</li> </ul>
---------	---

## Command Default

The global default is used.

## Command Modes

Codec definition (config-sbc-sbe-codec-def)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command:

## Examples

The following example shows how to add an option to the codec.

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec system GSM id 3
Router(config-sbc-sbe-codec-def)# inband-dtmf
```

## option (editor)

To add an option to an editor, use the **option** command in the Session Initiation Protocol (SIP) Option Editor configuration mode. To remove an option, use the **no** form of this command.

**option** *opt-name*

**no option** *opt-name*

Syntax Description	opt-name	Name of the option.
--------------------	----------	---------------------

Command Default	No default behavior or values are available.
-----------------	--

Command Modes	SIP Option Editor configuration (config-sbc-sbe-mep-opt)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
------------------	--

Examples	The following example shows how to add an option to an editor:
----------	--

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-editor optedi
Router(config-sbc-sbe-mep-opt)# option opt1
```

Related Commands	Command	Description
	<b>sip option-editor</b>	Configures an option editor.

# option (session border controller)

To add an option to a profile, use the **option** command in SIP option mode. Use the **no** form of this command to remove an existing option from this profile.

**option** *opt-name*

**no option** *opt-name*

## Syntax Description

*opt-name*

Name of profile to use.

The *opt-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

**Note** Except for the underscore character, do not use any special character to specify field names.

## Command Default

The global default is used.

## Command Modes

SIP option (sip-opt)

## Command History

### Release

### Modification

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command:

## Examples

The following example shows how to add an option to the profile.

```
Router# configure terminal
Router(config)# sbc sanity
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-profile optpr1
Router(config-sbc-sbe-sip-opt)# option opt1
```

# origin-host

To configure the domain name of an IMS local host, use the **origin-host** command in Diameter configuration mode. To remove the origin host, use the no form of this command.

**origin-host** *host-name*

**no origin-host** *host-name*

<b>Syntax Description</b>	<i>host-name</i>	Specifies the name of the local host. The maximum length is 255 characters.
---------------------------	------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Diameter configuration (config-sbc-sbe-diameter)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The domain name of the local host (origin-host) is reported in the Diameter Origin-host AVP.

**Examples**

The following example shows how to configure the domain name of an IMS local host.

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# diameter
Router(config-sbc-sbe-diameter)# origin-host Host1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.
	<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
	<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
	<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.

<b>Command</b>	<b>Description</b>
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.



## origin-host (Rf interface)

To specify the domain name of an origin host for Rf support on the Session Border Element (SBE) of the Session Border Controller (SBC), use the **origin-host** command in the SBC SBE billing Rf configuration mode. To unconfigure the domain name of an origin host for Rf support on the SBE of the SBC, use the **no** form of this command.

**origin-host** *host-name*

**no origin-host** *host-name*

Syntax Description	<i>host-name</i>	Unique name (case sensitive) for an origin host. String length range: 1 to 30.
--------------------	------------------	--

Command Default	None
-----------------	------

Command Modes	SBC SBE billing Rf configuration (config-sbc-sbe-billing-rf)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to specify the domain name of an origin host for Rf support on the SBE of the SBC:

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# rf 0
Router(config-sbc-sbe-billing-rf)# origin-host mySBC
```

Related Commands	Command	Description
	<b>origin-realm (session border controller)</b>	Specifies the domain name of an origin realm for Rf support on the SBE of the SBC.
<b>rf</b>	Enables Rf support via billing configuration.	

# origin-realm

To configure the domain name of an IMS local realm, use the **origin-realm** command in Diameter configuration mode. To remove the origin realm, use the no form of this command.

**origin-realm** *realm-name*

**no origin-realm** *realm-name*

<b>Syntax Description</b>	<i>realm-name</i>	Specifies the domain name of the local realm. The maximum length is 63 characters.
---------------------------	-------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** Diameter configuration (config-sbc-sbe-diameter)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Diameter is a realm-based routing protocol, where multiple IMS peers can be configured. The domain name of the local realm (origin-realm) is reported in the Diameter Origin-Realm AVP.

**Examples** The following example shows how to configure the domain local name of an IMS realm.

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# diameter
Router(config-sbc-sbe-diameter)# origin-realm R1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.
	<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
	<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.

<b>Command</b>	<b>Description</b>
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# origin-realm (Rf interface)

To specify the domain name of an origin realm for Rf support on the Session Border Element of the Cisco Session Border Controller (SBC), use the **origin-realm** command in the SBC SBE billing Rf configuration mode. To unconfigure the domain name of an origin realm for Rf support on the SBE of the SBC, use the **no** form of this command.

**origin-realm** *realm-name*

**no origin-realm** *realm-name*

<b>Syntax Description</b>	<i>realm-name</i>	Unique name (case sensitive) of an origin realm. String length range: 1 to 30.
---------------------------	-------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	SBC SBE billing Rf configuration (config-sbc-sbe-billing-rf)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to specify the domain name of an origin realm for Rf support on the SBE of the SBC:

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# rf 0
Router(config-sbc-sbe-billing-rf)# origin-realm mySBC
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>origin-host (session border controller)</b>	Specifies the domain name of an origin host for Rf support on the SBE of the SBC.
	<b>rf</b>	Enables Rf support via billing configuration.

# outbound-flood-rate

To configure the maximum desired rate of outbound request signals on this adjacency (excluding ACK/PRACK requests) in signals per second, use the **outbound-flood-rate** command in adjacency SIP configuration mode. Use the **no** form of this command to disable flood protection.

**outbound-flood-rate** *rate*

**no** **outbound-flood-rate**

Syntax Description	rate	Desired rate of outbound request signals in signals per second.
--------------------	------	---

**Command Default** No flood protection.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the maximum desired rate of outbound request signals on this adjacency to 1,000 signals per second:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# outbound-flood-rate 1000
Router(config-sbc-sbe-adj-sip)#
```

## overload-time-threshold (session border controller)

To configure the threshold for media gateway (MG) overload control detection, use the **overload-time-threshold** command in SBC-DBE configuration mode. This threshold defines the maximum delay allowed by a SBC that has subscribed to overload control events for the DBE to add a new flow. If the threshold is exceeded, the DBE generates an overload event notification. To reset the threshold value to its default value of 100 milliseconds, use the **no** form of this command.

**overload-time-threshold** *time*

**no overload-time-threshold**

<b>Syntax Description</b>	<i>time</i> The time threshold in milliseconds. The possible values are 0 to 0-2000000000.
---------------------------	--

<b>Command Default</b>	If a time threshold value is not configured, the default value is 100 milliseconds.
------------------------	---

<b>Command Modes</b>	SBC-DBE configuration (config-sbc-dbe)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	If an SBC has subscribed for overload control events, the DBE outputs an overload event notification for every request to add a new flow whose execution takes longer than this threshold.
-------------------------	--

<b>Examples</b>	The following example configures the threshold for media gateway (MG) overload control detections with a value of 400 milliseconds:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# overload-time-threshold 400
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dbe</b>	Enters into DBE-SBE configuration mode.

# packetcable-em transport radius

To configure a packet-cable billing instance, use the **packetcable-em transport radius** command in the SBE billing configuration mode. To disable the packet-cable billing instance, use the **no** form of this command.

**packetcable-em** *method-index* **transport radius** *RADIUS-client-name*

**no packetcable-em** *method-index* **transport radius** *RADIUS-client-name*

## Syntax Description

<i>method-index</i>	Specifies the packetcable billing instance. The range is 0 to 7.
<i>RADIUS-client-name</i>	The RADIUS client name. The maximum size is 80 characters.

## Command Default

No default behavior or values are available.

## Command Modes

SBE billing configuration (config-sbc-sbe-billing)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

*The following example* configures packet-cable billing instances of four with a RADIUS client name of 'test':

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
(config-sbc-sbe)# billing
(config-sbc-sbe-billing)# packetcable-em 4 transport radius test
(config-sbc-sbe-billing-packetcable-em)#
```

## Related Commands

Command	Description
<b>activate (radius)</b>	Activates the billing functionality after configuration is committed.
<b>billing</b>	Configures billing.
<b>ldr-check</b>	Configures the time of day (local time) to run the Long Duration Check (LDR).
<b>local-address ipv4</b>	Configures the local IPv4 address that appears in the CDR.

<b>Command</b>	<b>Description</b>
<b>method packetcable-em</b>	Enable the packet-cable billing method.
<b>show sbc sbe billing remote</b>	Displays the local and billing configurations.



# parameter-editor

To add a parameter editor associated with a header, use the **parameter-editor** command in the SIP Header Editor element configuration mode. To remove a parameter editor, use the **no** form of this command.

**parameter-editor** *editor-name*

**no parameter-editor**

## Syntax Description

<i>editor-name</i>	Name of the parameter editor.  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
--------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SIP Header Editor element configuration (config-sbc-sbe-sip-hdr-ele)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

The parameter editor should be initially configured using the **sip parameter-editor** command in the SBE configuration mode.

## Examples

The following example shows how to add a parameter editor to the header element of a header editor:

```
Router# config
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-editor parmprof1
Router(config-sbc-sbe-mep-prm)# exit
Router(config-sbc-sbe)# sip header-editor headerprof1
Router(config-sbc-sbe-mep-hdr)# header To
Router(config-sbc-sbe-mep-hdr-ele)# parameter-editor parmprof1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip method-editor</b>	Configures a method editor.
<b>sip header-editor</b>	Configures a header editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>sip body-editor</b>	Configures a body editor.

# parameter-profile

To add a parameter profile associated with a header, use the **parameter-profile** command in SBE configuration mode. To remove the parameter profile, use the **no** form of this command.

**parameter-profile** *profile-name*

**no parameter-profile** *profile-name*

<b>Syntax Description</b>	<p><i>profile name</i> Name of the parameter profile.</p> <p>The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	---

**Command Default** No default behavior or values are available.

**Command Modes** SIP header configuration element (config-sbc-sbe-sip-hdr-ele)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to add a parameter profile to the header element for a header profile:

```
Router# config
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile headerprof1
Router(config-sbc-sbe-sip-hdr)# header To
Router(config-sbc-sbe-sip-hdr-ele)# parameter-profile parmprof1
```

Related Commands	Command	Description
	<b>sip method-profile</b>	Configures a method-profile.
	<b>sip header-profile</b>	Configures a header profile.



## parameter (editor)

To add a parameter to an editor, use the **parameter** command in the SIP Parameter Editor configuration mode. To remove a parameter from an editor, use the **no** form of this command.

**parameter** *parameter-name*

**no parameter** *parameter-name*

<b>Syntax Description</b>	<i>parameter-name</i>	Name of the parameter to be added to the parameter editor. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.
---------------------------	-----------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SIP Parameter Editor configuration (config-sbc-sbe-mep-prm)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
-------------------------	--

Use the **parameter** command to enter the SIP Parameter Editor Element configuration mode.

<b>Examples</b>	The following example shows how the <b>parameter</b> command adds a parameter named user to the parameter editor:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-editor paramedit
Router(config-sbc-sbe-mep-prm)# parameter user
Router(config-sbc-sbe-mep-prm-ele)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>action</b>	Configures the action to be taken in an editor.
	<b>parameter-editor</b>	Configures a parameter editor.

# parameter (session border controller)

To add a parameter with a specified name to a SIP message profile, use the **parameter** command in SBE SIP parameter-profile configuration mode. To remove the method from the profile, use the **no** form of this command.

**parameter** {*parameter name*}

**no parameter** {*parameter name*}

## Syntax Description

<i>parameter name</i>	Name of the parameter added to the parameter profile. Valid names are 1 to 32 characters in length (inclusive) and are case-sensitive.
-----------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SIP parameter-profile configuration

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.

## Examples

The following example shows how the **parameter** command adds a parameter named user to the parameter profile Myprofile:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-profile Myprofile
Router(config-sbc-sbe-sip-prm)# parameter user
Router(config-sbc-sbe-sip-prm-ele)# action add-not-present value phone
```

## Related Commands

Command	Description
<b>action</b>	Configures the action to take in a profile.
<b>parameter-profile</b>	Configures a parameter profile.

# pass-body

To permit SIP message bodies to pass through [for non-vital SIP methods accepted by a method profile] in the SIP method profile mode of an SBE entity, use the **pass-body** command in SIP method configuration mode. To remove the message bodies out of non-vital SIP messages accepted by the method profile, use the **no** form of this command.

**pass-body**

**no pass-body**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, the message bodies are removed out of non-vital SIP messages.

**Command Modes** SIP method (config-sbc-sbe-sip-mth)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **pass-body** command permits SIP message bodies to pass through for non-vital SIP methods accepted by method profile test1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile test1
Router(config-sbc-sbe-sip-mth)# pass-body
```

# payload-type asymmetric

To configure an SBC to support Asymmetric payload types, use the **payload-type asymmetric** command. Use the **no** form of this command to disallow an SBC from supporting Asymmetric payload types.

**payload-type asymmetric {allowed | disallowed}**

**no payload-type asymmetric {allowed | disallowed}**

## Syntax Description

<b>allowed</b>	Specifies that asymmetric payload types be allowed.
<b>disallowed</b>	Specifies that asymmetric payload types are not allowed.

## Command Default

*By default, Asymmetric payload types are allowed.*

## Command Modes

Configure CAC Policy CAC Table (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the SBC to specify support for asymmetric payload types on the mySBC SBC:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# cac-table TAB1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# payload-type asymmetric allowed
Router(config-sbc-sbe-cacpolicy-cactable-entry)# complete
Router(config-sbc-sbe)# cac-policy-set global 1
Router(config-sbc-sbe)# end
Router#
```



Following is a command output for the command **show sbc sbe cac-policy-set** command:

```
(config)#show sbc RAND sbe cac-policy-set 1 TAB1
```

```
SBC Service "RAND"

CAC Policy Set 1
  Active policy set: Yes
  Description:
  Averaging period: 60 sec
  First CAC table: TAB1
  First CAC scope: global

Table name: TAB1
  Description:
  Table type: policy-set
  Total call setup failures (due to non-media limits): 0

Entry 1
  CAC scope:
  CAC scope prefix length: 0
  Action: CAC complete
  Number of call setup failures (due to non-media limits): 0
  Max calls per scope:           Unlimited           Max call rate per scope:           Unlimited
  Max in-call message rate:      Unlimited           Max out-call message rate:         Unlimited
  Max reg. per scope:            Unlimited           Max reg. rate per scope:           Unlimited
  Max channels per scope:        Unlimited           Max updates per scope:             Unlimited
  Early media:                   Allowed           Early media direction:             Both
  Early media timeout:           None             Transcoder per scope:              Allowed
  Callee Bandwidth-Field:        AS-to-TIAS      Caller Bandwidth-Field:            None
  Asymmetric Payload Types: Allowed           Media bypass:                       Allowed
  Renegotiate Strategy:          Delta
  Max bandwidth per scope:        Unlimited
  SRTP Transport:                 Trusted-Only (by default)
  Caller hold setting:            Standard
  Callee hold setting:            Standard
  Caller privacy setting:         Never hide
  Callee privacy setting:         Never hide
  Caller voice QoS profile:       Default
  Callee voice QoS profile:       Default
  Caller video QoS profile:       Default
  Callee video QoS profile:       Default
  Caller sig QoS profile:         Default
  Callee sig QoS profile:         Default
  Caller inbound SDP policy:      None
  Callee inbound SDP policy:      None
  Caller outbound SDP policy:     None
  Callee outbound SDP policy:     None
  SDP Media profile               :           None
  Caller media disabled:          None
  Callee media disabled:          None
  Caller unsignaled secure media: Not Allowed
  Callee unsignaled secure media: Not Allowed
  Caller tel-event payload type:  Default
  Callee tel-event payload type:  Default
  Media flag:                      None

  Restrict codecs to list:         Default
  Restrict caller codecs to list:  Default
  Restrict callee codecs to list:  Default
  Caller media-type:               Inherit (default)
  Callee media-type:               Inherit (default)
  Maximum Call Duration:           Unlimited
```

# peer (session border controller)

To create an IMS peer and configure the name and IPv4 address of the peer, use the **peer** command in diameter configuration mode. To remove the peer, use the no form of this command.

```
peer peer-name [vpn vpn-name] [ipv4 ipv4-address | dns-name] [port port-number]
```

```
no peer peer-name [vpn vpn-name] [ipv4 ipv4-address | dns-name] [port port-number]
```

## Syntax Description

<i>peer-name</i>	Specifies the name of the peer.  The <i>peer-name</i> can have a maximum of 32 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
<b>ipv4</b> <i>ipv4-address</i>   <i>dns-name</i>	Assigns a standard IPv4 address to the peer, or a DNS FQDN.
<b>vpn</b> <i>vpn-name</i>	Name of the existing VPN to assign to the peer.
<b>port</b> <i>port-number</i>	Assigns a port number to the peer connect socket. The range is 1 to 65535. The default is 3868.

## Command Default

If port is not specified, the default port number of the peer is 3868.

## Command Modes

Diameter configuration (config-sbc-sbe-diameter)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

When you configure the peer with a VPN, only the IPv4 address can be configured with it. You cannot use the DNS name.

## Examples

The following example shows how to create an IMS peer:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# diameter
Router(config-sbc-sbe-diameter)# peer Peer1 ipv4 10.10.10.10
Router(config-sbc-sbe-diameter)#
```

Related Commands	Command	Description
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.
	<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
	<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
	<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
	<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
	<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
	<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
	<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
	<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
	<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
	<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# ping-bad-rsp-codes

To configure the congestion response codes on SIP Adjacency by sending SIP OPTIONS pings to it , use the **ping-bad-rsp-codes** command in adjacency ping option mode. Use the **no** form of this command to disable congestion response codes on SIP Adjacency.

**ping-bad-rsp-codes**

**no ping-bad-rsp-codes**

## Syntax Description

<b>range</b>	The response code range that SBC considers as ping failure indication. The default value range is from 300 to 399.
--------------	---

## Command Default

*range* = 300 to 399

## Command Modes

Ping option (config-sbc-sbe-adj-sip-ping)

## Command History

Release	Modification
Cisco IOS XE Release 3.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the congestion response codes on SIP adjacency by sending SIP OPTIONS pings:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# ping-enable
Router(config-sbc-sbe-adj-sip-ping)# ping-bad-rsp-codes ranges 300,398
Router(config-sbc-sbe-adj-sip-ping)# exit
Router(config-sbc-sbe-adj-sip)#
```

# ping-enable

To configure the adjacency to poll its remote peer by sending SIP OPTIONS pings to it and to enter the ping option mode, use the **ping-enable** command in adjacency SIP configuration mode. Use the **no** form of this command to disable polling the remote peer for the adjacency.

**ping-enable**

**no ping-enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Options pings are disabled by default.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the adjacency to poll its remote peer by sending SIP OPTIONS pings:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# ping-enable
Router(config-sbc-sbe-adj-sip-ping)# exit
Router(config-sbc-sbe-adj-sip)#
```

# ping-fail-count

To configure the number of consecutive pings that must fail before the adjacencies peer is deemed to be unavailable, use the **ping-fail-count** command in ping option mode. Use the **no** form of this command to set the fail count to default.

**ping-fail-count** *fail-count*

**no ping-fail-count**

## Syntax Description

<b>fail-count</b>	The number of consecutive failures before the peer is deemed to be unavailable. The possible values are 1 to 4294967295.  Note that this does not apply to the converse, that is, if an endpoint has been marked as unavailable, it only takes a single successful ping to mark it as available again.  This field may be changed while active, though this will not take effect until the next ping transaction completes, and will not retroactively cause a peer marked as unavailable to become available again without a subsequent successful ping response.
-------------------	--

## Command Default

*fail-count = 3*

## Command Modes

Ping option (config-sbc-sbe-adj-sip-ping)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the number of consecutive pings that must fail before the adjacencies peer is deemed to be unavailable:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# ping-enable
Router(config-sbc-sbe-adj-sip-ping)# ping-fail-count 10
Router(config-sbc-sbe-adj-sip-ping)#
```

# ping-interval

To configure the interval between SIP OPTIONS pings which are sent to the remote peer, use the **ping-interval** command in ping option mode. Use the **no** form of this command to set the interval to default.

**ping-interval** *interval*

**no ping-interval**

Syntax Description	interval	The number of seconds. The possible values are 1 to 2147483.
--------------------	----------	--

Command Default	32 seconds
-----------------	------------

Command Modes	Ping option (config-sbc-sbe-adj-sip-ping)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
------------------	--

Examples	The following example shows how to configure the interval between SIP OPTIONS pings that are sent to the remote peer to 100 seconds:
----------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# ping-enable
Router(config-sbc-sbe-adj-sip-ping)# ping-interval 100
Router(config-sbc-sbe-adj-sip-ping)#
```

# ping-lifetime

To configure the duration for which SBC waits for a response to an options ping for the adjacency, use the **ping-lifetime** command in ping option mode. Use the **no** form of this command to set the duration to default.

**ping-lifetime** *duration*

**no ping-lifetime**

## Syntax Description

<b>duration</b>	The number of seconds. The possible values are 1 to 2147483.
-----------------	--

## Command Default

32 seconds

## Command Modes

Ping option (config-sbc-sbe-adj-sip-ping)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

If no response is received in the duration time, then the ping is deemed to have failed.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the duration for which SBC waits for a response to an options ping for the adjacency to 100 seconds:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# ping-enable
Router(config-sbc-sbe-adj-sip-ping)# ping-lifetime 100
Router(config-sbc-sbe-adj-sip-ping)#
```



# ping-suppression

To configure SBC to send ping when required on sip Adjacency, use the **ping-suppression** command in ping option mode. Use the **no** form of this command to disable sending pings on SIP adjacency.

**ping-suppression**

**no ping-suppression**

<b>Syntax Description</b>	<p><b>options</b></p> <ul style="list-style-type: none"> <li>• <b>ood-request</b>—SBC considers a peer reachable when any out of dialog (or dialog creating) request is received, excluding OPTIONS and REGISTER messages.</li> <li>• <b>ood-response</b>—SBC considers a peer reachable when any out of dialog (or dialog creating) 2xx response is received, excluding OPTIONS and REGISTER messages.</li> <li>• <b>ind-request</b>—SBC considers a peer reachable when any in dialog request is received.</li> <li>• <b>ind-response</b>—SBC considers a peer reachable when any in dialog 2xx response is received.</li> </ul> <p>The default value is none.</p>
---------------------------	--

<b>Command Default</b>	<i>options = none</i>
------------------------	-----------------------

<b>Command Modes</b>	Ping option (config-sbc-sbe-adj-sip-ping)
----------------------	---

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 3.2</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 3.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 3.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure SBC to send ping when required on sip Adjacency by sending SIP OPTIONS pings:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# ping-enable
Router(config-sbc-sbe-adj-sip-ping)# ping-suppression odd-request
Router(config-sbc-sbe-adj-sip-ping)# exit
```

```
Router(config-sbc-sbe-adj-sip)#
```

# policy (session border controller)

To configure the packetization period policy, use the **policy** command in the codec list configuration mode. To deconfigure the packetization period policy, use the **no** form of this command.

```
policy {minimum | transrating}
```

```
no policy
```

Syntax Description	minimum	Specifies that the packetization period is the minimum.
	<b>transrating</b>	Specifies that the packetization period is transrating.

**Command Default** No default behavior or values are available.

**Command Modes** Codec list (sbc-codec-list)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure a minimum packetization period policy using the **policy** command in the codec list configuration mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec-list my_codecs
Router(config-sbc-sbe-codec-list)# policy minimum
```

Related Commands	Command	Description
	<b>codec list</b>	Creates a codec list.
	<b>codec</b>	Sets a minimum packetization period for a codec.
	<b>packetization-period</b>	

# port (session border controller)

To configure a port for a redundant peer, use the **port** command in adjacency Session Initiation Protocol (SIP) peer configuration mode. To deconfigure a port, use the **no port** form of this command.

**port** *port*

**no port** *port*

## Syntax Description

*port* The **port** of a redundant peer. The range is from **0** to **65535**.

## Command Default

Default port is 5060.

## Command Modes

Adjacency SIP peer configuration (config-sbc-sbe-adj-sip-peer)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

## Examples

The following example shows how the **port** command is used to configure a port for a redundant peer on a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# redundant peer 1
Router(config-sbe-adj-sip-peer)# port 2
```

## Related Commands

Command	Description
<b>address</b>	Configures either an IP address or a host name to act as the redundant peer.
<b>network</b>	Configures either an IPv4 or IPv6 network in a redundant peer.
<b>priority</b>	Configures a redundant peer's priority.
<b>redundant peer</b>	Configures an alternative signaling peer for an adjacency.

## port (SBE H.248)

To configure an SBE to use a given IPv4 H.248 port for H.248 communications when acting as a media gateway controller, use the port command in H.248 control address mode. To delete a given IPv4 H.248 port, use the **no** form of this command.

**port** *port-number*

**no port** *port-number*

<b>Syntax Description</b>	<i>port-number</i> Specifies the listening port number. The range is from 1 to 9999.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	H.248 control address (config-sbc-sbe-ctrl-h248)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure an SBE to use port 2000:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# control address h248 index 0
Router(config-sbc-sbe-ctrl-h248)# ipv4 1.1.1.1
Router(config-sbc-sbe-ctrl-h248)# port 2000
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>control address h248 index</b>	Selects index value and enters H.248 control address mode.
	<b>ipv4 (SBE H.248)</b>	Configures an SBE to use a given IPv4 H.248 control address.
	<b>transport (SBE H.248)</b>	Configures an SBE to use a certain transport for H.248 communications.

## port-range

To create a port range associated with corresponding media address pool entries, use the **port-range** command in media address configuration mode. To delete a port range, use the **no** form of this command.

**port-range** *start-rtp-port end-rtp-port*

**no port-range** *start-rtp-port end-rtp-port*

Syntax Description		
<i>start-rtp-port</i>	The starting port number of the range. The possible values are:	<ul style="list-style-type: none"> <li>• 16384 to 21644</li> <li>• 21845 to 32767.</li> </ul>
		The <i>start-rtp-port</i> value must be less than or equal to the <i>end-rtp-port</i> value.
<i>end-rtp-port</i>	The ending port number of the range. The possible values are:	<ul style="list-style-type: none"> <li>• 16384 to 21644</li> <li>• 21845 to 32767.</li> </ul>
		The <i>start-rtp-port</i> value must be less than or equal to the <i>end-rtp-port</i> value .

**Command Default** The default is no port range.

**Command Modes** Media address configuration (conf-media-addr-range)

Command History	Release	Modification
	Cisco IOS XE Release 3.9S	This command was introduced.

**Usage Guidelines** Use the **port-range** command in the media address configuration mode to specify up to 10 port ranges for a single media address.

**Examples** The following example for a unified SBC shows how to create two port ranges for a media address:

```
Router# configure terminal
Router(config)# voice service voip
Router(conf-voi-serv)# media-address 1.3.1.2 1.3.1.2
Router(conf-media-addr-range)# port-range 32766 32766
Router(conf-media-addr-range)# port-range 16384 16384
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>media-address</b>	Adds an IPv4 or IPv6 address to the set of addresses that can be used by the DBE as a local media address.
<b>media-address pool</b>	Creates a pool of IPv4 or IPv6 addresses that can be used by the DBE as local media addresses.

# precedence (session border controller)

To configure the precedence of the routing entry, use the *precedence* command in RTG routing table entry configuration mode. To deconfigure the precedence of the routing entry, use the **no** form of this command.

*precedence precedence*

**no** *precedence precedence*

<b>Syntax Description</b>	<i>precedence</i>	Range: [0-0xFFFFFFFF]. A value of 0 means the entry will never be matched. Zero is the default.
---------------------------	-------------------	---

<b>Command Default</b>	Zero is the default.
------------------------	----------------------

<b>Command Modes</b>	RTG routing table entry configuration (config-sbc-sbe-rtgpolicy-rtgtable-entry)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	<p>If more than one entry matches the current time, selection is based on precedence.</p> <p>To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.</p>
-------------------------	---

**Examples** The following example shows how to configure an SBE to use port 2000:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-category-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# precedence 0
Router(config-sbc-sbe-rtgpolicy-rtgtable)# end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>entry</b>	Creates or modifies an entry in a table.



# preferred-transport

To set the preferred transport protocol for SIP signaling on an adjacency, use the **preferred-transport** command in adjacency SIP configuration mode.

**preferred-transport {tcp | udp}**

**no preferred-transport**

Syntax Description		
	<i>tcp</i>	Sets the preferred transport to TCP.
	<i>udp</i>	Sets the preferred transport to UDP.

**Command Default** Adjacencies use UDP by default.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following command sets the preferred transport of the SipAdj1 adjacency to TCP:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipAdj1
Router(config-sbc-sbe-adj-sip)# preferred-transport tcp
Router(config-sbc-sbe-adj-sip)# exit
```

# prefix (session border controller)

To configure whether the match-address of this entry matches the start of the source or destination address, use the **prefix** command in the routing table configuration mode. To delete the table-type in the routing table, use the **no** form of this command.

**prefix**

**no prefix**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, the match-address is not be denoted as a prefix.

**Command Modes** Routing table entry (config-sbc-sbe-rtgpolicy-rtgtable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure an entry to match dialed numbers starting with 9:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-address 9
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# prefix
```

## priority (session border controller)

To configure the priority of the accounting or authentication server, use the **priority** command in the appropriate configuration mode. To disable any previously set priority, use the **no** form of this command.

**priority** *pri*

**no priority**

<b>Syntax Description</b>	<i>pri</i> Specifies the priority. Range is 1 to 10.
---------------------------	--

<b>Command Default</b>	By default, this command assumes that <i>pri</i> is 1.
------------------------	--

<b>Command Modes</b>	Server accounting (config-sbc-sbe-acc-ser) Server authentication (config-sbc-sbe-auth)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

The priority determines which of the configured servers is selected as the default server and where all requests are sent. A RADIUS client contacts the RADIUS servers sequentially, in order of priority, to establish an active RADIUS session. Each RADIUS client sends call detail records to the currently active RADIUS server.

<b>Examples</b>	The following example shows how to configure accounting servers acctsvr as priority 1 and acctsvr2 as priority 2 on mySbc for RADIUS client instance radius1:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting radius1
Router(config-sbc-sbe-acc)# server acctsvr
Router(config-sbc-sbe-acc-ser)# priority 1
Router(config-sbc-sbe-acc-ser)# exit
Router(config-sbc-sbe-acc)# server acctsvr2
Router(config-sbc-sbe-acc-ser)# priority 2
```

# privacy restrict outbound

To configure an H.323 adjacency to apply privacy restriction on outbound messages if the user requests it, use the **privacy restrict outbound** command in the adjacency H.323 configuration mode. To disallow privacy restriction on outbound messages sent out by the adjacency, use the **no** form of this command.

**privacy restrict outbound**

**no privacy restrict outbound**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **privacy restrict outbound** command is used to configure an H.323 adjacency to apply privacy restriction on outbound messages if a user requests it:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp422
Router(config-sbe-adj-h323)# privacy restrict outbound
```

Related Commands	Command	Description
	<b>allow private info</b>	Configures an H.323 adjacency to allow private information on messages sent out by the H.323 adjacency.

# privacy (session border controller)

To configure the trust level for determining whether the privacy service should be applied, use the **privacy** command in adjacency SIP configuration mode. To disable the trust level, use the **no** form of this command.

**privacy** [**inherit-profile** | **trusted** | **untrusted**]

**no privacy**

Syntax Description	inherit-profile	Specifies that the trust level for determining whether privacy services are required is derived from the adjacencies inherit-profile.
	<b>trusted</b>	Specifies that the adjacency is trusted and does not require privacy services to be applied.
	<b>untrusted</b>	Specifies that the adjacency is not trusted and requires privacy services to be applied.

**Command Default** By default, the trust level is set to **inherit-profile**.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the trust level of the SIP adjacency to trusted:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# privacy trusted
```

Related Commands	Command	Description
	<b>adjacency</b>	Configures an adjacency for an SBC.
	<b>inherit-profile</b>	Configures a global inherit profile for the SIP adjacency.



# profile (session border controller)

To apply a delegate registration profile to a delegate registration subscriber, use the **profile** command in subscriber-delegate configuration mode. To remove the delegate registration profile, use the **no profile** command.

**profile** {profile name}

**no profile** {profile name}

## Syntax Description

<i>profile name</i>	This is the name of the delegate client registration profile that can be applied to a delegate subscriber.  The profile name is a string field of 24 characters maximum length.
---------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

subscriber-delegate configuration mode (config-sbc-sbe-subscriber-delegate)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

apply the delegate registration profile, created previously with the **delegate-profile** command, to a delegate registration subscriber

After a delegate profile is configured, the following profile parameters may optionally be configured:

- duration
- retry-count
- retry-interval
- refresh-buffer

Delegate registration is done underneath the SBE configuration for globally unique subscribers.

## Examples

The following example configures a provisioned delegate registration profile that can be applied to a delegate registration subscriber and configures a delegate registration for delegate client (aor=sip:bob@isp.example). The delegate registration profile is configured with a duration expiration time of 1000 seconds, a retry count of 5 times, a retry interval of 60 seconds, and a refresh timeout time of 200 seconds:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# delegate-profile my-profile
Router(config-sbc-sbe-subscriber-delegate-prof)# duration 1000
```

```

Router(config-sbc-sbe-subscriber-delegate-prof)# retry-count 5
Router(config-sbc-sbe-subscriber-delegate-prof)# retry-interval 60
Router(config-sbc-sbe-subscriber-delegate-prof)# refresh-buffer 200
Router(config-sbc-sbe-subscriber-delegate-prof)# exit
Router(config-sbc-sbe)# subscriber sip:bob@isp.example
Router(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
Router(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
Router(config-sbc-sbe-subscriber-contact)# exit
Router(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
Router(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
Router(config-sbc-sbe-subscriber-delegate)# profile my-profile
Router(config-sbc-sbe-subscriber-delegate)# activate
Router(config-sbc-sbe-subscriber-delegate)# end

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>delegate-profile</b>	Configures a delegate registration profile that is applied to a delegate registration subscriber.
<b>sip-contact</b>	Configures the SIP contact information for a specified Uniform Resource Identifier (URI) for a delegate subscriber
<b>delegate-registration</b>	Configures a delegate registration for a delegate client.
<b>show sbc sbe sip subscribers</b>	Displays subscribers for whom Provisioned Delegate Registration has been provisioned.
<b>show sbc sbe sip delegate-profile</b>	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.



# qos fax

To **configure a fax QoS profile**, use the **qos fax** command in SBE configuration mode. To **destroy the given profile**, use the **no** form of this command.

**qos fax** *qos-name*

**no qos fax** *qos-name*

## Syntax Description

<i>qos-name</i>	Specifies the QoS profile. The string <b>default</b> is reserved. The <i>qos-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to enter the mode for configuring a fax QoS profile named residential:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos fax residential
Router(config-sbc-sbe-fax)# exit
```

# qos sig

To **configure a signaling QoS profile**, use the **qos sig** command in SBE configuration mode. To **destroy the given profile**, use the **no** form of this command.

**qos sig** *qos-name*

**no qos sig** *qos-name*

## Syntax Description

<i>qos-name</i>	Specifies the name of an existing QoS profile. The string <b>default</b> is reserved. The <i>qos-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how **qos sig** command enters the mode for configuring a signaling QoS profile residential:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos sig residential
Router(config-sbc-sbe-sig)# exit
```

# qos video

To **configure a video QoS profile**, use the **qos video** command in the SBE configuration mode. To **destroy the given profile**, use the **no** form of this command

```
qos video qos-name
```

```
no qos video qos-name
```

## Syntax Description

<i>qos-name</i>	Specifies the QoS profile. The string <b>default</b> is reserved.  The <i>qos-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to enter the mode for configuring a video QoS profile named residential:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos video residential
Router(config-sbc-sbe-video)# exit
```

# qos voice

To **configure a voice QoS profile**, use the **qos voice** command in SBE configuration mode. To **destroy the given profile**, use the **no** form of this command.

**qos voice** *qos-name*

**no qos voice** *qos-name*

## Syntax Description

<i>qos-name</i>	Specifies the QoS profile. The string <b>default</b> is reserved.  The <i>qos-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to enter the mode for configuring a voice QoS profile named residential:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# qos voice residential
Router(config-sbc-sbe-voice)# exit
```

# range (session border controller)

To map a range of response codes to a response code, use the **range** command in the session initiation protocol (SIP) method profile map configuration mode or the SIP method editor map configuration mode. To **remove the mapping**, use the **no** form of this command.

**range** *statuscoderange* **value** *statuscodevalue*

**no range** *statuscoderange*

## Syntax Description

<b>statuscoderange</b>	Range of response codes. These are specified by a three-digit number, where the first digit has the range 0 to 6, the second digit has the range 0 to 9/X, and the third digit has the range 0 to 9/X. X is a wild card.
<b>value</b>	Specifies the value of the range the response code is mapped to.
<b>statuscodevalue</b>	Range of the response code. This is mapped to the specified three-digit number, where the first digit has the range 0 to 6, the second digit has the range 0 to 9, and the third digit has the range 0 to 9.

## Command Default

No default behavior or values are available.

## Command Modes

SIP method profile map configuration (config-sbc-sbe-sip-mth-ele-map)  
SIP method editor map configuration (config-sbc-sbe-mep-mth-ele-map)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.3S	This command was modified. This command was added in the SIP method editor map configuration mode.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how the **method** command adds a method, test, to the Myprofile method profile:

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile mthdprof1
Router(config-sbc-sbe-sip-mth)# method INVITE
Router(config-sbc-sbe-sip-mth-ele)# map-status-code
Router(config-sbc-sbe-sip-mth-ele)# map-status-code
Router(config-sbc-sbe-sip-mth-ele-map)# range 5XX value 500
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>blacklist</b>	Configures SIP header or method blacklist profiles on a SIP message.
<b>description</b>	Configures descriptive text for a method profile.
<b>pass-body</b>	Permits SIP message bodies to pass through for nonvital SIP methods accepted by a method profile.

The following example shows how to specify the range for mapping the response codes received for a method:

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-editor MethodEditor1
Router(config-sbc-sbe-sip-mth)# method INVITE
Router(config-sbc-sbe-sip-mth-ele)# map-status-code
Router(config-sbc-sbe-sip-mth-ele-map)# range 5XX value 500
```

## ras retry (session border controller)

To configure an H.323 Registration, Admission, and Status (RAS) retry count for an RAS transaction type, use the **ras retry** command in the appropriate configuration mode. To return to the default value for the specified RAS transaction type, use the **no** form of this command.

```
ras retry {arq | brq | drq | grq | rrq | urq} value
```

```
no ras retry {arq | brq | drq | grq | rrq | urq} value
```

### Syntax Description

<b>arq</b>	Specifies an admission request (ARQ) transaction.
<b>brq</b>	Specifies a bandwidth request (BRQ) transaction.
<b>drq</b>	Specifies a disengage request (DRQ) transaction.
<b>grq</b>	Specifies a gatekeeper request (GRQ) transaction.
<b>rrq</b>	Specifies a registration request (RRQ) transaction.
<b>urq</b>	Specifies an unregistration request (URQ) transaction.
<i>value</i>	Specifies the retry count value. Valid values are 0 to 30.

### Command Default

The default values are 2 for all except URQ which is 1.

### Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
H.323 configuration (config-sbc-sbe-h323)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how the **ras retry** command configures an H.323 RAS retry count in Adjacency H.323 configuration mode:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# ras retry arq 5
```

The following example shows how the **ras retry** command configures an H.323 RAS retry count in H.323 configuration mode:

```
Router# configure
```

```
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# h323  
Router(config-sbc-sbe-h323)# ras retry arq 5
```

Related Commands	Command	Description
	<b>ras rrq</b>	Configures the registration request (RRQ).
	<b>ras timeout</b>	Configures an H.323 RAS timeout interval.



# ras rrq

To configure the registration request (RRQ), use the **ras rrq** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

```
ras rrq {keepalive | ttl} value
```

```
no ras rrq {keepalive | ttl} value
```

Syntax Description	keepalive	Specifies keepalive messages used to refresh an H.323 adjacency.
	ttl	Specifies time to live (TTL) for an RRQ request.
	value	Specifies the <b>keepalive</b> or <b>ttl</b> value. Valid values for <b>keepalive</b> are from 15000 to 150000 milliseconds. Valid values for <b>ttl</b> are from 16 to 300 seconds.
		The <b>ttl</b> value must be higher than the <b>keepalive</b> value.

**Command Default** *The default **keepalive** value is 45000 milliseconds.*  
*The default **ttl** value is 2 seconds.*

**Command Modes** Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
 H.323 configuration (config-sbc-sbe-h323)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **ras rrq** command configures H.323 RAS RRQ in adjacency H.323 configuration mode:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# ras rrq ttl 100
Router(config-sbc-sbe-adj-h323)# ras rrq keepalive 60
```

The following example shows how the **ras rrq** command configures RAS RRQ in H.323 configuration mode:

```
Router# configure
Router(config)# sbc mySbc
```

```
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# ras rrq ttl 100
Router(config-sbc-sbe-h323)# ras rrq keepalive 60
```

**Related Commands**

Command	Description
<b>ras retry</b>	Configures an H.323 RAS retry count for an RAS transaction type.
<b>ras timeout</b>	Configures an H.323 RAS timeout interval.

## ras timeout (session border controller)

To configure an H.323 RAS timeout interval, use the **ras timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

```
ras timeout {arq | brq | drq | grq | rrq | urq} value
```

```
no ras timeout {arq | brq | drq | grq | rrq | urq} value
```

### Syntax Description

<b>arq</b>	Specifies ARQ transaction.
<b>brq</b>	Specifies BRQ transaction.
<b>drq</b>	Specifies DRQ transaction.
<b>grq</b>	Specifies GRQ transaction.
<b>rrq</b>	Specifies RRQ transaction.
<b>urq</b>	Specifies URQ transaction.
<i>value</i>	Specifies timeout value (seconds). Valid values are from 1000 to 45000 milliseconds.

### Command Default

The default values vary depending on the transaction type.

### Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
H.323 configuration (config-sbc-sbe-h323)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

### Examples

The following example shows how the **ras timeout** command configures an H.323 RAS timeout interval in adjacency H.323 configuration mode.

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# ras timeout arq 1
```

The following example shows how the **ras timeout** command configures an H.323 RAS timeout interval in H.323 configuration mode.

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# h323
Router(config-sbc-sbe-h323)# ras timeout arq 1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ras retry</b>	Configures an RAS retry count for an RAS transaction type.
<b>ras rrq</b>	Configures the registration request (RRQ)

# realm

To configure an adjacency with the realm that it belongs to as part of configuring an IP Realm under an adjacency, use the **realm** command in adjacency SIP configuration mode. To remove the IP realm from the adjacency, use the **no realm** command.

```
realm {IP realm identifier}
```

```
no realm {IP realm identifier}
```

<b>Syntax Description</b>	<p><i>IP realm identifier</i></p> <p>The IP Realm Identifier is used to indicate to which packet network the media addresses belong. The IP Realm identifier is a string, which may be in a domain name format, for example, “mynet.net” or any other string format.</p> <p>The format of the realm string is up to the user with certain restrictions. Realms strings are case insensitive and are made up of the characters described in the table in the “IP Realm Support” chapter of the <i>Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model</i>.</p>
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the unified model on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	In the SBC unified model, use the <b>realm</b> command to tag the adjacencies with the realm that they belong to. This will enable subsequent calls to use media addresses from that realm.
-------------------------	---

<b>Examples</b>	The following example shows how to tag the SIP adjacency Cisco-gw with the realm cisco.com:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip Cisco-gw
Router(config-sbc-sbe-adj-sip)# realm cisco.com
```

The following example shows the running configuration after the SIP adjacency Cisco-gw is tagged with the realm cisco.com:

```
Router# show run
adjacency sip Cisco-gw
signaling-address ipv4 200.100.50.8
realm cisco.com
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>adjacency</b>	Configures an adjacency for a Session Border Controller (SBC) service.
	<b>media-address ipv4</b>	Configures an IPv4 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
	<b>media-address pool ipv4</b>	Configures a pool of sequential IPv4 media addresses that can be used by the data border element (DBE) as local media addresses.

# realm (diameter)

To configure a peer and assign the peer to a realm, use the **realm** command in diameter configuration mode. To remove the peer from the realm, use the no form of this command.

```
realm realm-name [app rx] peer peer-name [priority priority]
```

```
no realm realm-name [app rx] peer peer-name [priority priority]
```

Syntax Description	
<i>realm-name</i>	Name of the existing route realm in which to assign the peer. The maximum length is 63.
<b>app rx</b>	The type of application for this route entry. Currently only Rx is valid.
<b>peer</b> <i>peer-name</i>	Name of the existing peer.
<b>priority</b> <i>priority</i>	Specifies the priority of the peer. The range is 1 to 100. The default 1.

**Command Default** If priority is not specified, the default priority of the peer is 1.

**Command Modes** Diameter configuration (config-sbc-sbe-diameter)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure a peer and assign the peer to a realm:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# diameter
Router(config-sbc-sbe-diameter)# origin-realm Realm1
Router(config-sbc-sbe-diameter)# peer Peer1 ipv4 10.10.10.10
Router(config-sbc-sbe-diameter)# realm Realm1 app rx peer Peer1 priority 2
Router(config-sbc-sbe-diameter)#
```

Related Commands	Command	Description
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.

<b>Command</b>	<b>Description</b>
<b>origin-host</b>	Configures the domain name of an IMS local host.
<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.



## realm (H.248 BAC)

To configure an IP realm of the Border Access Controller (BAC) under an adjacency, use the **realm** command in the H248 BAC adjacency configuration mode. To unconfigure the IP realm from the adjacency, use the **no** form of this command.

**realm** *realm-number*

**no realm** *realm-number*

<b>Syntax Description</b>	<i>realm-number</i>	Number of the IP realm that belongs to the BAC. The range is from 1 to 100.
---------------------------	---------------------	---

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	H248 BAC adjacency configuration (config-h248-bac-adj)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	A realm group can contain multiple media addresses. When you configure a realm group under an adjacency, the IP address and port for the media stream of this adjacency is allocated from the media addresses in this realm group.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>realm</b> command is used to configure an adjacency:
-----------------	---

```
Router# configure terminal
Router(config)# sbac h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# realm 2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>media-address ipv4</b>	Adds an IPv4 address to the set of addresses that the BAC can use as local media address.

# realm (Rf billing)

To configure the realm information for Rf billing support on the Session Border Element of the Session Border Controller (SBC), use the **realm** command in the SBC SBE billing Rf configuration mode. To unconfigure the realm information for Rf billing support on the SBE of the SBC, use the **no** form of this command.

```
realm realm-name [usePCFAHeader | cdf cdf-name { FQDN FQDN-name | ipv4 ipv4-addr | vpn vpn-name } [port port-num] [priority priority]]
```

```
no realm realm-name [usePCFAHeader | cdf cdf-name { FQDN FQDN-name | ipv4 ipv4-addr | vpn vpn-name } [port port-num] [priority priority]]
```

## Syntax Description

<b>realm</b>	Configures the realm.
<i>realm-name</i>	Name of the realm. String length range: 1 to 63.
<b>usePCFAHeader</b>	Configures the P-Charging-Function-Addresses (PCFA) header.
<b>cdf</b>	Configures the Charging Data Function (CDF).
<i>cdf-name</i>	Name of the CDF.
<b>FQDN</b>	Configures the Fully Qualified Domain Name (FQDN) of the CDF.
<i>FQDN-name</i>	Fully Qualified Domain Name
<b>ipv4</b>	Configures IPv4.
<i>ipv4-addr</i>	IPv4 address.
<b>vpn</b>	Configures VPN.
<i>vpn-name</i>	VPN name.
<b>port</b>	Configures port information.
<i>port-num</i>	Port number of the CDF socket. Range: 1 to 65535. Default: 3868.
<b>priority</b>	Configures priority.
<i>priority</i>	Priority of the realm. Range: 1 to 100. Default: 1.

## Command Default

None

## Command Modes

SBC SBE billing Rf configuration (config-sbc-sbe-billing-rf)

## Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples**

The following example shows how to configure the usePCFAHeader for Rf billing support on the SBE of the SBC:

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# rf 0
Router(config-sbc-sbe-billing-rf)# realm asr1k usePCFAHeader
```

# reason

To enable the entry of a user into a mode for configuring a limit to a specific event type on the source (a port, IP address, VPN, and global address space), use the **reason** command in SBE blacklist mode. The **no** form of this command returns the event to its previous values.

**reason** {*event* | *description*}

**no reason**

## Syntax Description

<i>event</i>	The event type that should trigger the limit can be defined as any of the following: <ul style="list-style-type: none"> <li>• <b>authentication-failure</b>—Requests that fail authentication.</li> <li>• <b>bad-address</b>—Packets from unexpected addresses.</li> <li>• <b>corrupt-message</b>—Signaling packets that are corrupt and cannot be decoded.</li> <li>• <b>endpoint-registration</b>—Endpoint registrations.</li> <li>• <b>cac-policy-rejection</b>—Requests that are rejected by the configured CAC policy.</li> <li>• <b>rtg-policy-rejection</b>—Requests that fail to be routed onward by SBC.</li> <li>• <b>na-policy-rejection</b>—Requests that are rejected by the configured number analysis policy.</li> </ul>
<i>description</i>	Helpful description of the event that should trigger blacklisting.

## Command Default

No default behavior or values are available.

## Command Modes

SBE blacklist (config-sbc-sbe-blacklist)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2S	The event type policy-rejection and routing-failure was changed to cac-policy-rejection and rtg-policy-rejection. A new na-policy-rejection event type was also introduced.

## Usage Guidelines

The event field can only take the strings described in the Syntax Description.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples**

The following example shows the use of the **reason** command in context:

```
Router# configure
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 125.12.12.15
Router(config-sbc-sbe-blacklist-ipv4)# reason authentication-failure
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>critical-alert-size</b>	Configures the number of specified events that most occur before a critical alert is triggered.
<b>major-alert-size</b>	Configures the number of specified events that most occur before a major alert is triggered.
<b>minor-alert-size</b>	Configures the number of specified events that most occur before a minor alert is triggered.
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before blacklisting is triggered, and blocks all the packets from the source.
<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the <b>trigger-size</b> command.
<b>timeout</b>	Defines the length of time for which packets from the source are blocked, should the limit be exceeded.
<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the configured sources. Values not explicitly defined for each source are within brackets.
<b>show sbc sbe blacklist source</b>	Lists the limits in force for a particular source (whether they are from defaults or are explicitly configured) in a form in which they can be entered in the CLI. Also listed are any defaults for a smaller scope configured at this address. Values not explicitly configured (and therefore inherited from other defaults) are within brackets.
<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits that cause sources to be blacklisted.

# redirect-limit

To configure the maximum number of redirections that SBC performs on a call, use the **redirect-limit command** in SBE configuration **mode**. The **no** form of this command returns the adjacency to the default behavior.

**redirect-limit** *limit*

**no redirect-limit** *limit*

<b>Syntax Description</b>	limit	Specifies the maximum number of SIP 3xx retry attempts. The range is 0 to 200.
---------------------------	-------	--

**Command Default** The default number of redirections is 2.

**Command Modes** SBE configuration (config-sbc-sbe)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the maximum number of SIP 3xx retries as 4:

```
Router# configure
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# redirect-limit 4
```

# redirect-mode

To configure the behavior of SBC on receipt of a 3xx response to an invite from the SIP adjacency, use the **redirect-mode** command in adjacency SIP configuration mode. The no form of this command returns the adjacency to the default behavior.

```
redirect-mode {pass-through | recurse}
```

```
no redirect-mode {pass-through | recurse}
```

Syntax Description	pass-through	recurse
	Passes all 3xx responses back to the caller.	On 300, 301, 302, and 305 invite responses, the SBC resends the invite to the first listed contact address, or else passes the 3xx responses back.

**Command Default** pass-through

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to resend an invite to the first listed contact address or else pass the 3xx responses back to the sender:

```
Router# configure
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test1
Router(config-sbc-sbe-adj-sip)# redirect-mode recurse
Router(config-sbc-sbe-adj-sip)#
```

Related Commands	Command	Description
	redirect-limit	Configures the maximum number of redirections SBC performs on a call.

# redundant peer

To configure an alternative signaling peer for an adjacency, use the **redundant peer** command in the adjacency SIP configuration mode. To deconfigure an alternative signaling peer, use the **no** form of this command.

**redundant peer** *index*

**no redundant peer** *index*

<b>Syntax Description</b>	<i>index</i>	The index number of a peer, ranging from 1 to 5.
---------------------------	--------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.
-------------------------	---

**Examples** The following example shows how the **redundant peer** command is used to configure an alternative signaling peer for an adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# redundant peer 1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>priority</b>	Configures a redundant peer's priority.
	<b>address</b>	Configures either an IP address or a host name to act as the redundant peer.
	<b>network</b>	Configures either an IPv4 or IPv6 network in a redundant peer.
	<b>port</b>	Configures a port for the redundant peer.
	<b>signaling-peer-switch</b>	Configures a SIP adjacency to switch the signaling peer to an available destination.
	<b>signaling-peer-priority</b>	Configures the priority of a signaling peer on a SIP adjacency.
	<b>force-signaling-peer</b>	Forces SIP messages to go to a configured signaling peer.



# refresh-buffer

To configure the length of time by which the Cisco Unified Border Element (SP Edition) attempts to renew or refresh the address location with a delegate registration before the specified expiration time, use the **refresh-buffer** command in subscriber delegate profile configuration mode. To reset the refresh time to the default refresh time, use the **no refresh-buffer** command.

**refresh-buffer** *{timeout in secs}*

**no refresh-buffer** *{timeout in secs}*

<b>Syntax Description</b>	<i>timeout in secs</i>	This is the refresh expiration time in seconds. The range is 1 to 2,147,483 seconds. The default is 30 seconds.
---------------------------	------------------------	---

<b>Command Default</b>	The default refresh expiration time is 30 seconds.
------------------------	--

<b>Command Modes</b>	Subscriber delegate profile configuration mode (config-sbc-sbe-subscriber-delegate-prof)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	This is the length of time by which the SBC attempts to renew or refresh the address location with a delegate registration before the specified expiration time (configured with the <b>duration</b> command). This is one of the delegate profile parameters you can configure.
-------------------------	--

After a delegate profile is configured, the following profile parameters may optionally be configured:

- duration
- retry-count
- retry-interval
- refresh-buffer

<b>Examples</b>	The following example configures a provisioned delegate registration profile that can be applied to a delegate registration subscriber and configures a delegate registration for delegate client (aor=sip:bob@isp.example). The delegate registration profile is configured with a duration expiration time of 1000 seconds, a retry count of 5 times, a retry interval of 60 seconds, and a refresh timeout time of 200 seconds:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# delegate-profile my-profile
Router(config-sbc-sbe-subscriber-delegate-prof)# duration 1000
Router(config-sbc-sbe-subscriber-delegate-prof)# retry-count 5
```

```

Router(config-sbc-sbe-subscriber-delegate-prof)# retry-interval 60
Router(config-sbc-sbe-subscriber-delegate-prof)# refresh-buffer 200
Router(config-sbc-sbe-subscriber-delegate-prof)# exit
Router(config-sbc-sbe)# subscriber sip:bob@isp.example
Router(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
Router(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
Router(config-sbc-sbe-subscriber-contact)# exit
Router(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
Router(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
Router(config-sbc-sbe-subscriber-delegate)# profile my-profile
Router(config-sbc-sbe-subscriber-delegate)# activate
Router(config-sbc-sbe-subscriber-delegate)# end

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>duration</b>	Configures the length of time in seconds during which the SBC tries to perform delegate registration before stopping.
<b>retry-count</b>	Configures the number of times the SBC repeats the delegate registration processing after the retry interval ends.
<b>retry-interval (registration)</b>	Configures the length of time the SBC waits before it retries delegate registration.
<b>delegate-profile</b>	Configures a delegate registration profile that is applied to a delegate registration subscriber.
<b>delegate-registration</b>	Configures a delegate registration for a delegate client.
<b>show sbc sbe sip delegate-profile</b>	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.

# reg-min-expiry

To configure the minimum registration period in seconds on the SIP adjacency, use the **reg-min-expiry** command in the adjacency SIP configuration mode. To enter the default value, use the **no** form of this command.

*reg-min-expiry period*

*no reg-min-expiry period*

<b>Syntax Description</b>	<i>period</i>	The minimum expiry period in seconds. The range is 1 to 2000000.
---------------------------	---------------	--

<b>Command Default</b>	3000 seconds
------------------------	--------------

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	This is the minimum expiry period accepted on a subscriber registration if not fast-pathing, or the minimum-expiry period passed onward if fast-pathing is in use.
-------------------------	--

The minimum registration period cannot be changed after an adjacency has been configured. To change the minimum registration period, remove the adjacency by running **no sbc *sbc-name* sbe adjacency sip *adjacency-name*** command and then reconfigure the adjacency.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

<b>Examples</b>	The following example shows how to enable the register minimum expiry on the SIP adjacency SipToIsp42 to 300 seconds:
-----------------	---

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# reg-min-expiry 300
Router(config-sbc-sbe-adj-sip)# exit
```

# register-rate

To configure the register rate for a Session Border Controller (SBC) H.248 access adjacency, use the **register-rate** command in the H248 BAC adjacency configuration mode. To set the default value for the register rate, use the **no** form of this command.

**register-rate** *reg-rate*

**no register-rate** *reg-rate*

<b>Syntax Description</b>	<i>reg-rate</i>	Register rate for an SBC H.248 access adjacency, in seconds. Range: 30 to 300. Default: 100.
<b>Command Default</b>	The default value for <i>reg-rate</i> is 100.	
<b>Command Modes</b>	H248 BAC adjacency configuration (config-h248-bac-adj)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to configure the register rate for an SBC H.248 access adjacency:

```
Router> enable
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access vrfex
Router(config-h248-bac-adj)# control-address ipv4 10.0.0.1 port 1
Router(config-h248-bac-adj)# register-rate 33
```

# registration aggregate

To enable Aggregate Registration, use the **registration aggregate** command in adjacency sip configuration mode. To disable Aggregate Registration, use the **no registration aggregate** command.

**registration aggregate**

**no registration aggregate**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** adjacency sip configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command enables Aggregate Registration support from the specified SIP adjacency facing the Registrar server.

**Examples** The following example enables Aggregate Registration on adjacency Cary-IP-PBX, which has a preset access profile specified because it faces an access device on a UNI network. The last three commands in the configuration, entered in the correct order, enable the aggregate registration call routing to work.

```
sbc mySbc
sbe
  adjacency sip Cary-IP-PBX
  registration rewrite-register
  inherit profile preset-access
  registration aggregate
  header-name to passthrough
  request-line request-uri rewrite
```

The following example displays detailed output for adjacency Cary-IP-PBX, including the “Register Aggregate:” field that shows Aggregate Registration is “Enabled.”

```
Router# show sbc mySbc sbe adjacencies Cary-IP-PBX detail
SBC Service "mySBC"
  Adjacency Cary-IP-PBX (SIP)
    Status:                Attached
    Signaling address:     100.100.100.100:5060, VRF Admin
    Signaling-peer:        10.10.51.10:5060
    Force next hop:        No
    Account:
    Group:                  None
```

```

In header profile:      Default
Out header profile:    Default
In method profile:     Default
Out method profile:    Default
In UA option prof:    Default
Out UA option prof:    Default
In proxy opt prof:    Default
Out proxy opt prof:    Default
Priority set name:     None
Local-id:              None
Rewrite REGISTER:     Off
Target address:       None
Register Out Timer:   1800 seconds
Register Aggregate:   Enabled
NAT Status:           Auto Detect
Reg-min-expiry:       30 seconds
Fast-register:        Enabled
Fast-register-int:    30 seconds
Authenticated mode:   None
Authenticated realm:  None
Auth. nonce life time: 300 seconds
IMS visited NetID:    None
Inherit profile:      Default
Force next hop:       No
Home network Id:      None
UnEncrypt key data:   None
SIPi passthrough:    No
Rewrite from domain:  Yes
Rewrite to header:    Yes
Media passthrough:    No
Preferred transport:  UDP
Hunting Triggers:     Global Triggers
Redirect mode:         Pass-through
Security:              Untrusted
Outbound-flood-rate:  None
Ping-enabled:         No
Signaling Peer Status: Not Tested
Rewrite Request-uri: Enabled
Registration Monitor: Disabled
    
```

The following is a configuration example showing that Aggregate Registration and SoftSwitch Shielding are configured:

```

sbc test
sbe
sip header-profile myheader
  header P-Called-Party-ID entry 1
  action pass
adjacency sip sippa =====> Adjacency facing IP-PBX
  header-profile inbound myheader
  header-profile outbound myheader
  inherit profile preset-access
  preferred-transport udp
  signaling-address ipv4 99.99.103.150
  signaling-port 5080
  remote-address ipv4 100.100.1.64 255.255.255.255
  signaling-peer 100.100.1.64
  signaling-peer-port 5080
  registration rewrite-register
  account sipp-a
  registration aggregate
  fast-register disable
  header-name to passthrough
    
```

```

request-line request-uri rewrite

attach
adjacency sip sippb      =====> Adjacency facing REGISTRAR
nat force-off
header-profile inbound myheader
header-profile outbound myheader
inherit profile preset-core
preferred-transport udp
signaling-address ipv4 99.99.103.150
signaling-port 5082
remote-address ipv4 100.100.1.64 255.255.255.255
signaling-peer 100.100.1.64
signaling-peer-port 5082
account sipp-b
registration target address 100.100.1.64
registration target port 5084
fast-register disable
attach
cac-policy-set 1
first-cac-table mytable
first-cac-scope src-adjacency
cac-table mytable
  table-type limit adjacency
  entry 1
    match-value sippa
    max-num-calls 10
    action cac-complete
  complete
cac-policy-set global 1
call-policy-set 1
first-call-routing-table src-acc-table
first-reg-routing-table src-acc-table
rtg-src-adjacency-table src-acc-table
  entry 1
    action complete
    dst-adjacency sippb
    match-adjacency sippa
  entry 2
    action complete
    dst-adjacency sippa
    match-adjacency sippb
  complete
call-policy-set 2
call-policy-set default 1
!
vdbe global
unexpected-source-alerting
media-address ipv4 99.99.103.156
media-timeout 9999
activate
!
Softswitch shielding config
=====
sbc test
sbe
adjacency sip sippa
signaling-address ipv4 99.99.103.150
signaling-port 5080
remote-address ipv4 100.100.1.64 255.255.255.255
signaling-peer 100.100.1.64
signaling-peer-port 5080
registration rewrite-register
account sipp-a

```

```

attach
adjacency sip sipb
  signaling-address ipv4 99.99.103.150
  signaling-port 5082
  remote-address ipv4 100.100.1.64 255.255.255.255
  signaling-peer 100.100.1.64
  signaling-peer-port 5082
  account sipb
  registration outgoing timer 86400
  registration target address 100.100.1.64
  registration target port 5084
attach
call-policy-set 1
  first-call-routing-table src-acc-table
  first-reg-routing-table src-acc-table
  rtg-src-adjacency-table src-acc-table
  entry 1
    action complete
    dst-adjacency sipb
    match-adjacency sipba
  entry 2
    action complete
    dst-adjacency sipba
    match-adjacency sippb
  complete
call-policy-set default 1
!
media-address ipv4 99.99.103.156
media-timeout 9999
activate
!
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>registration monitor</b>	Enables the Registrar server to monitor subscriber event changes due to registration changes.
<b>registration outgoing timer</b>	Enable SoftSwitch Shielding by setting the registration timeout timer for the time interval when Cisco Unified Border Element (SP Edition) forwards outgoing registration messages.
<b>registration rewrite-register</b>	Configures the SIP register request rewriting on an adjacency.
<b>inherit profile</b>	Configures a global inherit profile for the SIP adjacency.
<b>adjacency</b>	Configures the adjacency facing the registrar.



# registration contact username

To configure a contact username in a SIP REGISTER request to either pass through unchanged or be allowed to be modified, use the **registration contact username** command in the Adjacency SIP configuration mode. To reset to the default, use the **no** form of this command.

*registration contact username* [*passthrough* | *rewrite* [**numeric** | **userid-and-numeric**]]

*no registration contact username* [*passthrough* | *rewrite* [**numeric** | **userid-and-numeric**]]

## Syntax Description

<i>passthrough</i>	Specifies that the contact username in a SIP REGISTER request is passed through unchanged.  <b>Note</b> If a contact username is longer than 32 characters, the username is not passed, and the contact username is rewritten as a hashed value.
<i>rewrite</i>	Allows the contact username in a SIP REGISTER request to be changed or rewritten.
<b>numeric</b>	Rewrites the contact username in a SIP REGISTER request as an originating hashed numeric value.
<b>userid-and-numeric</b>	Rewrites the contact username in a SIP REGISTER request as an originating user ID and a hashed numeric value.

## Command Default

By default, the contact username in a SIP REGISTER request can be changed or rewritten.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.3S	This command was modified. The <b>numeric</b> and <b>userid-and-numeric</b> keywords were added.

## Usage Guidelines

The **registration contact-username** command must be configured on the adjacency facing the registrar. The **registration contact username** command with the **passthrough** option allows you to specify that the contact username in the SIP REGISTER request should be passed through unchanged when rewriting contacts. The **passthrough** option disambiguates subscribers who register from different devices with the same private username by using a unique local port number when multiple contact URIs are registered for the same public ID.

The range of valid signaling ports are configured with the **signaling-port** command on a registrar-facing adjacency. If **signaling-port** is not configured on the adjacency, the SBC is not able to disambiguate subscribers who register from different devices with the same username.

**Note**

If a contact username is longer than 32 characters, the username is not passed, and the contact username is rewritten as a hashed value.

**Examples**

The following example shows how to pass a single contact username unchanged:

```
adjacency sip SIPP1Reg
  group SIPP1Reg
  inherit profile preset-core
  signaling-address ipv4 192.168.101.1
  statistics-setting summary
  signaling-port 5060 5062
  remote-address ipv4 192.168.101.12 255.255.255.255
  signaling-peer 192.168.101.12
  signaling-peer-port 7068
  registration target address 192.168.101.12
  registration target port 7069
  registration contact username passthrough
attach
```

```
REGISTER UE to SBC (packet flow)
REGISTER sip:1.2.3.4 SIP/2.0
Via: SIP/2.0/UDP 192.169.0.1;branch=z9hG4bK+ddil+5489756
From: <sip:bob@registrar.com>;tag=tag
To: <sip:bob@registrar.com>
Call-ID: reg00001@upstream.com
CSeq: 1 REGISTER
Contact: <sip:bob@1.1.1.1>
Expires: 60
```

```
REGISTER SBC to Core (packet flow)
REGISTER sip:registrar.com SIP/2.0
Via: SIP/2.0/UDP
192.168.101.1:5060;branch=z9hG4bK+a1a6922fdaa29911319b1d263134925c1+1.2.3.4+1
Max-Forwards: 70
From: <sip:bob@registrar.com>;tag=192.168.101.1+1+14e5461d+b196176d
Content-Length: 0
To: <sip:bob@registrar.com>
Call-ID: 83d9583ea51ae624b897ec6881114e84@192.168.101.1
CSeq: 1 REGISTER
Contact: <sip:bob@192.168.101.1:5060>
```

The following is an example flow of multiple registrations for the same subscriber. The example shows how a sequence of REGISTER requests registering multiple contacts behaves. This example assumes that all the headers, apart from the contact headers, are omitted from the requests, and that the registrar-facing adjacency has a signaling port range of 5060 to 5063 (this means that four local ports are available).

```
adjacency sip SIPP1Reg
  group SIPP1Reg
  inherit profile preset-core
  signaling-address ipv4 192.168.101.1
  statistics-setting summary
  signaling-port 5060 5063
  remote-address ipv4 192.168.101.12 255.255.255.255
  signaling-peer 192.168.101.12
  signaling-peer-port 7068
  registration target address 192.168.101.12
  registration target port 7069
```

```
registration contact username passthrough
attach
```

1. A REGISTER is received registering two contact addresses for the number 5551234:

```
REGISTER sip:5551234@1.2.3.4 SIP/2.0
Contact: <sip:bob@1.1.1.1>
Contact: <sip:robert@1.1.1.1>
```

2. The SBC forwards this REGISTER to the registrar after rewriting the contact address and port:

```
REGISTER sip:5551234@1.2.3.4 SIP/2.0
Contact: <sip:bob@192.168.101.1:5060>
Contact: <sip:robert@192.168.101.1:5061>
```

3. Another REGISTER is received for the number 5551234, registering another endpoint with a duplicate username:

```
REGISTER sip:5551234@1.2.3.4 SIP/2.0
Contact: <sip:bob@2.2.2.2>
```

4. The SBC forwards this to the registrar, passing the username through unchanged:

```
REGISTER sip:5551234@1.2.3.4 SIP/2.0
Contact: <sip:bob@192.168.101.1:5062>
```

5. A third endpoint is registered for the same number. This endpoint provides a very long contact name in the Contact field:

```
REGISTER sip:5551234@1.2.3.4 SIP/2.0
Contact: <sip:this_is_an_extremely_long_contact_username@2.2.2.2>
```

6. The SBC forwards this request to the registrar and rewrites the username because it is over the maximum passthrough length (32):

```
REGISTER sip:5551234@1.2.3.4 SIP/2.0
Contact: <sip: 6e83bca53a48bd629a153a93ff8f4af1@192.168.101.1:5063>
```

The following example shows how to rewrite a contact username in a SIP REGISTER request as an originating user ID and a hashed numeric value:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# registration contact username rewrite userid-and-numeric
```

The following examples show the SIP headers when the **userid-and-numeric** keyword is used:

- Incoming register at the SBC:

```
From: <sip:1234@example.com>;tag=1111
To: <sip:1234@example.com>
Contact: <sip:1234@1.1.1.1>;expires=3600
```

- Outgoing register from the SBC:

```
From: <sip:1234@example.com>;tag=1234
To: <sip:1234@example.com>
Contact: <sip:1234-j1j2j3j4@10.10.10.1>;expires=3600
```

The following example shows how to rewrite a contact username in a SIP REGISTER request as an originating hashed numeric value:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SIPP
Router(config-sbc-sbe-adj-sip)# registration contact username rewrite numeric
```

The following examples show the SIP headers when the **numeric** keyword is used:

- Incoming register at the SBC:

```
From: <sip:1234@example.com>;tag=1111
To: <sip:1234@example.com>
Contact: <sip:1234@1.1.1.1>;expires=3600
```

- Outgoing register from the SBC:

```
From: <sip:1234@example.com>;tag=1234
To: <sip:1234@example.com>
Contact: <sip:12345678@10.10.10.1>;expires=3600
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>registration rewrite-register</b>	Configures the SIP register request rewriting.
<b>signaling-port</b>	Configures a range of valid signaling ports on a registrar-facing adjacency to allow the SBC to disambiguate subscribers who register from different devices with the same username.

# registration monitor

To enable the Registrar server to monitor subscriber event changes due to registration changes, use the **registration monitor** command in adjacency sip configuration mode. To disable registration monitoring, use the **no registration monitor** command.

**registration monitor**

**no registration monitor**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values are available.

## Command Modes

adjacency sip configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command enables the Registrar server to monitor event subscriptions due to changes to the state of the registration. Subscription changes for each subscriber that re-registers with the Registrar server situation on the specified adjacency may cause Cisco Unified Border Element (SP Edition) to add, remove, or update the subscriber state.

## Examples

The following example shows how registration monitoring is enabled:

```
sbc Raleigh-SBC
sbe
  adjacency sip Cary-IP-PBX
  registration monitor
```

The following example displays detailed output for adjacency Cary-IP-PBX, including the “Registration Monitor:” field that shows Registration Monitoring is “Enabled:”

```
Router# show sbc mySBC sbe adjacencies Cary-IP-PBX detail
SBC Service "mySbc"
Adjacency Cary-IP-PBX (SIP)
  Status:                Attached
  Signaling address:     100.100.100.100:5060, VRF Admin
  Signaling-peer:        10.10.51.10:5060
  Force next hop:        No
  Account:
  Group:                  None
  In header profile:     Default
  Out header profile:    Default
  In method profile:     Default
```

```

Out method profile:      Default
In UA option prof:      Default
Out UA option prof:     Default
In proxy opt prof:      Default
Out proxy opt prof:     Default
Priority set name:       None
Local-id:                None
Rewrite REGISTER:       Off
Target address:          None
Register Out Timer:     1800 seconds
Register Aggregate:     Enabled
NAT Status:              Auto Detect
Reg-min-expiry:          30 seconds
Fast-register:           Enabled
Fast-register-int:      30 seconds
Authenticated mode:     None
Authenticated realm:    None
Auth. nonce life time:  300 seconds
IMS visited NetID:      None
Inherit profile:         Default
Force next hop:          No
Home network Id:         None
UnEncrypt key data:     None
SIPi passthrough:       No
Rewrite from domain:    Yes
Rewrite to header:      Yes
Media passthrough:      No
Preferred transport:    UDP
Hunting Triggers:       Global Triggers
Redirect mode:           Pass-through
Security:                Untrusted
Outbound-flood-rate:    None
Ping-enabled:            No
Signaling Peer Status:  Not Tested
Rewrite Request-uri:    Disabled
Registration Monitor: Enabled
    
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>registration aggregate</b>	Enables Aggregate Registration.
<b>registration outgoing timer</b>	Enables SoftSwitch Shielding by setting the registration timeout timer for the time interval when Cisco Unified Border Element (SP Edition) forwards outgoing registration messages.
<b>registration rewrite-register</b>	Configures the SIP register request rewriting on an adjacency.
<b>inherit profile</b>	Configures a global inherit profile for the SIP adjacency.
<b>adjacency</b>	Configures the adjacency facing the registrar.

# registration outgoing timer

To enable SoftSwitch Shielding by setting the registration outgoing timer for the time interval when Cisco Unified Border Element (SP Edition) forwards outgoing registration messages, use the **registration outgoing timer** command in adjacency sip configuration mode. To set the outgoing time interval to zero and disable SoftSwitch Shielding, use the **no registration outgoing timer** command.

**registration outgoing timer** *{sec}*

**no registration outgoing timer** *{sec}*

<b>Syntax Description</b>	<i>sec</i>	Specifies number of seconds. The value is 1 to 2147483647 seconds. The default is zero.
---------------------------	------------	--

**Command Default** The default value of zero disables SoftSwitch Shielding.

**Command Modes** adjacency sip configuration (config-sbc-sbe-adj-sip)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command enables SoftSwitch Shielding. It sets the registration timeout timer for the time interval in seconds when Cisco Unified Border Element (SP Edition) keeps forwarding outgoing REGISTER messages to the softswitch before timing out.

**Examples** The following example configures SoftSwitch Shielding on adjacency “SoftSwitch:”

```
sbc mySbc
sbe
 adjacency sip SoftSwitch
  registration outgoing timer <sec>
  registration rewrite-register
  inherit profile preset-core
```

The following is a configuration example showing that SoftSwitch Shielding is configured for adjacency sippb:

```
SoftSwitch Shielding Configuration
=====
sbc test
sbe
 adjacency sip sippa
  signaling-address ipv4 99.99.103.150
  signaling-port 5080
```

```

remote-address ipv4 100.100.1.64 255.255.255.255
signaling-peer 100.100.1.64
signaling-peer-port 5080
registration rewrite-register
account sipp-a
attach
adjacency sip sippb
signaling-address ipv4 99.99.103.150
signaling-port 5082
remote-address ipv4 100.100.1.64 255.255.255.255
signaling-peer 100.100.1.64
signaling-peer-port 5082
account sipp-b
registration outgoing timer 86400
registration target address 100.100.1.64
registration target port 5084
attach
call-policy-set 1
first-call-routing-table src-acc-table
first-reg-routing-table src-acc-table
rtg-src-adjacency-table src-acc-table
entry 1
  action complete
  dst-adjacency sippb
  match-adjacency sippa
entry 2
  action complete
  dst-adjacency sippa
  match-adjacency sippb
complete
call-policy-set default 1
!
media-address ipv4 99.99.103.156
media-timeout 9999
activate
!

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>registration monitor</b>	Enables the Registrar server to monitor subscriber event changes due to registration changes.
<b>registration aggregate</b>	Enables Aggregate Registration.
<b>delegate-registration</b>	Configures Provisioned Delegate Registration for a specific delegate client.



# registration required

To specify that registration is required for a call to proceed, use **registration required** command in the SBC SBE Adjacency SIP mode. Use the **no** form of this command to specify that registration is not required for the call to proceed.

**registration required**

**no registration required**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBC SBE Adjacency SIP (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode.

**Examples** The following example specifies that registration is required for a call to proceed on the SIP adjacency CORE:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip CORE
Router(config-sbc-sbe-adj-sip)# registration required
```

The following show command output provide details on the above configuration. Note the value of the registration required field:

```
Router# show sbc test sbe adjacencies CORE detail
SBC Service "test"
  Adjacency CORE (SIP)
    Status: Detached
    Signaling address: 44.21.171.8:default
    Signaling-peer: :5060 (Default)
    Force next hop: No
    Account:
    Group: None
    In header profile: Default
    Out header profile: Default
    In method profile: Default
    Out method profile: Default
    In body profile: None
```

```

Out body profile:      None
In UA option prof:    Default
Out UA option prof:   Default
In proxy opt prof:    Default
Out proxy opt prof:   Default
Priority set name:     None
Local-id:             None
Rewrite REGISTER:     Off
Register contact username: Rewrite
Target address:       None
NAT Status:           Auto Detect
Reg-min-expiry:       3000 seconds
Fast-register:        Enabled
Fast-register-int:    30 seconds
Register aggregate:   Disabled
Registration Required: Enabled
Register Out Interval: 0 seconds
Parse username params: Disabled
Supported timer insert: Disabled
Suppress Expires:     Disabled
p-asserted-id header-value: not defined
p-assert-id assert:   Disabled
Authenticated mode:   None
Authenticated realm:  None
Auth. nonce life time: 300 seconds
IMS visited NetID:    None
Inherit profile:      Default
Force next hop:       No
Home network Id:      None
UnEncrypt key data:   None
SIPi passthrough:    No
Passthrough headers:
Media passthrough:    No
Incoming 100rel strip: No
Incoming 100rel supp: No
Out 100rel supp add:  No
Out 100rel req add:   No
Parse TGID parms:    No
IP-FQDN inbound:
IP-FQDN outbound:
FQDN-IP inbound:
FQDN-IP outbound:
Outbound Flood Rate:  None
Hunting Triggers:     Global Triggers
Add transport=tls param: Disabled
Redirect mode:         Pass-through
Security:              Untrusted-Unencrypted
TLS mutual authentication: No
Ping:                  Disabled
Ping Interval:         32 seconds
Ping Life Time:       32 seconds
Ping Peer Fail Count: 3
Ping Trap sending:     Enabled
Ping Peer Status:      Not Tested
Rewrite Request-uri:   Disabled
Registration Monitor:  Disabled
DTMF SIP NOTIFY Relay: Enabled
DTMF SIP NOTIFY Interval: 2000
DTMF SIP default duration: 200
DTMF Preferred Method: SIP NOTIFY
Realm                  : None

```

Statistics setting: Summary

# registration rewrite-register

To configure the SIP register request rewriting, use the **registration rewrite-register** command in Adjacency SIP configuration mode. To deconfigure the register request rewriting, use the **no** form of this command.

**registration rewrite-register**

**no registration rewrite-register**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **registration rewrite-register** command configures the SIP register request rewriting on SIP adjacency SipToIsp42.

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# registration rewrite-register
```

# registration target address

To set the address to be used when an outbound SIP register request rewriting occurs, use the **registration target address** command in Adjacency SIP configuration mode. To remove the address, use the **no** form of this command.

**registration target address** *host address*

**no registration target address** *host address*

## Syntax Description

<i>host address</i>	Specifies the host address to use when an outbound SIP register request rewriting occurs. This parameter can be a DNS name or an IPv4 address in dotted decimal format. Valid strings are from 1 to 255 characters in length.
---------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **registration target address** command sets the target address for SIP adjacency SipToIsp42 as example.com:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# registration target address example.com
```

# registration target port

To set the port to be used when an outbound SIP REGISTER request rewriting occurs, use the **registration target port** command in Adjacency SIP configuration mode. To enter the default value, use the **no** form of this command.

**registration target port** *port-number*

**no registration target port** *port-number*

## Syntax Description

<i>port-number</i>	Specifies the port number to use when an outbound SIP REGISTER request rewriting occurs. Valid values can be from 1 to 65535. If you enter the default value of <b>0</b> , no port address is set.
--------------------	--

## Command Default

Default value is 0. This cannot be directly entered.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **registration target port** command sets the port number for SIP adjacency SipToIsp42 as 5070:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# registration target port 5070
```

# registration unencrypted-convert

To enable the conversion of SIPS URIs to SIP URIs on a trusted-unencrypted adjacency, use the **registration unencrypted-convert** command in adjacency SIP configuration mode. To remove this configuration, use the **no** form of this command.

**registration unencrypted-convert**

**no registration unencrypted-convert**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 3.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how the **registration unencrypted-convert** command is used to enable the conversion of SIPS URIs to SIP URIs on the my\_adjacency adjacency:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip my_adjacency
Router(config-sbc-sbe-adj-sip)# registration unencrypted-convert
```

Related Commands	Command	Description
	<b>registration aggregate</b>	Enables aggregate registration.
	<b>registration contact username</b>	Configures a contact username in a SIP REGISTER request to either pass through unchanged or be allowed to be modified.
	<b>registration monitor</b>	Enables the registrar server to monitor subscriber event changes due to registration changes.

<b>Command</b>	<b>Description</b>
<b>registration outgoing timer</b>	Enables SoftSwitch Shielding by setting the registration outgoing timer for the time interval when the Cisco Unified Border Element (SP Edition) forwards outgoing registration messages.
<b>registration required</b>	Specifies that registration is required for a call to proceed.
<b>registration rewrite-register</b>	Configures the SIP register request rewriting.
<b>registration target address</b>	Sets the address to be used when an outbound SIP register request rewriting occurs.
<b>registration target port</b>	Sets the port to be used when an outbound SIP REGISTER request rewriting occurs.

# reject-threshold

To configure the memory threshold and reject rate for new calls, use the **reject-threshold** command. Use the **no** form of this command to restore the default values.

```
reject-threshold [level] memory [percentage] [reject rate]
```

```
[no] reject-threshold [level] memory [percentage]
```

Syntax Description		
<i>level</i>		Level of threshold. Values are: minor, major, and critical.
<i>percentage</i>		Percentage of total processor memory remaining. The value range is from 6 to 50.
<i>reject rate</i>		Number of new calls to be rejected out of each 10 calls.

**Command Modes** Configure SBC SBE (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

Follow these rules when configuring the threshold using this command:

- Percentage for minor level must be greater than current major level.
- Percentage for major level must be greater than current critical level.
- Percentage for major level must be less than current minor level.
- Percentage for critical level must be less than current major level.

**Examples** The following example shows how to configure the minor memory congestion level set when 30 percentage of total memory is available. The reject rate at this level is set to 0:

```
(config)# sbc mySBC
(config-sbc)# sbe
(config-sbc-sbe)# reject-threshold minor memory 30 0
```

The following example shows how to restore the default major memory threshold and drop rate:

```
(config)# sbc mySBC
(config-sbc)# sbe
(config-sbc-sbe)# no reject-threshold major memory
```



Following is an example of the show command output for reject threshold:

```
Router# show sbc mySBC sbe call-stats reject-threshold
```

```
Level      Memory Trigger  Action
-----
minor     < 25 percent    0 in 10 calls dropped
major     < 20 percent    4 in 10 calls dropped
critical  < 15 percent    9 in 10 calls dropped
halt      < 10 percent   10 in 10 calls dropped
```

Current level: NORMAL

Total calls rejected due to low memory threshold: 0

# remote-address ipv4

To configure a remote IPv4 H.248 signaling address for the Media Gateway Control Function (MGCF) and the Access Gateway Control Function (AGCF), use the **remote-address ipv4** command in the H248 BAC adjacency configuration mode. To unconfigure the MGC and the AGCF from using a remote IPv4 H.248 signaling address, use the **no** form of this command.

```
remote-address ipv4 ipv4-address port port-number
```

```
no remote-address ipv4 ipv4-address port port-number
```

Syntax Description	Parameter	Description
	<b>ipv4</b>	Configures an IPv4 H.248 signaling remote address for the MGCF and AGCF.
	<i>ipv4-address</i>	IPv4 address assigned to an H.248 association.
	<b>port</b>	Specifies the port for the adjacency address.
	<i>port-number</i>	Number for the adjacency address port. The range is from 1 to 65535.

**Command Default** None

**Command Modes** H.248 BAC adjacency configuration (config-h248-bac-adj)

Command History	Release	Modification
	Cisco IOS XE Release 3.7	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command can be configured only in the core adjacency submode and not in the access adjacency submode.

**Examples** The following example shows how the **remote-address ipv4** command is used to configure a remote IPv4 H.248 signaling address for the MGCF and AGCF:

```
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access iad_80_123
Router(config-h248-bac-adj)# remote-address ipv4 192.168.102.14 port 2944
```

Related Commands	Command	Description
	<b>control-address ipv4</b>	Configures a local IPv4 H.248 signaling address for the BAC.

# remote-port (session border controller)

To define the port to connect to on the SBE for an H.248 controller, use the **remote-port** command in VDBE h248 mode.

**remote-port** *port-num*

<b>Syntax Description</b>	<i>port-num</i>	This is the port number to be configured.  If the port is not configured or is configured with the value zero, then the H.248 default port number, 2944, is used.
---------------------------	-----------------	---

<b>Command Default</b>	Port number 2944
------------------------	------------------

<b>Command Modes</b>	VDBE h248 (config-sbc-dbe-h248)
----------------------	---------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	<p>The local-port and control-address are not applied until the controller is added and the remote address is configured. Also, the controller should be deleted to delete the remote address.</p> <p>If the port is not configured, or is configured with the value zero, then the H.248 default port number, 2944, is used.</p> <p>To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.</p>
-------------------------	---

<b>Examples</b>	The following example configures the port to 2944 on the H.248 controller with index 1:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-port 2944
Router(config-sbc-dbe-vdbe-h248)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dbe</b>	Enters into DBE-SBE configuration mode.
	<b>vdbe</b>	Configures a virtual data border element (VDBE) and enters the VDBE configuration mode.
	<b>controller h248</b>	Creates an H.248 controller for a DBE.

# req-timeout

To configure the ENUM request timeout period, use the **req-timeout** command in ENUM configuration mode. To return the timeout period to the default value, use the no form of this command.

**req-timeout** *timeout*

**no req-timeout** *timeout*

<b>Syntax Description</b>	<i>timeout</i>	ENUM request timeout period in milliseconds. The range is 0 to 2147483647.
---------------------------	----------------	--

<b>Command Default</b>	The default is 5000 milliseconds.	
------------------------	-----------------------------------	--

<b>Command Modes</b>	ENUM configuration (config-sbc-sbe-enum)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.	
-------------------------	--	--

<b>Examples</b>	The following example shows how to configure the ENUM request timeout period:	
	<pre>Router# <b>configure terminal</b> Router(config)# <b>sbc MySBC</b> Router(config-sbc)# <b>sbe</b> Router(config-sbc-sbe)# <b>enum 1</b> Router(config-sbc-sbe-enum)# <b>req-timeout 10000</b></pre>	

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
	<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.

<b>Command</b>	<b>Description</b>
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

# request-line

To configure the actions for modifying a request line, on the outbound side, use the **request-line** command in the SIP Header Editor configuration mode. To deconfigure the actions, use the **no** form of this command.

**request-line** [*entry entry-number*]

**no request-line** [*entry entry-number*]

## Syntax Description

<b>entry</b>	Specifies the filtered entry number. By default, it is 1.
<b>entry-number</b>	Entry number. It can range from 1 to 99.

## Command Default

By default, the entry number is 1.

## Command Modes

SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to configure the actions required to modify a request line:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Myeditor
Router(config-sbc-sbe-mep-hdr)# request-line
Router(config-sbc-sbe-mep-hdr-ele)# action replace-value value sip:user@host
```

## Related Commands

Command	Description
<b>blacklist</b>	Configures a SIP header or method blacklist editors on a SIP message.
<b>description</b>	Configures descriptive text for a SIP header.
<b>sip header-editor</b>	Configures a header editor.

# request-line request-uri rewrite

To request the SBC to rewrite the Request-URI to a different user and hostname before sending a request to a registered subscriber, use the **request-line request-uri rewrite** command in Adjacency SIP configuration mode.

## request-line request-uri rewrite

### Syntax Description

This command has no arguments or keywords.

**Note** Uniform Resource Identifier (URI) is an IP address of the subscriber. It is a string field of 62 characters maximum length.

### Command Default

No default behavior or values are available.

### Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

### Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

This command is used in Aggregate Registration only and is configured on the adjacency facing the IP-PBX which requires Aggregate Registration. This command allows outgoing calls to the endpoint registered with Aggregate Registration. The SBC rewrites the Request-URI as <user>@<hostname>, before sending a request to the registered subscriber (IP-PBX) on an adjacency.

The “**request-uri**” field indicates whether this adjacency faces an aggregation device, such as an IP-PBX, which cannot route incoming messages based on the P-Called-Party-ID or To header, but only on the Request-URI.

The Request-URI would normally be set to the Contact address registered by the IP-PBX rather than an endpoint address.

Before sending a request to a registered subscriber, for example IP-PBX, on this adjacency, the SBC will rewrite the Request-URI as <user>@<hostname> where:

- <user> is taken from the P-Called-Party-ID header if present, or if not, the To header.
- <hostname> is taken from the Contact address that was registered for this subscriber.

Uniform Resource Identifier (URI) is an IP address of the subscriber. It is a string field of 62 characters maximum length.

### Examples

The following example shows the rewrite of the Request-URI to sip:bill@1.1.1.1 in an Aggregate Registration configuration:

```
Router(config-sbc-sbe-adj-sip)# request-line request-uri rewrite sip:bill@1.1.1.1
```

The following example enables Aggregate Registration on adjacency Cary-IP-PBX, which has a preset access profile specified because it faces an access device on a UNI network. The last three commands in the configuration, entered in the correct order, enable the aggregate registration call routing to work.

```
sbc mySbc
 sbe
  adjacency sip Cary-IP-PBX
  registration rewrite-register
  inherit profile preset-access
  registration aggregate
  header-name to passthrough
  request-line request-uri rewrite
```

Related Commands	Command	Description
	<b>header-name</b>	Configures the contact header and passthrough header in non-REGISTER requests.
	<b>registration aggregate</b>	Enables Aggregate Registration.



# resource-priority-set

To establish the resource priority set to be used with the specified SIP adjacency in the mode of an SBE entity, use the **resource-priority-set** command in adjacency SIP configuration mode. To remove the priority set, use the **no** form of this command.

**resource-priority-set** *resource-priority-set-name*

**no resource-priority-set** *resource-priority-set-name*

## Syntax Description

<i>resource-priority-set-name</i>	Specifies the name of the resource priority set.  The <i>resource-priority-set-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **resource-priority-set** command sets the SIP adjacency SipToIsp42 with the resource-priority-set named dsn:

```
Router# configure
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# resource-priority-set dsn
```

# resource-priority

To configure the priority of a resource-priority header string, use the **resource-priority** command in resource priority mode. To deconfigure the priority, use the **no** form of this command.

**resource-priority** *value*

**no resource-priority** *value*

## Syntax Description

<i>value</i>	Specifies the string value to be assigned the priority. The <i>value</i> must be followed by the priority as shown: <i>value.priority</i> .
--------------	---

## Command Default

No default behavior or values are available.

## Command Modes

Resource priority (config-sbc-sbe-rsrc-pri-set)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **resource-priority** command configures the priority for resource-priority header string dsn.

```
Router# configure
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# resource-priority-set dsn
Router(config-sbc-sbe-rsrc-pri-set)# resource-priority dsn.flash
```

# response-code-mapping

To define a response code map, use the **response-code-mapping** command in SIP method-profile configuration mode. The **no** form of this command removes all mappings.

**response-code-mapping** *map*

**no response-code-mapping** *map*

<b>Syntax Description</b>	<p><b>map</b> Specifies a list of SIP response codes and the value that they will be mapped to as follows:</p> <ul style="list-style-type: none"> <li>Response code 100: mapping not allowed.</li> <li>Response code 1xx: Maps to 1yy.</li> <li>Response code 2xx maps to 2yy.</li> <li>Response code 3xx maps to 3yy.</li> <li>Response code 4xx maps to 4yy, 5yy, or 6yy.</li> <li>Response code 5xx maps to 4yy, 5yy, or 6yy</li> <li>Response code 6xx maps to 4yy, 5yy, or 6yy</li> </ul>
---------------------------	--

**Command Default** No response code mapping.

**Command Modes** SIP method-profile configuration (config-sbc-sbe-sip-mth)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example defines a response code map:

```

Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile Myprofile
Router(config-sbc-sbe-sip-mth)# response-code-mapping maptest

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	sip method-profile	Configures a method-profile.

# retry-count

To configure the number of times the Cisco Unified Border Element (SP Edition) repeats the provisioned delegate registration processing after the retry interval ends, use the **retry-count** command in subscriber delegate profile configuration mode. To reset the retry count time to the default retry count time, use the **no retry-count** command.

```
retry-count {#times to retry}
```

```
no retry-count {#times to retry}
```

<b>Syntax Description</b>	<i>#times to retry</i>	the number of times the SBC repeats the delegate registration processing after the retry interval ends. The default is 3 times. The range is 0 to 255 times.
---------------------------	------------------------	--

<b>Command Default</b>	The default number of retries is 3 times.
------------------------	---

<b>Command Modes</b>	Subscriber delegate profile configuration mode (config-sbc-sbe-subscriber-delegate-prof)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	Configures the number of times the Cisco Unified Border Element (SP Edition) repeats the delegate registration processing after the retry interval ends. The default is 3 times. This is one of the delegate profile parameters you can configure.
-------------------------	--

After a delegate profile is configured, the following profile parameters may optionally be configured:

- duration
- retry-count
- retry-interval
- refresh-buffer

<b>Examples</b>	The following example configures a provisioned delegate registration profile that can be applied to a delegate registration subscriber and configures a delegate registration for delegate client (aor=sip:bob@isp.example). The delegate registration profile is configured with a duration expiration time of 1000 seconds, a retry count of 5 times, a retry interval of 60 seconds, and a refresh timeout time of 200 seconds:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# delegate-profile my-profile
```

```

Router(config-sbc-sbe-subscriber-delegate-prof)# duration 1000
Router(config-sbc-sbe-subscriber-delegate-prof)# retry-count 5
Router(config-sbc-sbe-subscriber-delegate-prof)# retry-interval 60
Router(config-sbc-sbe-subscriber-delegate-prof)# refresh-buffer 200
Router(config-sbc-sbe-subscriber-delegate-prof)# exit
Router(config-sbc-sbe)# subscriber sip:bob@isp.example
Router(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
Router(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
Router(config-sbc-sbe-subscriber-contact)# exit
Router(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
Router(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
Router(config-sbc-sbe-subscriber-delegate)# profile my-profile
Router(config-sbc-sbe-subscriber-delegate)# activate
Router(config-sbc-sbe-subscriber-delegate)# end

```

**Related Commands**

Command	Description
<b>duration</b>	Configures the length of time in seconds during which the SBC tries to perform delegate registration before stopping.
<b>retry-interval (registration)</b>	Configures the length of time the SBC waits before it retries delegate registration.
<b>refresh-buffer</b>	Configures the length of time by which the SBC attempts to refresh the address location with a delegate registration before the specified expiration time.
<b>delegate-profile</b>	Configures a delegate registration profile that is applied to a delegate registration subscriber.
<b>delegate-registration</b>	Configures a delegate registration for a delegate client.
<b>show sbc sbe sip delegate-profile</b>	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.

# retry-interval

To set the interval for resending an accounting request to the Radius server, use the **retry-interval** command in SBE accounting mode. To set the interval to its default, use the **no** form of this command.

**retry-interval** *range*

**no** **retry-interval** *range*

<b>Syntax Description</b>	<i>range</i>	Range is 10-10000 ms.
---------------------------	--------------	-----------------------

<b>Command Default</b>	1200 ms
------------------------	---------

<b>Command Modes</b>	Server accounting (config-sbc-sbe-acc-ser) Server authentication (config-sbc-sbe-auth)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to set the <b>retry-interval</b> to 1000 ms.
-----------------	--

```
Router# configure
Router(config)# sbc uut105-1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting SBC1-account-1
Router(config-sbc-sbe-acc)# retry-interval 1000
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>retry-limit</b>	Sets the retry interval to the RADIUS server.
	<b>concurrent-requests</b>	Sets the maximum number of concurrent requests to the RADIUS server.
	<b>activate</b>	Activates the RADIUS client.

# retry-interval (registration)

To configure the length of time the Cisco Unified Border Element (SP Edition) waits before it retries provisioned delegate registration, use the **retry-interval** command in subscriber delegate profile configuration mode. To reset the retry interval to the default retry interval, use the **no retry-interval** command.

**retry-interval** *{retry time in secs}*

**no retry-interval** *{retry time in secs}*

## Syntax Description

<i>retry time in secs</i>	This is the length of time before the delegate registration processing is retried after the retry interval ends. The range is 1 to 2,147,483 seconds. The default is 30 seconds.
---------------------------	--

## Command Default

The default retry time is 30 seconds.

## Command Modes

Subscriber delegate profile configuration mode (config-sbc-sbe-subscriber-delegate-prof)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Configures the length of time the SBC waits before it retries delegate registration after the retry interval ends. The default is 30 seconds. This is one of the delegate profile parameters you can configure.

After a delegate profile is configured, the following profile parameters may optionally be configured:

- duration
- retry-count
- retry-interval
- refresh-buffer

## Examples

The following example configures a provisioned delegate registration profile that can be applied to a delegate registration subscriber and configures a delegate registration for delegate client (aor=sip:bob@isp.example). The delegate registration profile is configured with a duration expiration time of 1000 seconds, a retry count of 5 times, a retry interval of 60 seconds, and a refresh timeout time of 200 seconds:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# delegate-profile my-profile
Router(config-sbc-sbe-subscriber-delegate-prof)# duration 1000
Router(config-sbc-sbe-subscriber-delegate-prof)# retry-count 5
```



```

Router(config-sbc-sbe-subscriber-delegate-prof)# retry-interval 60
Router(config-sbc-sbe-subscriber-delegate-prof)# refresh-buffer 200
Router(config-sbc-sbe-subscriber-delegate-prof)# exit
Router(config-sbc-sbe)# subscriber sip:bob@isp.example
Router(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
Router(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
Router(config-sbc-sbe-subscriber-contact)# exit
Router(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
Router(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
Router(config-sbc-sbe-subscriber-delegate)# profile my-profile
Router(config-sbc-sbe-subscriber-delegate)# activate
Router(config-sbc-sbe-subscriber-delegate)# end

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>duration</b>	Configures the length of time in seconds during which the SBC tries to perform delegate registration before stopping.
<b>retry-count</b>	Configures the number of times the SBC repeats the delegate registration processing after the retry interval ends.
<b>refresh-buffer</b>	Configures the length of time by which the SBC attempts to refresh the address location with a delegate registration before the specified expiration time.
<b>delegate-profile</b>	Configures a delegate registration profile that is applied to a delegate registration subscriber.
<b>delegate-registration</b>	Configures a delegate registration for a delegate client.
<b>show sbc sbe sip delegate-profile</b>	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.

# retry-limit (radius)

To set the number of times for resending an accounting request to the Radius server, use the **retry-limit** command in SBE accounting mode. To set the number to its default, use the **no** form of this command.

**retry-limit** *range*

**no** *retry-limit range*

<b>Syntax Description</b>	<b>range</b>	Range for the maximum number of retries is 0-9.
---------------------------	--------------	---

<b>Command Default</b>	5 retries.	
------------------------	------------	--

<b>Command Modes</b>	Server accounting (config-sbc-sbe-acc) Server authentication (config-sbc-sbe-auth)	
----------------------	---	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	<p>The following example shows how to set the retry-limit to 4 attempts.</p> <pre>Router# <b>configure terminal</b> Router(config)# <b>sbc uut105-1</b> Router(config-sbc)# <b>sbe</b> Router(config-sbc-sbe)# <b>radius accounting SBC1-account-1</b> Router(config-sbc-sbe-acc)# <b>retry-limit 4</b></pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>retry-interval</b>	Sets the retry interval to connect to the RADIUS server.
	<b>concurrent-requests</b>	Sets the maximum number of concurrent requests to the RADIUS server.
	<b>activate</b>	Activates the RADIUS client.

## retry-limit (routing table)

To set the maximum number of routing table lookup retry attempts, use the **retry-limit** command in SBE configuration mode. To set the number to its default, use the **no** form of this command.

**retry-limit 0-200**

<b>Syntax Description</b>	<b>0-200</b>	Range for the maximum number of retries is 0-200.
---------------------------	--------------	---

<b>Command Default</b>	3 retries.
------------------------	------------

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to set the <b>retry-limit to 4 attempts</b> .
-----------------	---

```
Router# configure terminal
Router(config)# sbc uut105-1
Router(config-sbc)# sbe
Router(config-sbc-sbe)# retry-limit 4
```

## rf

To create a new Rf billing instance on the Session Border Element (SBE), use the **rf** command in the SBC SBE billing configuration mode. To delete a new Rf billing instance on the SBE, use the **no** form of this command.

**rf** *index*

**no rf** *index*

<b>Syntax Description</b>	<i>index</i>	Unique index for a billing instance. Range: 0 to 7.
---------------------------	--------------	---

<b>Command Default</b>	None	
------------------------	------	--

<b>Command Modes</b>	SBC SBE billing configuration (config-sbc-sbe-billing)	
----------------------	--	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to enable Rf support for index 0 on the SBE of the Cisco Session Border Controller (SBC):

```
Router> enable
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# billing
Router(config-sbc-sbe-billing)# rf 0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>origin-host (session border controller)</b>	Specifies the domain name of an origin host for Rf support on the SBE of the SBC.
<b>origin-realm (session border controller)</b>	Specifies the domain name of an origin realm for Rf support on the SBE of the SBC.	

# rtcp-mux

To configure the detection of RTCP streams multiplexed with RTP streams (or SRTCP streams multiplexed with SRTP streams), use the **rtcp-mux** command in the SBE configuration mode. To disable this feature, use the **no** form of the command.

**rtcp-mux**

**no rtcp-mux**

**Syntax Description** *This command has no arguments or keywords.*

**Command Default** *By default, the detection of RTCP streams multiplexed with RTP streams is disabled. The same applies to SRTCP streams multiplexed with SRTP streams.*

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

**Examples** The following example shows how to configure the detection of RTCP streams multiplexed with RTP streams using the **rtcp-mux** command. The same applies to SRTCP streams multiplexed with SRTP streams.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# rtcp-mux
```

Related Commands	Command	Description
	<b>sbe</b>	Enters the SBE configuration mode.

# rtcp-regenerate

To generate and terminate the RTCP packets on the SPA-DSP, use the **rtcp-regenerate** command in the SBC configuration mode for the Cisco Unified Border Element: Unified Model, and from the SBC DBE configuration mode for the Cisco Unified Border Element: Distributed Model.

**rtcp-regenerate**

**no rtcp-regenerate**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBC configuration (config-sbc) for the Unified Model  
SBC DBE configuration (config-sbc-dbe) for the Distributed Model

Command History	Release	Modification
	Cisco IOS XE Release 3.4.0S	This command was introduced.

**Usage Guidelines** Use this command to generate and terminate the RTCP packets on the SPA-DSP on a Cisco ASR 1000 Series Router.

**Examples** The following example shows how to generate and terminate the RTCP packets on the SPA-DSP on the Unified Model:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# rtcp-regenerate
```

The following example shows how to generate and terminate the RTCP packets on the SPA-DSP on the Distributed Model:

```
Router# configure terminal
Router(config)# sbc mySBC db
```

# rtg-carrier-id-table

To enter the configuration mode of a routing table or to create a new routing table, whose events match the carrier ID of an SBE policy set, use the **rtg-carrier-id-table** command in SBE call policy set mode.

The **no** form of the command destroys the routing table. However, a routing table may not be destroyed if it is in the context of the active policy set.

**rtg-carrier-id-table** *table-name*

**no rtg-carrier-id-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the routing table to be configured.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to add the carrier ID table MyCarrierIDTable:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-carrier-id-table MyCarrierIDTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-round-robin-table</b>	Enters the configuration mode of a policy table, with events that have no match-value parameters or next-table actions.
	<b>rtg-src-account-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source account.
	<b>rtg-src-adjacency-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source adjacency.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.



## rtg-category-table

To enter the mode of configuration of a routing table whose entries match on the category within the context of an SBE policy set, use the **rtg-category-table** command in SBE routing call policy mode.

The **no** form of the command destroys the routing table. However, a routing table may not be destroyed if it is in the context of the active policy set.

**rtg-category-table** *WORD*

**no rtg-category-table** *WORD*

<b>Syntax Description</b>	<i>WORD</i>	Name of the routing table to be configured.  The <i>WORD</i> field can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------------	-------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE routing policy (config-sbc-sbe-rtgpolicy)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	If necessary, a new routing table is created. The user is not allowed to enter the mode of routing table configuration in the context of the active policy set.
-------------------------	---

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

<b>Examples</b>	The following example creates the routing policy table MyRtgTable:
-----------------	--

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-category-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-round-robin-table</b>	Enters the configuration mode of a policy table, with events that have no match-value parameters or next-table actions.
	<b>rtg-src-account-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source account.
	<b>rtg-src-adjacency-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source adjacency.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.

# rtg-dst-address-table

To enter the configuration mode of a routing table whose entries match on the dialed number (after number analysis) within the context of an SBE policy set, use the **rtg-dst-address-table** command in the SBE routing policy mode. To remove the routing table, use the **no** form of this command.

**rtg-dst-address-table** *table-id*

**no rtg-dst-address-table** *table-id*

## Syntax Description

<i>table-id</i>	Specifies the name of the table.  The <i>table-id</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

If necessary, a new routing table is created. The user is not allowed to enter the mode of routing table configuration in the context of the active policy set.

A routing table may not be destroyed if it is in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command creates the routing policy table MyRtgTable:

```
Router# configure
Router(config)# sbc mySbc sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-carrier-id-table</b>	Enters the configuration mode for creation or configuration of a routing table, with entries that match the carrier ID of an SBE call policy set.
	<b>rtg-src-domain-table</b>	Enters the configuration mode for creation or configuration of a routing table, with entries that match the source domain name of an SBE call policy set.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.

# rtg-dst-domain-table

To enter the configuration mode of a routing table with entries that match the destination domain name of an SBE policy set, use the **rtg-dst-domain-table** command in SBE call policy set mode. If no table exists, the command creates a new routing table.

The **no** form of the command deletes the routing table.

**rtg-dst-domain-table** *table-name*

**no rtg-dst-domain-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the routing table to be configured.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

You cannot delete a routing table if it is in the active policy set. You cannot enter the mode of a routing table configuration in the active policy set.

## Examples

The following command creates the routing policy table *MyRtgTable*.

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-domain-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
<b>rtg-carrier-id-table</b>	Enters the configuration mode for creation or configuration of a routing table, with entries that match the carrier ID of an SBE call policy set.
<b>rtg-src-domain-table</b>	Enters the configuration mode for creation or configuration of a routing table, with entries that match the source domain name of an SBE call policy set.
<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.

# rtg-dst-trunk-group-id-table

To enter the configuration mode of an existing routing table or to create a new table whose entries match the destination TGID or TGID context parameters of an SBE policy set, use the **rtg-dst-trunk-group-id-table** command in SBE call policy set mode. Use the **no** form of this command to delete the routing table.

**rtg-dst-trunk-group-id-table** *table-id*

**no rtg-dst-trunk-group-id-table** *table-id*

<b>Syntax Description</b>	<i>table-id</i>	ID of the routing table to be configured.  The <i>table-id</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------------	-----------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE routing policy (config-sbc-sbe-rtgpolicy)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following command creates a new table, MyRtgTable, whose entries match the destination TGID or TGID context parameters.
-----------------	---

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# tgid-routing
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-trunk-group-id-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>rtg-src-trunk-group-id-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the source TGID or TGID context parameters of an SBE policy set.
	<b>tgid-routing</b>	Enables parsing the trunk-group identifier for call routing.



# rtg-least-cost-table

To configure the least-cost routing table and enter the mode of configuration of a routing table, use the *rtg-least-cost-table* command in SBE routing policy mode.

The **no** form of the command destroys the routing table. However, a routing table may not be destroyed if it is in the context of the active policy set.

*rtg-least-cost-table table\_name*

**no** *rtg-least-cost-table table\_name*

## Syntax Description

<i>table-name</i>	Name of the routing table to be configured.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

If necessary, a new routing table is created. The user is not allowed to enter the mode of routing table configuration in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command creates the routing policy table MyRtgTable:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-least-cost-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-round-robin-table</b>	Enters the configuration mode of a policy table, with events that have no match-value parameters or next-table actions.
	<b>rtg-src-account-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source account.
	<b>rtg-src-adjacency-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source adjacency.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.

# rtg-round-robin-table

To enter the configuration mode of a policy table, whose events have no match-value parameters or next-table actions, use the **rtg-round-robin-table** command SBE call policy set mode. Use the **no** form of this command to delete the table.

**rtg-round-robin-table** *table-name*

**no rtg-round-robin-table** *table-name*

## Syntax Description

<i>table-name</i>	Name of the routing table to be configured.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The actions of this command are restricted to setting destination adjacency. A group of adjacencies is chosen for an event if an entry in a routing table matches that event and points to a round-robin adjacency table in the next table action.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example show how to add the round robin routing table MyRoundRobinTable:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-round-robin-table MyRoundRobinTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-src-adjacency-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source adjacency.
	<b>rtg-carrier-id-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the carrier ID of an SBE policy set.
	<b>rtg-src-account-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source account.

# rtg-src-account-table

To enter the configuration mode of an existing routing table or to create a new one, with entries that match the source account, use the **rtg-src-account-table** command SBE call policy set mode.



## Note

You cannot issue this command if the table is part of the active policy set.

The **no** form of the command deletes the match value of the given entry in the routing table.

**rtg-src-account-table** *table-id*

**no rtg-src-account-table** *table-id*

## Syntax Description

<i>table-id</i>	Specifies the ID of the routing table to be configured.  The <i>table-id</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command enters the configuration mode of an existing routing table MyRtgTable:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-account-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-src-adjacency-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source adjacency.
	<b>rtg-round-robin-table</b>	Enters the configuration mode of a policy table, with events that have no match-value parameters or next-table actions.
	<b>rtg-carrier-id-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the carrier ID of an SBE policy set.

# rtg-src-address-table

To enter the configuration mode of a routing table whose entries match on the dialer's number within the context of an SBE policy set, use the **rtg-src-address-table** command in SBE routing policy mode. To remove the table entry, use the **no** form of this command.

**rtg-src-address-table** *table-id*

**no rtg-src-address-table** *table-id*

## Syntax Description

<i>table-id</i>	Specifies the name of the table.  The <i>table-id</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command creates the routing policy table MyRtgTable:

```
Router# configure
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# exit
Router(config-sbc-sbe-rtgpolicy)# exit
```

## Related Commands

Command	Description
<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, enters the configuration mode of an existing service.

<b>Command</b>	<b>Description</b>
<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
<b>rtg-src-account-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the source account
<b>rtg-round-robin-table</b>	Enters the configuration mode of a policy table whose events have no match-value parameters or next-table actions.



# rtg-src-adjacency-table

To enter the configuration mode of an existing routing table or to create a new table whose entries match the source adjacency, use the **rtg-src-adjacency-table** command in SBE call policy set mode. Use the **no** form of this command to delete the routing table.

**rtg-src-adjacency-table** *table-id*

**no rtg-src-adjacency-table** *table-id*

## Syntax Description

<i>table-id</i>	Specifies the ID of the routing table to be configured.  The <i>table-id</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command creates a new table, MyRtgTable, whose entries match the source adjacency.

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-adjacency-table MyRtgTable
```

## Related Commands

Command	Description
<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, enters the configuration mode of an existing service.
<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.

<b>Command</b>	<b>Description</b>
<b>rtg-src-account-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the source account
<b>rtg-round-robin-table</b>	Enters the configuration mode of a policy table whose events have no match-value parameters or next-table actions.

# rtg-src-domain-table

To enter the mode of a routing table configuration, with entries that match the source domain name, use the **rtg-src-domain-table** command in SBE call policy set mode. If no table exists, the command creates a new routing table.



## Note

You cannot enter the mode of a routing table configuration in the active policy set.

The **no** form of the command destroys the routing table.



## Note

You cannot destroy a routing table if it is in the active policy set.

**rtg-src-domain-table** *table-name*

**no rtg-src-domain-table** *table-name*

## Syntax Description

*table-name*

Name of the number analysis table within an SBE policy set, with entries matching the source account.

The *table-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

**Note** Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command creates the routing policy table *MyRtgTable*.

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-domain-table MyRtgTable
```

Router(config-sbc-sbe-rtgpolicy-rtgtable)#

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-dst-domain-table</b>	Enters the configuration submode for creation or configuration of a routing table, with entries that match the destination domain name of an SBE call policy set.
	<b>rtg-carrier-id-table</b>	Enters the configuration mode for creation or configuration of a routing table, with entries that match the carrier ID of an SBE call policy set.

# rtg-src-trunk-group-id-table

To enter the configuration mode of an existing routing table or to create a new table whose entries match the source TGID or TGID context parameters of an SBE policy set, use the **rtg-src-trunk-group-id-table** command in SBE call policy set mode. Use the **no** form of this command to delete the routing table.

**rtg-src-trunk-group-id-table** *table-id*

**no rtg-src-trunk-group-id-table** *table-id*

## Syntax Description

<i>table-id</i>	ID of the routing table to be configured.  The <i>table-id</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command creates a new table, MyRtgTable, whose entries match the source TGID or TGID context parameters.

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# tgid-routing
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-src-trunk-group-id-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>rtg-dst-trunk-group-id-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the destination TGID or TGID context parameters of an SBE policy set.
	<b>tgid-routing</b>	Enables parsing the trunk-group identifier for call routing.

# rtg-time-table

To configure time-based routing and enter the routing table mode, use the *rtg-time-table* command in SBE routing call policy mode.

The **no** form of the command destroys the routing table. However, a routing table may not be destroyed if it is in the context of the active policy set.

*rtg-time-table table\_name*

**no** *rtg-time-table table\_name*

## Syntax Description

<i>table-name</i>	Name of the routing table to be configured.  The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-------------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE routing policy (config-sbc-sbe-rtgpolicy)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

If necessary, a new routing table is created. The user is not allowed to enter the mode of routing table configuration in the context of the active policy set.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command creates the routing policy table MyRtgTable:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-time-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# end
```



<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>rtg-round-robin-table</b>	Enters the configuration mode of a policy table, with events that have no match-value parameters or next-table actions.
	<b>rtg-src-account-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source account.
	<b>rtg-src-adjacency-table</b>	Enters the configuration mode of an existing routing table or creates a new one, with entries that match the source adjacency.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, it enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.

# sbc

To enter the mode of an SBC service (creating it if necessary), use the **sbc** command in the SBC configuration mode. To delete the service, use the **no** form of this command.

```
sbc sbc-name
```

```
no sbc sbc-name
```

## Syntax Description

sbc-name Name of the SBC service.

The *sbc-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

**Note** Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBC configuration mode (config-sbc)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for the unified model.

## Examples

The following command creates SBC service mySbc.

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc)# exit
```

## Related Commands

Command	Description
<b>dbe</b>	Enters into DBE-SBE configuration mode.

# sbc dbe

To create the data border element (DBE) service on a session border controller (SBC) and enter into the SBC-DBE configuration mode, use the **sbc dbe** command in global configuration mode. To remove the DBE entity, use the **no** form of this command.

```
sbc {sbc-name} dbe
```

```
no sbc {sbc-name} dbe
```

<b>Syntax Description</b>	<i>sbc-name</i>	The SBC service name.
---------------------------	-----------------	-----------------------

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example creates a DBE service on an SBC called “mySbc,” and enters into SBC-DBE configuration mode:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>interface sbc</b>	Creates the session border controller (SBC) interface.

# sbc dump-alarms

To move alarm logs from the buffer to a file system, use the **sbc dump-alarms** command in privileged EXEC mode.

```
sbc dump-alarms [file-system]
```

<b>Syntax Description</b>	<i>file-system</i>	<p>Name of the file system to which you want the alarm logs to be moved. For example, <i>file-system</i> can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>bootflash:</b></li> <li>• <b>flash:</b></li> <li>• <b>fpd:</b></li> <li>• <b>ftp:</b></li> <li>• <b>http:</b></li> <li>• <b>https:</b></li> <li>• <b>obfl:</b></li> <li>• <b>pram:</b></li> <li>• <b>rcp:</b></li> <li>• <b>scp:</b></li> <li>• <b>tftp:</b></li> </ul> <p><b>Note</b> If you do not specify a file system, the alarm logs are moved to the default file system.</p>
---------------------------	--------------------	--

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 3.5S</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	<p>The following is the naming convention for the log file that is generated when you run the <b>sbc dump-alarms</b> command:</p>
-------------------------	---

```
yyyymmdd_hhmmss_manual_alarmtrc.log
```

<b>Examples</b>	<p>The following example show how the <b>sbc dump-alarms</b> command is used to move alarm logs to the bootflash file system:</p>
-----------------	---

```
Router# sbc dump-alarms bootflash:
```

The following is the name of a sample log file that is generated when the **sbc dump-alarms** command is run on 12-May-2011 at 04:34:31:

20110512\_043431\_manual\_alarmtrc.log

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug sbc alarm-filter</b>	Specifies the alarm types for which alarm logs must be generated.
<b>debug sbc alarm-log-level</b>	Specifies the output mode for and the alarm severity level at which alarms must be logged.
<b>sbc periodic-dump-alarms</b>	Configures periodic movement of alarm logs from the buffer to a file system.
<b>show debugging</b>	Displays information about the types of debugging that are enabled for the router.

# sbc periodic-dump-alarms

To configure periodic movement of alarm logs from the buffer to a file system, use the **sbc periodic-dump-alarms** command in the privileged EXEC mode.

```
sbc periodic-dump-alarms {dump-location file-system [time-period time-period] | time-period
time-period}
```

Syntax	Description
<b>dump-location</b>	Specifies that you want the alarm logs to be stored in a file system. If you do not specify the dump location, the alarm logs are moved to the default file system.
<i>file-system</i>	Name of the file system where you want the alarm logs to be moved. For example, <i>file-system</i> can be one of the following: <ul style="list-style-type: none"> <li>• <b>bootflash:</b></li> <li>• <b>flash:</b></li> <li>• <b>fpd:</b></li> <li>• <b>ftp:</b></li> <li>• <b>http:</b></li> <li>• <b>https:</b></li> <li>• <b>obfl:</b></li> <li>• <b>pram:</b></li> <li>• <b>rcp:</b></li> <li>• <b>scp:</b></li> <li>• <b>tftp:</b></li> </ul>
<b>time-period</b>	Specifies that you want the logs to be moved to a file system at periodic intervals.
<i>time-period</i>	Interval, in minutes, after which the logs must be moved. The range is from 0 to 1440. The default is 60.

**Command Default** The default is that alarm logs are moved to the default file system at 60-minute intervals.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

The buffer that is used to store alarm logs may run out of free space when log files are stored in it. In addition, you may want to store alarm logs for future reference. Use the **sbc periodic-dump-alarms** command to meet the requirements created by this scenario. Use the **sbc periodic-dump-alarms time-period 0** command if you want to disable the periodic movement of alarm logs from the buffer to a file system.

**Examples**

In the following example, the **sbc periodic-dump-alarms** command is used to specify that the logs must be moved to the bootflash file system at 120-minute intervals:

```
Router# sbc periodic-dump-alarms dump-location bootflash: time-period 120
```

The following is the naming convention for the log file that is generated:

```
yyyymmdd_hhmmss_periodic_alarmtrc.log
```

The following is the name of a sample log file that is generated when the **sbc periodic-dump-alarms** command is used to configure periodic dumping of log files at 1-hour intervals:

```
20110512_080005_periodic_alarmtrc.log
```

**Related Commands**

Command	Description
<b>debug sbc alarm-filter</b>	Specifies the alarm types for which alarm logs must be generated.
<b>debug sbc alarm-log-level</b>	Specifies the output mode for and the alarm severity level at which alarms must be logged.
<b>sbc dump-alarms</b>	Moves alarm logs from the buffer to a file system.
<b>show debugging</b>	Displays information about the types of debugging that are enabled for the router.

# sbc redundancy-group tcp (session border controller)

To assign a redundancy group for the Session Border Controller (SBC) to track, use the **sbc redundancy-group tcp** command in the global configuration mode. To unassign a redundancy group, use the **no** form of this command.

**sbc redundancy-group** *group-number* **tcp**

**no sbc redundancy-group** *group-number* **tcp**

## Syntax Description

<i>group-number</i>	The redundancy group number.
<b>tcp</b>	Specifies the Transmission Control Protocol (TCP), and the redundancy group protocol.

## Command Default

No default behavior or values are available.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to assign an redundancy group for the SBC to track:

```
Router# configure terminal
Router# sbc redundancy-group 1 tcp
```



# sc-cold-boot-delay

To configure a delay timer that delays generation of a ServiceChange coldBoot request, use the **sc-cold-boot-delay** command in VDBE configuration mode.

The **no** form of the command turns off the cold boot delay timer on the next reboot.

**sc-cold-boot-delay** *delay*

**no sc-cold-boot-delay** *delay*

## Syntax Description

<i>delay</i>	Specifies the delay in seconds, 0 through 1200 seconds.
--------------	---

## Command Default

No default behavior or values are available.

## Command Modes

VDBE configuration mode (config-sbc-dbe-vdbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers for distributed Session Border Controller (SBC).

## Usage Guidelines

This command is supported in distributed SBC. This command configures a delay timer that delays generation of the Service Change Cold Boot after SBC has started with the **activate** command. The delay of the Service Change Cold Boot can only occur while the system is booting. This delay allows SBC to start up and be ready to respond to a large number of SIP pinhole requests that will be initiated by the ServiceChange ColdBoot.

To disable the delay Service Change Cold Boot timer, you must issue the **no activate** command followed by an **activate** command to attach to the MGC immediately. The **no sc-cold-boot-delay** command is used to make sure that the delayed SC mode doesn't occur on the next reboot.

Use the **show sbc dbe controllers** command to display the configured delay and the time remaining before the Service Change will be issued.

## Examples

The following command describes a DBE configuration where a delay timer is configured to 120 seconds to delay generation of a ServiceChange coldBoot request:

```
Router# configure terminal
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# local-port 2970
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.40
Router(config-sbc-dbe-vdbe)# controller h248 2
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254
```

```

Router(config-sbc-dbe-vdbe-h248)# remote-port 2970
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers
Router(config-sbc-dbe-vdbe)# sc-cold-boot-delay 120
Router(config-sbc-dbe-vdbe)# exit
Router(config-sbc-dbe)# activate

```

The following example shows that the configured activation delay is 112 seconds, which is the time remaining before the Service Change is issued, and the controller status is detached.

```

Router# show sbc global dbe controllers
SBC Service "global"
  vDBE in DBE location 1

  DBE Admin Status:      Activation Delayed 112 seconds
  Media gateway controller in use:
    H.248 controller address
      200.50.1.254:2970
    Status:      Detached

                                Sent          Received      Failed

Retried
  Requests      1           0           0           1
  Replies       0           0           0           0

Segmentation:
  MGC PDU Size:  N/A
  MG PDU Size:   N/A
  MGC Seg timer: N/A
  MG Seg timer:  N/A
  Segments Sent: N/A
  Segments Rcvd: N/A

Configured controllers:
  H.248 controller 2:

```

## Related Commands

Command	Description
<b>activate</b>	To initiate the DBE service of the SBC.
<b>show sbc dbe controllers</b>	Lists the MGCs and controller address configured on each DBE.

## sck-pool-size

To configure the buffer size of a Session Initiation Protocol (SIP) socket control, use the **sck-pool-size** command in the SBE configuration mode. To reconfigure the buffer size of the SIP socket control to the default value, use the **no** form of this command.

**sck-pool-size** *pool\_size*

**no sck-pool-size** *pool\_size*

<b>Syntax Description</b>	<i>pool_size</i>	Pool size number. The range is from 1 to 65535. The default is 400.
---------------------------	------------------	---

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	SBE configuration mode
----------------------	------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS Release 15.2(04)S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to configure the buffer size of an SIP socket control:

```
Router> enable
Router# configure terminal
Router(config)# sbc 123
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sck-pool-size 23
```

# script-set lua

To configure a script set composed of scripts written using the Lua programming language, use the **script-set** command in the SBE configuration mode. To remove the configuration of the script set, use the **no** form of this command.

**script-set** *script-set-number* **lua**

**no script-set** *script-set-number*

## Syntax Description

<i>script-set-number</i>	Specifies the script set number.
--------------------------	----------------------------------

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **script-set** command is used to configure a script set with the script order number 10:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# script-set 10 lua
```

## Related Commands

Command	Description
<b>active-script-set</b>	Activates a script set,
<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.

<b>Command</b>	<b>Description</b>
<b>editor</b>	Specifies the order in which a particular editor must be applied.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# script

To configure a script written using the Lua programming language, use the **script** command in the SBE script-set configuration mode. To remove the configuration of the script, use the **no** form of this command.

**script** *script-name*

**no script** *script-name*

## Syntax Description

<i>script-name</i>	Specifies the name of the script.  The <i>script-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
--------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE script-set configuration (config-sbc-sbe-script-set)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **script** command is used to configure a script file with the name mySBCScript:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# script-set 10 lua
Router(config-sbc-sbe-script-set)# script mySBCScript
```

Related Commands	Command	Description
	<b>active-script-set</b>	Activates a script set,
	<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
	<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
	<b>editor</b>	Specifies the order in which a particular editor must be applied.
	<b>editor-list</b>	Specifies the stage at which the editors must be applied.
	<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
	<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
	<b>load-order</b>	Specifies the load order of a script in a script set.
	<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
	<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
	<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
	<b>sip header-editor</b>	Configures a header editor.
	<b>sip method-editor</b>	Configures a method editor.
	<b>sip option-editor</b>	Configures an option editor.
	<b>sip parameter-editor</b>	Configures a parameter editor.
	<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
	<b>test script-set</b>	Tests the working of a script set.
	<b>type</b>	Specifies the type of a script written using the Lua programming language.

# sdp repeat answer

To configure SBC to repeat an agreed Session Description Protocol (SDP), in a 200 INVITE response, after the successful provisioning of an offer-answer exchange when needed, use the **sdp repeat answer** command in CAC table entry configuration mode. To restore the default, where agreed SDPs are not repeated, use the no form of this command.

**sdp repeat answer**

**no sdp repeat answer**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, an agreed SDP in a 200 INVITE response is not repeated.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the repeat of an Session Description Protocol (SDP), in a 200 INVITE response, after the successful provisioning of an offer-answer exchange:

```
Router# configure terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table cac-tbl-1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# sdp repeat answer
```



# secure-media

To configure the Session Border Controller (SBC) to enable a DTLS or SRTP media passthrough, use the **secure-media** command in the SBE configuration mode. To disable the media passthrough, use the no form of this command.

**secure-media**

**no secure-media**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The media passthrough is disabled.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example configures the SBC to treat every media flow as an encrypted media flow. This allows media packets, such as DTLS and SRTP packets, to pass through the SBC.

```
Router# configure terminal
Router(config)# sbc global
Router(config-sbc)# sbe
Router(config-sbc-sbe)# secure-media
```

Related Commands	Command	Description
	<b>sbc</b>	Creates the SBC service on Cisco Unified Border Element (SP Edition).
	<b>sbe</b>	Enters the mode of the signaling border element (SBE) function of the SBC.

# security (session border controller)

To implement transport-level security on a Session Initiation Protocol (SIP) adjacency, use the **security** command in SBE adjacency SIP configuration mode. To indicate that the adjacency cannot be secured, use the **no** form of this command.

*security [untrusted | trusted-encrypted | untrusted-encrypted | trusted-unencrypted]*

*no security [untrusted | trusted-encrypted | untrusted-encrypted | trusted-unencrypted]*

## Syntax Description

<i>untrusted</i>	Specifies that this adjacency is not secured by any means. This is the default.
<i>trusted-encrypted</i>	Specifies that the encrypted signaling is used to ensure security on this adjacency.
<i>untrusted-encrypted</i>	Specifies that the adjacency is untrusted and SSL/TLS encryption is used.
<i>trusted-unencrypted</i>	Specifies that a non-encryption mechanism is used to guarantee secure signaling for all messages on this adjacency.

## Command Default

untrusted is the default.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Any number of accounting servers can be specified. Call Detail Reports are sent to the accounting server with the highest priority upon call termination.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command configures accounting servers castor and pollux on mySbc for RADIUS client instance radius1:

```
Router# configure
Router(config)# sbc mySbc
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip adjacency test
Router(config-sbc-sbe-adj-sip)# security trusted-encrypted
```

# server-retry disable

To disable the SBC from automatically retrying a failed RADIUS server, use the **server-retry disable** command in the server authentication mode or the server accounting mode. Use the **no** form of this command to enable the SBC to automatically retry a failed RADIUS server.

**server-retry disable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Server accounting (config-sbc-sbe-acc)  
Server authentication (config-sbc-sbe-auth)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If you have disabled the SBC from automatically retrying a failed RADIUS server with the **server-retry disable** command, you must use the **service sbc sbe radius accounting** command to reactivate the connection between the SBC and a RADIUS server after connectivity is lost or to restart billing after connectivity is restored.

**Examples** The following example shows how to stop the SBC from automatically retrying a failed RADIUS server:

```
Router# configure
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius authentication
Router(config-sbc-sbe-auth)# server-retry disable
```

Related Commands	Command	Description
	<b>service sbc sbe radius accounting</b>	Reactivates connection between the SBC and a RADIUS server after connectivity is lost or to restart billing after connectivity is restored.

# server ipv4

To configure the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF, use the **server ipv4** command in ENUM entry configuration mode. To remove IPv4 address of a DNS server for ENUM client, use the no form of this command.

```
server ipv4 ip_address [vrf vrf_name]
```

```
no server ipv4 ip_address [vrf vrf_name]
```

## Syntax Description

<i>ip_address</i>	Specifies the IPv4 address in standard format: <i>A.B.C.D</i> .
<b>vrf</b> <i>vrf_name</i>	(Optional) Specifies the VRF for the DNS server.

## Command Default

No default behavior or values are available.

## Command Modes

ENUM entry configuration (config-sbc-sbe-enum-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the IPv4 address of a DNS server for ENUM client and associate the DNS server to a VRF:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# enum 1
Router(config-sbc-sbe-enum)# entry ENUM_1
Router(config-sbc-sbe-enum-entry)# server ipv4 10.10.10.10 vrf VRF1
Router(config-sbc-sbe-enum-entry)#
```

## Related Commands

Command	Description
<b>activate (enum)</b>	Activates ENUM client.
<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).

<b>Command</b>	<b>Description</b>
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

# server (session border controller)

To enter a mode for configuring ordered lists of RADIUS accounting and RADIUS authentication servers, use the **server** command in server accounting and server authentication configuration modes. Use the **no** form of the command to leave the mode.

*server server-name*

*no server server-name*

## Syntax Description

<i>server-name</i>	Specifies the name of the server (local to this SBE). The <i>server-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
--------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Server accounting (config-sbc-sbe-acc)  
Server authentication (config-sbc-sbe-auth)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Any number of accounting servers and authentication servers can be specified. Call Detail Reports are sent to the accounting server or authentication server with the highest priority upon call termination.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command configures accounting servers castor and pollux on mySbc for RADIUS client instance radius1:

```
Router# configure
Router(config)# sbc mySbc
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# radius accounting radius1
Router(config-sbc-sbe-acc)# server castor
Router(config-sbc-sbe-acc-ser)# address ipv4 200.200.200.12
Router(config-sbc-sbe-acc-ser)# exit
Router(config-sbc-sbe-acc)# server pollux
Router(config-sbc-sbe-acc-ser)# address ipv4 200.200.200.15
Router(config-sbc-sbe-acc-ser)# exit
```



# service sbc sbe radius accounting

To reactivate connection between the SBC and a RADIUS server after connectivity is lost or to restart remote billing after connectivity is restored, use the **service sbc sbe radius accounting** command in the Privileged EXEC mode.

**service sbc name sbe radius accounting radius client name {resend | server word reactivate}**

## Syntax Description

resend	Restarts remote billing between SBC and RADIUS on the reactivated RADIUS server connection for new billing requests.
server	RADIUS account server commands.
name	Specifies the name of the SBC service.
radius client	Specifies the name of the RADIUS client.
<i>word</i>	Specifies the server name.
reactivate	Reactivates the connection between SBC and RADIUS server. You need to do this to manually recover the connection after it has failed.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to resend cached messages:

```
Router# service sbc test sbe radius accounting acc resend
```

The following example shows how to reactivate connection to a RADIUS server:

```
Router# service sbc test sbe radius accounting acc server svr reactivate
```



# session-refresh renegotiation

To enable or disable renegotiation of media bypass after session refreshes, use the **session-refresh renegotiation** command in the CAC table entry configuration mode. To remove this configuration, use the **no** form of this command.

**session-refresh renegotiation {allow | suppress}**

**no session-refresh renegotiation**

## Syntax Description

allow	Specifies that an offer that contains duplicate SDP must be processed using the normal offer-answer rules. Media reservations can change, and interworking functions can be renegotiated.
suppress	Specifies that an offer that contains duplicate SDP must be processed using the session refresh variant of the offer-answer rules. Media reservations are not changed, and interworking functions are not renegotiated. The SBC forwards the last sent offer or answer regardless of the offer or answer that was received.

## Command Default

The default is that the session refresh strategy for the call is not affected by this CAC policy entry.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples**

The following example shows how to disable renegotiation of media bypass after the session refreshes:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyTable
Router(config-sbc-sbe-cacpolicy-cactable)# table-type src-adjacency
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
```

**Related Commands**

Command	Description
<b>cac-policy-set</b>	Creates a policy set, copies an existing complete policy set, or swaps the references of a complete policy set to another policy set.
<b>cac-table</b>	Creates or configures an admission control table.
<b>entry</b>	Creates or modifies an entry in a table or an SDP media profile.
<b>table-type</b>	Configures a CAC table type that enables the priority of the call to be used as a criterion in a CAC policy.

# show debugging

To display information about the types of debugging that are enabled for your router, use the **show debugging** command in the privileged EXEC mode.

## show debugging

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	11.1	This command was introduced.
	12.3(7)T	The output of this command was enhanced to show TCP Explicit Congestion Notification (ECN) configuration.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.4(20)T	The output of this command was enhanced to show the user-group debugging configuration.
	3.5.0S	This command was implemented on Cisco IOS XE Release 3.5.0S. In addition, the output of this command was enhanced to display the output of the <b>debug sbc alarm-filter</b> command and the <b>debug sbc alarm-log-level</b> command.

**Examples** The following is sample output of the **show debugging** command. In this example, the remote host is neither configured nor connected.

```
Router# show debugging
!
TCP:
  TCP Packet debugging is on
  TCP ECN debugging is on
!
Router# telnet 10.1.25.234
!
Trying 10.1.25.234 ...
!
00:02:48: 10.1.25.31:11001 <---> 10.1.25.234:23 out ECN-setup SYN
00:02:48: tcp0: O CLOSED 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
          OPTS 4 ECE CWR SYN WIN 4128
00:02:50: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:02:50: cwnd from 1460 to 1460, ssthresh from 65535 to 2920
00:02:50: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
          OPTS 4 ECE CWR SYN WIN 4128
00:02:54: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
```

```

00:02:54: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:02:54: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
      OPTS 4 ECE CWR SYN WIN 4128
00:03:02: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:02: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:02: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
      OPTS 4 ECE CWR SYN WIN 4128
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23 SYN with ECN disabled
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:18: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:18: tcp0: O SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
      OPTS 4 SYN WIN 4128
00:03:20: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:20: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:20: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
      OPTS 4 SYN WIN 4128
00:03:24: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:24: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:24: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
      OPTS 4 SYN WIN 4128
00:03:32: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:32: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:32: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
      OPTS 4 SYN WIN 4128
!Connection timed out; remote host not responding

```

The following is sample output of the **show debugging** command when user-group debugging is configured:

```

Router# show debugging
!
usergroup:
  Usergroup Deletions debugging is on
  Usergroup Additions debugging is on
  Usergroup Database debugging is on
  Usergroup API debugging is on
!

```

The following is sample output of the **show debugging** command when SNAP debugging is configured:

```

Router# show debugging
Persistent variable debugging is currently All

SNAP Server Debugging ON

SNAP Client Debugging ON
Router#

```

Table 1 describes the significant fields in the output.

**Table 1** *show debugging Field Descriptions*

Field	Description
OPTS 4	Bytes of TCP expressed as a number. In this case, the bytes are 4.
ECE	Echo congestion experience.
CWR	Congestion window reduced.
SYN	Synchronize connections—Request to synchronize sequence numbers, used when a TCP connection is being opened.
WIN 4128	Advertised window size, in bytes. In this case, the bytes are 4128.
cwnd	Congestion window (cwnd)—Indicates that the window size has changed.
ssthresh	Slow-start threshold (ssthresh)—Variable used by TCP to determine whether or not to use slow-start or congestion avoidance.
usergroup	Statically defined user group to which source IP addresses are associated.

# show monitor event-trace sbc ha

To display the event trace messages for the Session Border Controller (SBC), use the **show monitor event-trace sbc** command in the privileged EXEC mode.

```
show monitor event-trace sbc ha {all [detail] | back {minutes | hours:minutes} [detail] | clock
hours:minutes [day month] [detail] | from-boot [seconds] [detail] | latest [detail] |
parameters}1
```

## Syntax Description

<b>ha</b>	Displays the event trace messages pertaining to the SBC high availability.
<b>all</b>	Displays all the event trace messages that are currently in memory pertaining to the SBC high availability.
<b>detail</b>	(Optional) Displays detailed trace information.
<b>back</b>	Specifies how far back from the current time you want to view messages. For example, you can view messages displayed over the last 30 minutes.
<i>minutes</i>	Time argument in minutes. The time argument is specified in the minutes format (mmm).
<i>hours:minutes</i>	Time argument in hours and minutes. The time argument is specified in the hours and minutes format (hh:mm).
<b>clock</b>	Displays event trace messages starting from a specific time in the hours and minutes format (hh:mm).
<i>day month</i>	(Optional) The day of the month (from 1 to 31), and the name of the month.
<b>from-boot</b>	Displays event trace messages that started after booting.
<i>seconds</i>	(Optional) Specifies the number of seconds to display event trace messages after booting. Range: 0 to the number of seconds elapsed since the boot.
<b>latest</b>	Displays only the event trace messages since the last <b>show monitor event-trace sbc ha</b> command was entered.
parameters	Displays the trace parameters. The parameters displayed are the size (number of trace messages) of the trace file and whether stacktrace is disabled.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.3	The <b>sbc_ha</b> keyword was bifurcated into two keywords, <b>sbc</b> and <b>ha</b> .
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

Use the **show monitor event-trace sbc ha** command to display trace message information pertaining to the SBC high availability.

The trace function is not locked when information is displayed on the console, which means that the new trace messages can be accumulated in memory. If entries are accumulated faster than they may be displayed, some messages can be lost. If this happens, the **show monitor event-trace sbc ha** command generates a message indicating that some messages may be lost. However, messages continue to be displayed on the console. If the number of lost messages is excessive, the **show monitor event-trace sbc ha** command stops displaying messages.

**Examples**

The following is a sample output of the **show monitor event-trace sbc ha all** command. In the following example, all the messages from the SBC high availability events are displayed:

```
Router# show monitor event-trace sbc ha all

*Jan 16 07:21:49.718: RF: Is Active, from boot = 0x1
*Jan 16 07:21:49.720: IPC: Initialised as master
*Jan 16 07:21:49.720: RF: Active reached, from boot = 0x1
*Jan 16 07:21:59.448: ILT: Registered on 48, result = 0x1
*Jan 16 07:21:59.448: RF: Start SM on 48
*Jan 16 07:49:02.523: IPC: Session to peer opened
*Jan 16 07:49:02.605: ISSU: Negotiation starting
*Jan 16 07:49:02.605: RF: Delaying progression at 300
*Jan 16 07:49:02.617: ISSU: Negotiation done
*Jan 16 07:49:02.617: RF: Negotiation result = 0x1
*Jan 16 07:49:02.617: RF: Peer state change, peer state = 0x1
*Jan 16 07:49:02.617: RF: Resuming progression at event 300
*Jan 16 07:50:00.853: ISSU: Transformed transmit message
*Jan 16 07:50:00.853: IPC: Queuing message type SBC_HA_MPF_CAPS_MSG_TYPE
*Jan 16 07:50:00.854: IPC: Queued message type SBC_HA_MPF_CAPS_MSG_TYPE
```

[Table 2](#) describes the significant fields shown in the display.

**Table 2** *show monitor event-trace sbc ha all Field Descriptions*

Field	Description
RF:	Redundancy Facility (RF) events. RF controls and drives the high availability redundancy events.
IPC:	Interprocess communication (IPC) messages.
ILT:	Interlocation Transport (ILT) events. ILT is the interface and mechanism for transporting the SBC high availability data.
ISSU:	In Service Software Upgrade (ISSU) events.

The following is a sample output of the **show monitor event-trace sbc ha latest** command. This command displays the messages from the SBC high availability events since the last **show monitor event-trace sbc ha** command was entered.

```
Router# show monitor event-trace sbc ha latest

*Jan 16 07:50:00.922: IPC: Sent message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: IPC: Received message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: ISSU: Transformed received message
*Jan 16 07:50:00.922: ILT: Received IPS for PID 0x30105000, type = 0x16820002
*Jan 16 07:50:00.922: ILT: Target 49 is remote, for PID 0x31105000
```

```
*Jan 16 07:50:00.922: ILT: Send IPS to PID 0x31105000, type = 0x16820001
*Jan 16 07:50:00.922: ISSU: Transformed transmit message
*Jan 16 07:50:00.922: IPC: Queuing message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: IPC: Queued message type SBC_HA_SEND_IPS_MSG_TYPE
*Jan 16 07:50:00.922: IPC: Sent message type SBC_HA_SEND_IPS_MSG_TYPE
```

This command displays the messages since the last **show monitor event-trace sbc ha** command was entered.

[Table 3](#) describes the significant fields shown in the display.

**Table 3** *show monitor event-trace sbc ha latest Field Descriptions*

Field	Description
IPC:	IPC messages.
ILT:	ILT events. ILT is the interface and mechanism for transporting SBC high availability data.
ISSU:	ISSU events.

The following is a sample output of the **show monitor event-trace sbc ha parameters** command. This command displays the number of event trace messages in the trace file, and whether stacktrace is disabled.

```
Router# show monitor event-trace sbc ha parameters
```

```
Trace has 2048 entries
Stacktrace is disabled by default
```

**Related Commands**

Command	Description
<b>monitor event-trace sbc ha (EXEC)</b>	Monitors and controls the event trace function for the SBC.
<b>monitor event-trace sbc ha (global)</b>	Configures event tracing for the SBC.



# show platform hardware qfp active feature sbc sfx

To display the Cisco QuantumFlow Processor SIP Fast-Register (SFX) counters, use the **show platform hardware qfp active feature sbc sfx** command in Privileged EXEC mode.

**show platform hardware qfp active feature sbc sfx [global]**

## Syntax Description

global	Specifies SIP Fast-Register (SFX) global state information.
--------	---

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Information about how SIP fast-register (SFX) messages are processed, that is, which SIP REGISTER request packets are punted to the Route Processor (RP) or dropped, may help explain why call rates are low and why the RP CPU load is high.

## Examples

The following example shows information about the parsing of SIP fast-register (SFX) messages in the Cisco QuantumFlow Processor (QFP):

```
Router# show platform hardware qfp active feature sbc sfx global
```

```
SBC QFP SIP Fast Register Dataplane Information
```

```
-----
SIP 200 OK Replies generated           = 0
SIP REGISTER punts :
  No table entry                       = 0
  Fast Timer expiry                    = 0
  Expires=0                            = 0
  SIP Syntax Error                     = 0
  QFP Out of Resources                  = 0
  QFP Internal Error                    = 0
SIP REGISTER drops :
  QFP Internal Error                   = 0
  UDP Length Error                     = 0
  UDP Checksum Error                   = 0
```

Table 1 lists field descriptions for the **show platform hardware qfp active feature sbc sfx** command.

**Table 1** *show platform qfp active feature sbc sfx Field Descriptions*

Field	Description
SIP 200 OK Replies generated	A SIP REGISTER request was replied to in the QFP fast path using a 200 OK success reply.
SIP REGISTER punts	
No table entry	A SIP REGISTER request could not be matched with a programmed SIP Fast-Register entry. This means that the combination of AoR (Address of Record, the To: field) and the Contact URI did not match any entry. The SIP REGISTER request is then punted to the Route Processor (RP).
Fast Timer expiry	When a SIP Fast-Register entry is added for fast-pathing the SIP REGISTER requests for the combination of AoR and Contact URI, a time limit for fast-pathing the re-REGISTER requests is set. When that time limit is exceeded, then the next SIP REGISTER request is punted to the RP.
Expires=0	A SIP REGISTER request was received with either an individual Contact specifying “expires=0” or with a SIP request global “Expires: 0” message header. The SIP REGISTER request is then punted to the RP.
SIP Syntax Error	A field in a SIP REGISTER message could not be parsed in the QFP fast path. The request is then punted to the RP.
QFP Out of Resources	A resource on the QFP could not be allocated to process a SIP REGISTER request. The request is then punted to the RP.
QFP Internal Error	An internal inconsistency in processing a SIP REGISTER request was encountered. The request is then punted to the RP for processing.
SIP REGISTER drops	
QFP Internal Error	A failure to format the reply packet or to send the reply packet back was encountered. The request packet is dropped.
UDP Length Error	A packet's UDP length did not match the IP total length and is dropped.
UDP Checksum Error	The UDP checksum was incorrect in the SIP REGISTER packet. The packet is dropped.

**Related Commands**

Command	Description
<b>clear platform hardware qfp active feature sbc sfx</b>	Clears information about SIP fast-register (SFX) messages in the Cisco QuantumFlow Processor (QFP).

# show sbc

To list all the Session Border Controllers (SBCs) configured on the chassis, use the **show sbc** command in the Privileged EXEC mode.

**show sbc**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.6.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.1S	The output of the command was changed to include the mode and status of the SBC.

## Examples

The following example shows how the **show sbc** command displays the list of all SBCs configured on the chassis.

```
Router# show sbc
SBC name is asr1k-sbc
SBC mode is Unified
SBC is Active
```

## Related Commands

Command	Description
<b>show sbc services</b>	Displays the list of all SBC services on the chassis.

# show sbc dbe addresses (session border controller)

To list the H.248 control addresses and media addresses configured on data border elements (DBEs), use the **show sbc dbe addresses** command in user EXEC or privileged EXEC mode.

**show sbc {sbc-name} dbe addresses**

<b>Syntax Description</b>	<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	User EXEC (>)	
	Privileged EXEC (#)	

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		Cisco IOS XE Release 2.1
	Cisco IOS XE Release 3.1S	The format of the output displayed by this command was modified in a release earlier than Release 3.1S.

**Examples** The following example shows the H.248 control and media addresses, VRF name, port ranges, and service class configured on a DBE that is on the mySbc SBC:

```
Router# show sbc mySbc dbe addresses

SBC Service "mySbc"
  H.248 control address:10.0.0.1

Media-Address:          1.1.1.1
VRF:                    Global
Port-Range (Service-Class): 5-6 (signaling)
                        16384-20000 (any)

Media-Address:          1.1.1.2-1.1.1.3
VRF:                    Global
Port-Range (Service-Class):

Media-Address:          1.1.1.5-1.1.1.6
VRF:                    Global
Port-Range (Service-Class):

Media-Address:          6::2 - 6::3
VRF:                    Global
Port-Range (Service-Class): 4-6 (signaling)

Media-Address:          6::5
VRF:                    Global
```

```

Port-Range (Service-Class):

Media-Address:
    1111:2222:3333:4444::1 -
    1111:2222:3333:4444::5
VRF:                                Global
Port-Range (Service-Class):        2-6 (signaling)

Media-Address:
    1111:2222:3333:4444::8
VRF:                                Global
Port-Range (Service-Class):

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show sbc dbe controllers</b>	Displays the media gateway controllers and the controller address configured on each DBE.
<b>show sbc dbe forwarder-stats</b>	Displays the global list of statistics for the DBE forwarding process.
<b>show sbc dbe media-stats</b>	Displays general DBE statistics. These statistics do not include data from active calls.
<b>show sbc dbe media-flow-stats</b>	Displays the statistics about one or more media flows collected on the DBE.
<b>show sbc dbe signaling-flow-stats</b>	Displays the statistics about one or more signaling flows collected on the DBE.
<b>unexpected-source-alerting</b>	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

# show sbc dbe controllers (session border controller)

To list the media gateway controllers (MGCs) and the controller address configured on each data border element (DBE), use the **show sbc dbe controllers** command in user EXEC or privileged EXEC mode.

**show sbc {sbc-name} dbe controllers**

<b>Syntax Description</b>	<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	User EXEC (>)	
	Privileged EXEC (#)	

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	Output was modified to add Session Establishment Time, Transaction Long Timer, and TMAX Timeout fields.
	Cisco IOS XE Release 2.4	This command was modified for distributed SBC—output was modified to show Service Change Cold Boot delay timer information.

**Examples** The following example shows that the controller is detached and a new field indicating that a delay timer is set to delay generation of a Service Change Cold Boot for 112 seconds was added in Cisco IOS XE Release 2.4 for distributed SBC:

```
Router# show sbc global dbe controllers
SBC Service "global"
  vDBE in DBE location 1

  DBE Admin Status:   Activation Delayed 112 seconds
  Media gateway controller in use:
    H.248 controller address
      200.50.1.254:2970
    Status:   Detached

    Requests      Sent      Received   Failed   Retried
    Replies       0         0         0         0

  Segmentation:
    MGC PDU Size:  N/A
    MG PDU Size:   N/A
    MGC Seg timer: N/A
    MG Seg timer:  N/A
    Segments Sent: N/A
    Segments Rcvd: N/A
```

```
Configured controllers:
  H.248 controller 2:
```

The following example shows that the controller is attached and a new field displaying the Session Establishment Time (“**since 2008/02/19 13:56:30**”) that was added in Cisco IOS XE Release 2.2:

```
Router# show clock
*09:06:03.135 UTC Mon Feb 18 2008

Router# show sbc global dbc controllers
SBC Service "global"
  vDBE in DBE location 1

  DBE Admin Status:    Active
  Media gateway controller in use:
    H.248 controller address
      200.50.1.254:2970
    Status:    Attached, since 2008/02/19 13:56:30

    Requests      Sent      Received   Failed   Retried
    Replies       0         1          0        0

  Segmentation:
    MGC PDU Size:  N/A
    MG PDU Size:   N/A
    MGC Seg timer: N/A
    MG Seg timer:  N/A
    Segments Sent: N/A
    Segments Rcvd: N/A

  Configured controllers:
    H.248 controller 2:
```

The following example establishes controller connection prior to the TMAX timeout being changed:

```
Router# show sbc global dbc controller
SBC Service "global"
  vDBE in DBE location 1

  DBE Admin Status:    Active
  DBE Transaction Long Timer 15000 (ms)
  DBE TMAX Timeout 10000 (ms)

  Media gateway controller in use:
    H.248 controller address
      200.50.1.254:2970
    Status:    Attached, since 2008/02/22 17:35:43

    Requests      Sent      Received   Failed   Retried
    Replies       0         1          0        0

  Segmentation:
    MGC PDU Size:  N/A
    MG PDU Size:   N/A
    MGC Seg timer: N/A
    MG Seg timer:  N/A
    Segments Sent: N/A
    Segments Rcvd: N/A

  Configured controllers:
    H.248 controller 2:
```

```
Remote address: 200.50.1.254:2970
Transport:      UDP
```

The following example shows that the Tmax timeout has been changed to 20 seconds and entering the **show controller** command again displays the new fields, Transaction Long Timer and TMAX Timeout, added in Cisco IOS XE Release 2.2:

```
Router# show sbc global dbc controllers
SBC Service "global"
  vDBE in DBE location 1

  DBE Admin Status:    Active
  DBE Transaction Long Timer 25000 (ms)
  DBE TMAX Timeout 20000 (ms)

  Media gateway controller in use:
    H.248 controller address
      200.50.1.254:2970
    Status:    Detached

    Requests      Sent      Received   Failed   Retried
    Replies       0         0          0        2
    Replies       0         0          0        0

  Segmentation:
    MGC PDU Size:  N/A
    MG PDU Size:   N/A
    MGC Seg timer: N/A
    MG Seg timer:  N/A
    Segments Sent: N/A
    Segments Rcvd: N/A

  Configured controllers:
    H.248 controller 2:
      Remote address: 200.50.1.254:2970
      Transport:      UDP
```

The following example shows the H.248 controllers configured on the virtual data border element (vDBE) with a location ID of 1 on an SBC called "mySbc." In this example, the H.248 status is active.

```
Router# show sbc mySbc dbc controllers

SBC Service "mySbc"
  vDBE in DBE location 1

  DBE Admin Status:    Active
  Media gateway controller in use:
    H.248 controller address
      200.100.1.254:2991
    Status:    Detached

    Requests      Sent      Received   Failed   Retried
    Replies       0         0          0        2
    Replies       0         0          0        0

  Segmentation:
    MGC PDU Size:  33 bytes
    MG PDU Size:   N/A
    MGC Seg timer: 44 ms
    MG Seg timer:  N/A
    Segments Sent: N/A
    Segments Rcvd: N/A
```



```

Configured controllers:
  H.248 controller 1:
    Remote address: 200.100.1.254:2991
    Transport:      UDP (with IAH)

```

The following example shows the H.248 controllers configured on the virtual data border element (vDBE) with a location ID of 1 on an SBC called "mySbc." In this example, the H.248 status is inactive.

```
Router# show sbc mySbc dbe controllers
```

```

SBC Service "mySbc"
vDBE in DBE location 1

DBE Admin Status:  Inactive
Media gateway controller in use:

Configured controllers:
  H.248 controller 5:
    Remote address: 10.1.1.1:6
    Transport:      UDP

```

Table 2 describes the significant fields shown in the display.

**Table 2** *show sbc dbe controllers Field Descriptions*

Field	Description
DBE Admin Status	Possible values are Active and Inactive.
Media gateway controller in use:	Statistics that follow are applicable to the MGC(s) in use.
H.248 controller address	H.248 controller address.
Status:	Status of the controller. Possible values are Attached and Detached.
Requests	Number of H.248 requests sent, received, failed, or retried.
Replies	Number of H.248 replies sent, received, failed, or retried.
Segmentation:	Statistics that follow are applicable to the H.248 Segmentation package.
MGC PDU Size	Maximum protocol data unit (PDU) size, in bytes, that the User Datagram Protocol (UDP) should use for H.248 control signaling.
MG PDU Size	Not applicable.
MGC Seg timer	Time interval, in milliseconds, on the segmentation timer.
MG Seg timer	Not applicable.
Segments Sent:	Number of segments sent.
Segments Rcvd:	Number of segments received.
Configured controllers:	Statistics that follow are applicable to configured H.248 controllers.
Remote address	Remote address of the configured controller.
Transport	Transport in use on the configured controller. Possible values are UDP, UDP (with IAH), TCP, and TCP (with IAH)

**Table 2** *show sbc dbe controllers Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Session Establishment Time	This has the format (YY/MM/DD hour/minute/second). If the router time is changed, the operator is expected to detect this from any console log, as the Session Establishment Time is not updated.
Transaction Long Timer	This timer determines the total time the DBE waits (and keep retrying) from initially sending a request until receiving a response. It is set to TMAX + MaxRTT, where TMAX is configurable and MaxRTT is hard coded to 0.5 seconds.  The association to the MGC is lost if this timer expires before the transaction reply is received.
TMAX Timeout	This is the maximum delay in seconds. It is a parameter of the TMAX timer that limits the maximum delay of retransmissions by the DBE when sending messages to the MGC. The default is 10 seconds.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show sbc dbe addresses</b>	Displays the H.248 control addresses and media addresses configured on DBEs.
<b>show sbc dbe forwarder-stats</b>	Displays the global list of statistics for the DBE forwarding process.
<b>show sbc dbe media-stats</b>	Displays general DBE statistics. These statistics do not include data from active calls.
<b>show sbc dbe media-flow-stats</b>	Displays the statistics about one or more media flows collected on the DBE.
<b>show sbc dbe signaling-flow-stats</b>	Displays the statistics about one or more signaling flows collected on the DBE.
<b>unexpected-source-alerting</b>	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

# show sbc dbf flow-stats (session border controller)

To list all flow statistics, both signaling and media flows, collected on the data border element (DBE), use the **show sbc dbf flow-stats** command in user EXEC or privileged EXEC mode.

```
show sbc {sbc-name} dbf flow-stats [{summary | detail}] [vrf vrf-name] [ {ipv4 A.B.C.D | ipv6
ipv6-address} [port port-number]] [context {id}| termination {termination substring}]]
```

Syntax Description	
<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
summary	(Optional) Displays a summary of all flow statistics, including pinhole flows, for the DBE.
detail	(Optional) Displays detailed flow statistics, including pinhole flows, for the DBE.
vrf <i>vrf-name</i>	(Optional) Displays only flows to or from the specified VPN routing and forwarding instance (VRF).
ipv4 <i>A.B.C.D</i>	(Optional) Displays only flows to or from the specified IPv4 media IP address.
ipv6 <i>ipv6-address</i>	(Optional) Displays only flows to or from the specified IPv6 media IP address.
port <i>port-number</i>	(Optional) Displays only flows to or from the specified port number.
context	(Optional) Shows summary or detailed display of all pinhole flows within the context ID.
id	(Optional) Specifies the context ID number.
termination	(Optional) Shows summary or detailed display of pinhole flows that match the termination substring.
termination substring	(Optional) Specifies the termination substring number.

**Command Default** No default behavior or values are available.

**Command Modes** User EXEC (>)  
Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.4	This command is supported for the unified model.

**Usage Guidelines** The flow-stats per-flow counters are updated dynamically.

Not all endpoints report RTP Control Protocol (RTCP) endpoint statistics. In addition, not all endpoints that report RTCP statistics report all the fields shown.

When the "Media Flowing" field is reported as Yes, it either means that media has been observed flowing on the call within the media timeout period, or the call has failed over within the last media timeout period and the SBC has not yet had a chance to observe whether media is flowing or not.

**Examples**

The following example displays all the active flows, signaling and media flows:

```
Router# show sbc global dbe flow-stats
SBC Service "global"
Media flow statistics
Media Flow:
Context ID:          2
Stream ID:           2
State of Media Flow: Allocated
Call Established Time: 15:27:27 PDT Apr 9 2008
Flow Priority:       Unspecified
Side A:
Name                 mycompany/voice/gn/0/1/0/1/ac/3
Reserved Bandwidth: 12600 (bytes/second)
Status               OutofService
VRF Name:            Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:       202.50.2.1
Local Port:          10002
Remote Address:      10.10.127.22
Remote Port:         17384
Packets Received:    0
Packets Sent:        0
Packets Discarded:   0
Data Received:       0 (bytes)
Data Sent:            0 (bytes)
Data Discarded:      0 (bytes)
GM Discarded Packets: 0
Time To Recovery:    Not known
RTCP Packets Sent:   Not known
RTCP Packets Received: Not known
RTCP Packets Lost:   Not known
DTMF Interworking:   No
Media Flowing:       No
Unexpected SrcAddr Packets: No
Billing ID:           000000000000000000000000000000000000000000000000000000000000000000000000
Media directions allowed: inactive
Max Burst size:       0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:           m=application $ udp 0
Graceful deactivation: No
DiffServ Code Point: 0
Media Loss Event:     No
NAT Latch Event:     No

Side B:
Name                 mycompany/voice/gn/0/2/0/1/bb/4
Reserved Bandwidth: 12600 (bytes/second)
Status               OutofService
VRF Name:            Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:       202.50.2.1
Local Port:          10004
Remote Address:      200.0.0.1
Remote Port:         19384
Packets Received:    0
Packets Sent:        0
```

```

Packets Discarded:          0
Data Received:              0 (bytes)
Data Sent:                  0 (bytes)
Data Discarded:            0 (bytes)
GM Discarded Packets:      0
Time To Recovery:          Not known
RTCP Packets Sent:         Not known
RTCP Packets Received:     Not known
RTCP Packets Lost:        Not known
DTMF Interworking:         No
Media Flowing:             No
Unexpected SrcAddr Packets: No
Billing ID:                 00000000000000000000000000000000000000000000000000000000000000000000
Media directions allowed:  inactive
Max Burst size:            0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:                m=application $ udp 0
Graceful deactivation:     No
DiffServ Code Point:      0
Media Loss Event:          No
NAT Latch Event:          No

```

SBC Service "global"

Signaling flow statistics

Media Flow:

```

Context ID:          2
Stream ID:           1
State of Signaling Flow: Allocated
Call Established Time: 15:24:38 PDT Apr 9 2008
Flow Priority:       Unspecified

```

Side A:

```

Name                mycompany/sip4/gn/0/1/0/1/ac/1
Reserved Bandwidth: 0 (bytes/second)
Status              InService
VRF Name:           Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:      202.50.2.1
Local Port:         10000
Remote Address:     3.0.0.3
Remote Port:        5000
Packets Received:   0
Packets Sent:       0
Packets Discarded:  0
Data Received:      0 (bytes)
Data Sent:          0 (bytes)
Data Discarded:     0 (bytes)
GM Discarded Packets: 0
Time To Recovery:   Not known
Media Flowing:      No
Unexpected SrcAddr Packets: No
Max Burst size:     0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:         m=application $ udp 0
Graceful deactivation: No
DiffServ Code Point: 0
Media Loss Event:   No
NAT Latch Event:   No

```

Side B:

```

Name                mycompany/sip4/gn/0/1/0/1/bb/2
Reserved Bandwidth: 0 (bytes/second)
Status              InService
VRF Name:           Global
VLAN Tags(Priorities): 0(0), 0(0)

```

```

Local Address:          202.50.2.1
Local Port:             10001
Remote Address:        3.0.0.3
Remote Port:           5000
Packets Received:      0
Packets Sent:          0
Packets Discarded:     0
Data Received:         0 (bytes)
Data Sent:             0 (bytes)
Data Discarded:        0 (bytes)
GM Discarded Packets:  0
Time To Recovery:      Not known
Media Flowing:         No
Unexpected SrcAddr Packets: No
Max Burst size:        0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:            m=application $ udp 0
Graceful deactivation: No
DiffServ Code Point:   B8
Media Loss Event:      No
NAT Latch Event:       No
    
```

The following example displays a summary of all flows with context ID number 1:

```

Router# show sbc global dbe flow-stats summary context 1
SBC Service "global"
Media flow statistics
Context ID 1          Stream ID 2
Side A:              Name mycompany/voice/gn/0/1/0/1/ac/3   Media Flowing: No
  Local Address/Port: 202.50.2.1/10002
  Remote Address/Port: 10.10.127.22/17384
  Status:             OutofService
Side B:              Name mycompany/voice/gn/0/2/0/1/bb/4   Media Flowing: No
  Local Address/Port: 202.50.2.1/10004
  Remote Address/Port: 200.0.0.1/19384
  Status:             OutofService

SBC Service "global"
Signaling flow statistics
Context ID 1          Stream ID 1
Side A:              Name mycompany/sip4/gn/0/1/0/1/ac/1   Media Flowing: No
  Local Address/Port: 202.50.2.1/10000
  Remote Address/Port: 3.0.0.3/5000
  Status:             InService
Side B:              Name mycompany/sip4/gn/0/1/0/1/bb/2   Media Flowing: No
  Local Address/Port: 202.50.2.1/10001
  Remote Address/Port: 3.0.0.3/5000
  Status:             InService
    
```

The following example displays a summary of flows with the termination string, mycompany:

```

Router# show sbc global dbe flow-stats summary termination mycompany
SBC Service "global"
Media flow statistics
Context ID 1          Stream ID 2
Side A:              Name mycompany/voice/gn/0/1/0/1/ac/3   Media Flowing: No
  Local Address/Port: 202.50.2.1/10002
  Remote Address/Port: 10.10.127.22/17384
  Status:             OutofService
Side B:              Name mycompany/voice/gn/0/2/0/1/bb/4   Media Flowing: No
  Local Address/Port: 202.50.2.1/10004
  Remote Address/Port: 200.0.0.1/19384
    
```

```

Status:                OutofService

SBC Service "global"
Signaling flow statistics
Context ID 1           Stream ID 1
Side A:                Name mycompany/sip4/gn/0/1/0/1/ac/1   Media Flowing: No
  Local Address/Port: 202.50.2.1/10000
  Remote Address/Port: 3.0.0.3/5000
  Status:              InService
Side B:                Name mycompany/sip4/gn/0/1/0/1/bb/2   Media Flowing: No
  Local Address/Port: 202.50.2.1/10001
  Remote Address/Port: 3.0.0.3/5000
  Status:              InService

```

The following example displays a summary of flows with the combination of context ID 1 and the termination string, mycompany:

```

Router# show sbc global dbe flow-stats summary context 1 termination mycompany
SBC Service "global"
Media flow statistics
Context ID 1           Stream ID 2
Side A:                Name mycompany/voice/gn/0/1/0/1/ac/3   Media Flowing: No
  Local Address/Port: 202.50.2.1/10002
  Remote Address/Port: 10.10.127.22/17384
  Status:              OutofService
Side B:                Name mycompany/voice/gn/0/2/0/1/bb/4   Media Flowing: No
  Local Address/Port: 202.50.2.1/10004
  Remote Address/Port: 200.0.0.1/19384
  Status:              OutofService

SBC Service "global"
Signaling flow statistics
Context ID 1           Stream ID 1
Side A:                Name mycompany/sip4/gn/0/1/0/1/ac/1   Media Flowing: No
  Local Address/Port: 202.50.2.1/10000
  Remote Address/Port: 3.0.0.3/5000
  Status:              InService
Side B:                Name mycompany/sip4/gn/0/1/0/1/bb/2   Media Flowing: No
  Local Address/Port: 202.50.2.1/10001
  Remote Address/Port: 3.0.0.3/5000
  Status:              InService

```

[Table 3](#) describes the significant fields shown in the display.

**Table 3** *show sbc dbe flow-stats Field Descriptions*

Field	Description
Context ID	The context ID to which the flow is associated.
Stream ID	Stream ID.

**Table 3** *show sbc dbe flow-stats Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
State of Media Flow	Flow (or Termination) state (Active, Allocated, or Unknown).  Active—The DBE has programmed the flow pair and media has started flowing in at least one direction.  Allocated—The DBE has programmed the flow pair, but no media has started to flow.  Unknown—The DBE has not yet been given enough information by the controller to be able to program the flow pair.
State of Signaling Flow	Flow state (Active, Allocated, or Unknown). <ul style="list-style-type: none"> <li>• Active—DBE has programmed the flow pair and the media has started flowing in at least one direction.</li> <li>• Allocated—DBE has programmed the flow pair, but no media has started to flow.</li> <li>• Unknown—DBE has not yet been given enough information by the controller to be able to program the flow pair.</li> </ul>
Call Established Time	Call established time in the format 23:51:29 UTC Jun 21 2007.
Flow Priority	Priority of the call (Routine or Urgent).
Side A	Information for the initiating side of the call.
Side B	Information for the terminating side of the call.
Name	Name of the flow.
Reserved Bandwidth	Bandwidth reserved for the call in bytes per second. (This value maps to the tman/sdr value.)
Status	Status is InService or OutofService.  InService—Flow on this side is in service.  OutofService—No media is forwarded.
VRF Name	Either the VRF name, or “Global” when there is no VRF.
VLAN Tags (Priorities)	VLAN tags and Ethernet priorities information.
Local Address	Local address on the DBE on which packets are received for this side of the call.
Local Port	Local port on the DBE on which packets are received for this side of the call.
Remote Address	Address of the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Port	Port on the remote endpoint from which packets are expected to be sent for this side of the call.



**Table 3** *show sbc dbe flow-stats Field Descriptions (continued)*

Field	Description
Remote Source Address Mask	If specified, all packets matching the Remote Source Address Mask are classified as belonging to this flow rather than just those matching the full remote and port. (This value maps to the gm/sam value.)
Packets Received	Number of packets received from the remote endpoint.
Packets Sent	Number of packets forwarded to the remote endpoint.
Packets Discarded	Number of packets dropped (due to bandwidth policing, for example).
Data Received	Number of bytes of data received from the remote endpoint.
Data Sent	Number of bytes of data forwarded to the remote endpoint.
Data Discarded	Number of bytes of data dropped (due to bandwidth policing, for example). (This value maps to the gm/sam value.)
GM Discarded Packets	This counter is always set to zero because it is not currently implemented. It will be the number of data packets received from the remote endpoint that have been discarded locally because of source address/port filtering.
Time To Recovery	The tsc/ttr value from Termination State Control (TSC) package, in milliseconds.
RTCP Packets Sent	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being sent.
RTCP Packets Received	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being received.
RTCP Packets Lost	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being lost.
DTMF Interworking	Indicates whether DTMF interworking is in operation for the flow.
Media Flowing	Indicates whether packets are flowing from the endpoint.
Unexpected SrcAddr Packets	If unexpected-source-alerting is switched on with the <b>unexpected-source-alerting</b> command, this counter records the number of alerts generated for the flow when media packets for a call are received from an unexpected source address and port.  An unexpected source event happens when a packet is received, matched to a flow (but not by a full 5-tuple comparison), and found to have come from the wrong remote address.
Delay variation tolerance	The delay variation tolerance (tman/dvt) associated with the Tman package. Defines the delay variation tolerance for the stream in tenths of microseconds when enforcing the PDR value in the first leaky bucket.

**Table 3** *show sbc dbe flow-stats Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
SDP string	The SDP string is that present on the H.248 ADD request to provision the call.
Graceful deactivation	Description to be added.
DiffServ Code Point	The Diffserv Code point is the (DSCP value) provided on the H.248 request to mark the media packets. This reflects the ds/dscp parameters.
Media Loss Event	Media Loss Event is “Yes” if the flow has the nt/qualert subscription.
NAT Latch Event	The NAT Latch Event is “Yes” if the flow has adr/rsac subscribed.
Billing ID	Signaling border element (SBE) billing ID for this side of the call.
Media directions allowed	Allowed directions of media flow for this side of the call (inactive, sendonly, recvonly, or sendrecv).

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show sbc dbe addresses</b>	Displays the H.248 control addresses and media addresses configured on DBEs.
<b>show sbc dbe controllers</b>	Displays the media gateway controllers and the controller address configured on each DBE.
<b>show sbc dbe forwarder-stats</b>	Displays the global list of statistics for the DBE forwarding process.
<b>show sbc dbe media-stats</b>	Displays general DBE statistics. These statistics do not include data from active calls.
<b>show sbc dbe signaling-flow-stats</b>	Displays the statistics about one or more signaling flows collected on the DBE.
<b>unexpected-source-alerting</b>	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

# show sbc dbe forwarder-stats (session border controller)

To display the global list of statistics for the DBE forwarding process, use the **show sbc dbe forwarder-stats** command in user EXEC mode or privileged EXEC mode.

```
show sbc {sbc-name} dbe forwarder-stats
```

<b>Syntax Description</b>	<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
---------------------------	-----------------	--

**Command Default** No default behavior or values are available.

**Command Modes** User EXEC (>)  
Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.4	Added "Packets violated" field.

**Usage Guidelines** This command provides a live snapshot of the current state of the DBE forwarding process by showing low-level statistics on the packets processed by the process. This command is intended to be used by Cisco customer support engineers to diagnose media problems.

Because DBE forwarding statistics can overwrite after approximately 4 billion packets, overall packet counts might not be accurate. For more accurate statistics on completed calls, use the **show sbc dbe media-stats** command. For accurate information on active flows, use the **show sbc dbe media-flow-stats** command.

**Examples** The following example shows the list of statistics for the DBE forwarding process:

```
Router# show sbc global dbe forwarder-stats

IOSd MPF Stub Message statistics
-----
Total global PMI messages received           = 1
Total global PMI messages transmitted        = 1
Total call PMI messages received             = 0
Total call PMI messages transmitted         = 0
Total global PMI message handling failures  = 0
Total call PMI message handling failures    = 0
Total global TDL messages received          = 1
Total global TDL messages transmitted       = 1
Total call TDL messages received            = 0
Total call TDL messages transmitted         = 0
Total global TDL message handling failures  = 0
Total call TDL message handling failures    = 0
```

```

Total packets injected           = 0
Total packets punted            = 0
Total injected packets dropped   = 0
Total punted packets dropped     = 0
Total global message timeouts    = 0
Total call message timeouts      = 0

Call ID database is NOT Initialised

IOSd MPF Stub Call statistics
-----
Number of currently in-use Calls = 0
High-water number of in-use Calls = 0
Maximum number of in-use Calls supported = 0

SBC Media Forwarder Statistics
-----
Summary information:
  Total packets received           = 28416
  Total packets forwarded          = 14336
  Total packets dropped             = 14080
  Total packets punted             = 0
  Incoming packets diverted to SBC subsystem = 0
  Outgoing packets inserted by SBC subsystem = 0

Detailed breakdown of statistics:

Dropped packets:
  IP TTL expired                   = 0
  No associated flow                = 0
  Wrong source for flow            = 0
  Ingress flow receive disabled    = 0
  Egress flow send disabled        = 0
  Not conforming to flowspec       = 14080
  Badly formed RTP                 = 0
  Badly formed RTCP                = 0
  Excessive RTCP packet rate       = 0
  Borrowed for outgoing DTMF       = 0
  Unknown destination address      = 0
  Misdirected                      = 0
  Feature disabled                 = 0
  Reprocess limit exceeded         = 0

Punted packets:
  H.248 control packets            = not implemented
  Packets containing options        = 0
  Fragmented packets               = 0
  Unexpected IP protocol           = 0
  Packets from invalid port range  = 0

Punted packets dropped through rate limiting = 0
Packets colored with configured DSCP         = 0

Diverted DTMF packets dropped:
  Excessive DTMF packet rate       = 0
  Bad UDP checksum                 = 0
  Diverted packet queue full       = not implemented
  Other                            = not implemented

Inserted packets dropped:
  Flow inactive or disabled        = 0
  No outgoing packet buffer available = 0
  Outgoing Queue full              = 0
  Other                            = 0

```

```

Generated event information:
  Number of media UP events           = 0
  Number of media DOWN events         = 0
  Number of unexpected source events   = 0

Platform specific statistics:
  Packets learn source address         = 0
  Packets Learn source address timed out = 0
  Packets conformed                   = 1982
  Packets violated                     = 18
  Packets exceed                       = 0
  Packets RTCP receive                 = 0

```

SBC Media Forwarder statistics can wrap after approximately 18 quintillion packets. For more accurate statistics on completed calls, please use `show sbc ... dbe media-stats`

[Table 4](#) describes the significant fields shown in the display.

**Table 4** *show sbc dbe forwarder-stats Field Descriptions*

Field	Description
IOSd MPF Stub Message statistics	
Total global PMI messages received	Total global packet management interface (PMI) messages received by the DBE forwarding process. This counter increments during normal operation.
Total global PMI messages transmitted	Total global packet management interface (PMI) messages transmitted by the DBE forwarding process. This counter increments during normal operation.
Total call PMI messages received	Total packet management interface (PMI) messages related to calls received by the DBE forwarding process. This counter increments during normal operation.
Total call PMI messages transmitted	Total packet management interface (PMI) messages related to calls transmitted by the DBE forwarding process. This counter increments during normal operation.
Total global PMI message handling failures	Failure counters indicating that something has gone wrong with handling total global packet management interface (PMI) messages. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total call PMI message handling failures	Failure counters indicating that something has gone wrong with handling total packet management interface (PMI) messages related to calls. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total global TDL messages received	Total global type definition language (TDL) messages received by the DBE forwarding process. This counter increments during normal operation.

**Table 4** show sbc dbe forwarder-stats Field Descriptions (continued)

Field	Description
Total global TDL messages transmitted	Total global type definition language (TDL) messages transmitted by the DBE forwarding process. This counter increments during normal operation.
Total call TDL messages received	Total type definition language (TDL) messages related to calls received by the DBE forwarding process. This counter increments during normal operation.
Total call TDL messages transmitted	Total type definition language (TDL) messages related to calls transmitted by the DBE forwarding process. This counter increments during normal operation.
Total global TDL message handling failures	Failure counters indicating that something has gone wrong with handling total global type definition language (TDL) messages. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total call TDL message handling failures	Failure counters indicating that something has gone wrong with handling total type definition language (TDL) messages related to calls. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total packets injected	Total dual-tone multifrequency (DTMF) packets inserted into the Real-time Transport Protocol (RTP) stream. If DTMF interworking is configured, then these counters are expected to increase.
Total packets punted	Total dual-tone multifrequency (DTMF) packets removed from the Real-time Transport Protocol (RTP) streams. If DTMF interworking is configured, then these counters are expected to increase.
Total injected packets dropped	Failure counters indicating that something has gone wrong—total DTMF packets inserted into RTP streams that have dropped. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total punted packets dropped	Failure counters indicating that something has gone wrong—total DTMF packets removed from RTP streams that have dropped. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
IOSd MPF Stub Call statistics	
Number of currently in-use Calls	Number of calls currently in use.
High-water number of in-use Calls	The maximum number of calls that have ever been in use.
Maximum number of in-use Calls supported	This will only be filled in once the Call IS database moves to initialized state.
SBC Media Forwarder Statistics	
Summary information	

**Table 4** *show sbc dbe forwarder-stats Field Descriptions (continued)*

Field	Description
Total packets received	Total packets received by the DBE forwarding process.
Total packets forwarded	Total packets forwarded by the DBE forwarding process.
Total packets dropped	Total packets dropped by the DBE forwarding process for any reason.
Total packets punted	Total packets punted to the IP stack by the DBE forwarding process.
Incoming packets diverted to SBC subsystem	Number of incoming packets diverted to the Media Gateway Manager (MGM).
Outgoing packets inserted by SBC subsystem	Number of outgoing packets inserted by MGM.
Detailed breakdown of statistics	
Dropped packets	
IP TTL expired	Number of packets rejected by DBE forwarding process and dropped because the IP time to live (TTL) has expired.
No associated flow	Number of packets rejected by DBE forwarding process and dropped because they do not correspond to a matching media flow.
Wrong source for flow	Number of packets rejected by DBE forwarding process and dropped because the source IP address and source port do not match the expected source address and source port for the flow.
Ingress flow receive disabled	Number of packets rejected by DBE forwarding process and dropped because receiving packets from the remote endpoint is disabled.
Egress flow send disabled	Number of packets rejected by DBE forwarding process and dropped because sending packets to the remote endpoint is disabled.
Not conforming to flowspec	Number of packets rejected by DBE forwarding process and dropped because they do not conform according to flowspec traffic policing for the flow. A flowspec is the traffic parameters of a stream of IP packets between two applications in IPv6 or IPv4.
Badly formed RTP	Number of packets rejected by DBE forwarding process and dropped due to Real Time Protocol (RTP) errors.
Badly formed RTCP	Number of packets rejected by DBE forwarding process and dropped due to Real Time Control Protocol (RTCP) errors.
Excessive RTCP packet rate	Number of RTCP packets rejected by DBE forwarding process and dropped because too many RTCP packets were sent on a given flow; policer indicated violated the flow specifier. The DBE forwarding process allows two RTCP packets per second for each flow.

**Table 4** *show sbc dbe forwarder-stats Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Borrowed for outgoing DTMF	Number of packets rejected by DBE forwarding process and dropped because they were borrowed from their own flow in order to allow an outgoing packet to be inserted into a flow.
Unknown destination address	Number of packets rejected by DBE forwarding process and dropped because the destination address is unknown.
Misdirected	Number of packets that was dropped due to having an address that would have caused the packets to be punted.
Feature disabled	Number of packets that was received while SBC was in the process of being deactivated. Depending on the volume of traffic, this number will remain small. This counter only increments during the deactivation process. Once the feature (SBC) is fully deactivated (with the <b>no activate</b> command), this counter will no longer increment.
Reprocess limit exceeded	Error condition counter. Counts errors when an SBC packet is re-processed too many times because the destination address was changed to be a local address on the DBE. After the destination address is translated and forwarded, the packet ends up in the SBC path again. This counter does not typically increase.
Punted packets	
H.248 control packets	Not implemented in command output.
Packets containing options	Number of packets rejected by DBE forwarding process and punted because the IP header contains IP options.
Fragmented packets	Number of packets rejected by DBE forwarding process and punted to the IP stack because the IP datagram is fragmented.
Unexpected IP protocol	Number of packets rejected by DBE forwarding process and punted because they are neither UDP nor TCP, or they are TCP but they are not destined for a signaling pinhole.
Packets from invalid port range	Number of packets rejected by DBE forwarding process and punted because the destination UDP port is outside the VoIP UDP port range.
Punted packets dropped through rate limiting	Number of packets not punted to the IP stack and dropped due to rate limiting.
Packets colored with configured DSCP	Number of packets colored with configured marker DSCP value by Two-Rate-Three-Color Marker feature.
Diverted DTMF packets dropped	
Excessive DTMF packet rate	Number of incoming packets diverted to MGM but dropped due to rate limiting. These packets are included in the divert count and drop count.
Bad UDP checksum	The UDP checksum was incorrect in the DTMF packet. The packet is dropped.
Diverted packet queue full	Not implemented in command output.
Other	Not implemented in command output.



**Table 4** *show sbc dbe forwarder-stats Field Descriptions (continued)*

Field	Description
Inserted packets dropped	
Flow inactive or disabled	Number of outgoing packets inserted by MGM but dropped because the request is invalid. These packets are included in the insert count and drop count.
No outgoing packet buffer available	Number of outgoing packets inserted by MGM but dropped because no packet buffers are available. These packets are included in the insert count and drop count.
Outgoing Queue full	Number of outgoing packets inserted by MGM but dropped because the outgoing packet queue is full. These packets are included in the insert count and drop count.
Other	Number of outgoing packets inserted by MGM but dropped for other reasons. These packets are included in the insert count and drop count.
Generated event information	
Number of media UP events	Number of media UP events generated.
Number of media DOWN events	Number of media DOWN events generated.
Number of unexpected source events	Number of unexpected source address events generated.
Platform specific statistics	
Packets learn source address	For flows that have source address latching configured, a count of the number of packets that are latched.
Packets Learn source address timed out	If a flow has be programmed to relatch the source address and a new source address was not received in the specified timeframe, then this counts the timeout.
Packets conformed	Count of the number of packets that the policer indicated conformed to the flow specifier.
Packets violated	Count of the number of packets that the policer indicated violated the flow specifier.
Packets exceed	Count of the number of packets that the policer indicated exceeded the flow specifier
Packets RTCP receive	Count of the number of RTCP packets received.

**Related Commands**

Command	Description
<b>show sbc dbe addresses</b>	Displays the H.248 control addresses and media addresses configured on DBEs.
<b>show sbc dbe controllers</b>	Displays the media gateway controllers and the controller address configured on each DBE.
<b>show sbc dbe media-flow-stats</b>	Displays the statistics about one or more media flows collected on the DBE.
<b>show sbc dbe media-stats</b>	Displays general DBE statistics. These statistics do not include data from active calls.
<b>show sbc dbe signaling-flow-stats</b>	Displays the statistics about one or more signaling flows collected on the DBE.



# show sbc dbe h248-profile

To list the information on the specified H.248 profile, including transport, H.248 form, and active packages, use the **show sbc dbe h248-profile** command in the Privileged EXEC mode.

**show sbc *sbc-name* dbe h248-profile**

## Syntax Description

<i>sbc-name</i>	Defines the name of the service.
-----------------	----------------------------------

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows the defaults and configured options for the H.248 profile:

```
Router# show sbc mysbc dbe h248-profile
Transport UDP IAH
H.248 Version 3
Packages:
Generic(g)
Base Root(root): Max Terminations per context 10
Network(l)
DiffServ(ds)
Gate Management(gm)
Traffic Management(tman)
IP NAPT(ipnapt)
Segment(seg): Max PDU Size 4096 bytes
```

## Related Commands

Command	Description
<b>h248-profile</b>	Configures the vDBE H.248 profile name to interoperate with the MGC.
<b>h248-profile-version</b>	Configures the vDBE H.248 profile version to interoperate with the MGC. This command is used after you have defined the name of the profile using the <b>h248-profile</b> command.

# show sbc dbe media-flow-stats (session border controller)

To list the media flow statistics collected on the data border element (DBE), use the **show sbc dbe media-flow-stats** command in user EXEC or privileged EXEC mode.

```
show sbc {sbc-name} dbe media-flow-stats [{summary | detail}] [vrf vrf-name] [ {ipv4 A.B.C.D
| ipv6 ipv6-address} [port port-number]] [context {id}| termination {termination substring}]
```

## Syntax Description

<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
summary	(Optional) Displays a summary of the media flow statistics, including pinhole flows, for the DBE.
detail	(Optional) Displays detailed media statistics, including pinhole flows, for the DBE.
vrf <i>vrf-name</i>	(Optional) Displays only media flows to or from the specified VPN routing and forwarding instance (VRF).
ipv4 <i>A.B.C.D</i>	(Optional) Displays only media flows to or from the specified IPv4 media IP address.
<b>ipv6</b> <i>ipv6-address</i>	(Optional) Displays only media flows to or from the specified IPv6 media IP address.
<b>port</b> <i>port-number</i>	(Optional) Displays only media flows to or from the specified port number.
context	(Optional) Shows summary or detailed display of all pinhole flows within the context ID.
id	(Optional) Specifies the context ID number.
termination	(Optional) Shows summary or detailed display of pinhole flows. that match the termination substring.
termination substring	(Optional) Specifies the termination substring number.

## Command Default

No default behavior or values are available.

## Command Modes

User EXEC (>)  
Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	The <b>context</b> and <b>termination</b> keywords were added. New fields (Max Burst size, Delay variation tolerance, SDP string, Graceful deactivation, DiffServ Code Point, Media Loss Event, and NAT Latch Event) were added to the output display.
Cisco IOS XE Release 2.4	This command is supported for the unified model.

**Usage Guidelines**

Not all endpoints report RTP Control Protocol (RTCP) endpoint statistics. In addition, not all endpoints that report RTCP statistics report all the fields shown.

When the “Media Flowing” field is reported as Yes, it either means that media has been observed flowing on the call within the media timeout period, or the call has failed over within the last media timeout period and the SBC has not yet had a chance to observe whether media is flowing or not.

**Examples**

The following example displays signaling and media flow pairs and additional fields added in Cisco IOS XE Release 2.2:

```
Router# show sbc global dbc media-flow-stats
SBC Service "global"
Media Flow:
Context ID:          6
Stream ID:          2
State of Media Flow: Allocated
Call Established Time: 16:54:29 UTC Feb 20 2008
Flow Priority:      Unspecified
Side A:
Name                mycompany/voice/gn/0/1/0/1/ac/3
Reserved Bandwidth: 12600 (bytes/second)
Status              OutofService
VRF Name:           Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:      202.50.2.1
Local Port:         10002
Remote Address:     10.10.127.22
Remote Port:        17384
Packets Received:   0
Packets Sent:       0
Packets Discarded:  0
Data Received:      0 (bytes)
Data Sent:          0 (bytes)
Data Discarded:     0 (bytes)
GM Discarded Packets: 0
Time To Recovery:   Not known
EndPoint Packets sent: Not known
EndPoint Packets received: Not known
EndPoint Packets Lost: Not known
DTMF Interworking:  No
Media Flowing:     No
Unexpected SrcAddr Packets: No
Billing ID:         0000000000000000000000000000000000000000000000000000000000000000
Media directions allowed: inactive
Max Burst size:     3250 (bytes)          <===== additional fields for side A
Delay variation tolerance: 0 (ms)
SDP string:         m=audio $ RTP/AVP 0
Graceful deactivation: No
DiffServ Code Point: 0
Media Loss Event:   No
NAT Latch Event:   No
Side B:
Name                mycompany/voice/gn/0/2/0/1/bb/4
Reserved Bandwidth: 12600 (bytes/second)
Status              OutofService
VRF Name:           Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:      202.50.2.1
Local Port:         10004
Remote Address:     200.0.0.1
Remote Port:        19384
```

```

Packets Received:          0
Packets Sent:              0
Packets Discarded:        0
Data Received:             0 (bytes)
Data Sent:                 0 (bytes)
Data Discarded:           0 (bytes)
GM Discarded Packets:     0
Time To Recovery:         Not known
EndPoint Packets Sent:     Not known
EndPoint Packets Received: Not known
EndPoint Packets Lost:    Not known
DTMF Interworking:        No
Media Flowing:            No
Unexpected SrcAddr Packets: No
Billing ID:                0000000000000000000000000000000000000000000000000000000000000000
Media directions allowed: inactive
Max Burst size:           3250 (bytes)          <===== additional fields for Side B
Delay variation tolerance: 0 (ms)
SDP string:               m=audio $ RTP/AVP 0
Graceful deactivation:    No
DiffServ Code Point:     0
Media Loss Event:        No
NAT Latch Event:         No

```

The following example shows detailed statistics from an IPv4 media flow collected on the DBE:

Router# **show sbc mySbc dbe media-flow-stats detail**

```

SBC Service "mySbc"
Media Flow:
Context ID:                1
Stream ID:                 2
State of Media Flow: Active
Call Established Time: 23:50:20 UTC Jun 21 2007
Flow Priority:             Routine
Side A:
Name                       abc/voice/gn/0/1/0/1/ac/3
Reserved Bandwidth:        12 (bytes/second)
Status                     InService
VRF Name:                  Global
VLAN Tags(Priorities):    0(0), 0(0)
Local Address:             202.50.255.113
Local Port:                20000
Remote Address:            100.50.255.110
Remote Port:               20000
Remote Source Address Mask: 100.50.255.0/24
Packets Received:         2272
Packets Sent:              1784
Packets Discarded:        0
Data Received:             266 (bytes)
Data Sent:                 209 (bytes)
Data Discarded:           0 (bytes)
GM Discarded Packets:     0
Time To Recovery:         Not known
EndPoint Packets Sent:    Not known
EndPoint Packets Received: Not known
EndPoint Packets Lost:    Not known
DTMF Interworking:        No
Media Flowing:            Yes
Unexpected SrcAddr Packets: No
Billing ID:                0000000000000000000000000000000000000000000000000000000000000000
Media directions allowed: sendrecv

```

```

Max Burst size:           3250 (bytes)           <===== additional fields for side A
Delay variation tolerance: 0 (ms)
SDP string:               m=audio $ RTP/AVP 0
Graceful deactivation:    No
DiffServ Code Point:     0
Media Loss Event:         No
NAT Latch Event:         No

Side B:
Name                     abc/voice/gn/0/1/0/1/bb/4
Reserved Bandwidth:     23 (bytes/second)
Status                   InService
VRF Name:               Global
VLAN Tags(Priorities):  0(0), 0(0)
Local Address:          202.50.255.113
Local Port:             20002
Remote Address:         200.50.255.110
Remote Port:            30000
Packets Received:       2249
Packets Sent:           2272
Packets Discarded:      465
Data Received:          263 (bytes)
Data Sent:              266 (bytes)
Data Discarded:         54 (bytes)
GM Discarded Packets:   0
Time To Recovery:       Not known
EndPoint Packets Sent:  Not known
EndPoint Packets Received: Not known
EndPoint Packets Lost:  Not known
DTMF Interworking:      No
Media Flowing:          Yes
Unexpected SrcAddr Packets: No
Billing ID:              0000000000000000000000000000000000000000000000000000000000000000
Media directions allowed: sendrecv
Max Burst size:         3250 (bytes)           <===== additional fields for side B
Delay variation tolerance: 0 (ms)
SDP string:             m=audio $ RTP/AVP 0
Graceful deactivation:   No
DiffServ Code Point:    0
Media Loss Event:       No
NAT Latch Event:       No

```

The following example shows detailed statistics from an IPv6 media flow collected on the DBE:

```
Router# show sbc mySbc dbc media-flow-stats detail
```

```

SBC Service "mySbc"
Media Flow:
Context ID:           13
Stream ID:            2
State of Media Flow: Allocated
Call Established Time: 23:51:29 UTC Jun 21 2007
Flow Priority:        Routine
Side A:
Name                 abc/voice/gn/0/1/0/1/ac/1
Reserved Bandwidth:  23 (bytes/second)
Status               InService
VRF Name:           Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:       3333:1111:1111:2222:3333:4444:5555:7777
Local Port:          30000
Remote Address:      2222:1111:1111:2222:3333:4444:5555:7777
Remote Port:         20000

```

```

Packets Received:            0
Packets Sent:                0
Packets Discarded:          0
Data Received:               0 (bytes)
Data Sent:                   0 (bytes)
Data Discarded:              0 (bytes)
GM Discarded Packets:       0
Time To Recovery:            Not known
EndPoint Packets Sent:       Not known
EndPoint Packets Received:   Not known
EndPoint Packets Lost:       Not known
DTMF Interworking:          No
Media Flowing:               No
Unexpected SrcAddr Packets: No
Billing ID:                  00000000000000000000000000000000000000000000
Media directions allowed:    sendrecv
Max Burst size:              3250 (bytes)          <===== additional fields for side A
Delay variation tolerance:    0 (ms)
SDP string:                  m=audio $ RTP/AVP 0
Graceful deactivation:       No
DiffServ Code Point:         0
Media Loss Event:            No
NAT Latch Event:            No

```

Side B:

```

Name                         abc/voice/gn/0/1/0/1/bb/2
Reserved Bandwidth:          12 (bytes/second)
Status                       InService
VRF Name:                    Global
VLAN Tags(Priorities):       0(0), 0(0)
Local Address:                2222:1111:1111:2222:3333:4444:5555:7777
Local Port:                   20000
Remote Address:               3333:1111:1111:2222:3333:4444:5555:7777
Remote Port:                  30000
Packets Received:            0
Packets Sent:                 0
Packets Discarded:           0
Data Received:                0 (bytes)
Data Sent:                    0 (bytes)
Data Discarded:               0 (bytes)
GM Discarded Packets:        0
Time To Recovery:            Not known
EndPoint Packets Sent:       Not known
EndPoint Packets Received:   Not known
EndPoint Packets Lost:       Not known
DTMF Interworking:          No
Media Flowing:               No
Unexpected SrcAddr Packets: No
Billing ID:                  00000000000000000000000000000000000000000000
Media directions allowed:    sendrecv
Max Burst size:              3250 (bytes)          <===== additional fields for side B
Delay variation tolerance:    0 (ms)
SDP string:                  m=audio $ RTP/AVP 0
Graceful deactivation:       No
DiffServ Code Point:         0
Media Loss Event:            No
NAT Latch Event:            No

```



The following example shows summary statistics collected for media flows on the DBE:

```
Router# show sbc mySbc dbc media-flow-stats summary

SBC Service "mySbc"
Context ID 1          Stream ID 2
Side A:              Name abc/voice6/gn/0/1/0/1/ac/3   Media Flowing: No
  Local Address/Port: 3:100:1:1:1:1:1/30000
  Remote Address/Port: 2:100:1:1:1:1:1/20000
  Status:              In Service
Side B:              Name abc/voice6/gn/0/1/0/1/bb/4   Media Flowing: No
  Local Address/Port: 2:100:1:1:1:1:1/20000
  Remote Address/Port: 3:100:1:1:1:1:1/30000
  Status:              In Service
Context ID 2          Stream ID 2
Side A:              Name abc/voice4/gn/0/1/0/1/ac/7   Media Flowing: No
  Local Address/Port: 202.100.1.3/20002
  Remote Address/Port: Not known
  Status:              In Service
Side B:              Name abc/voice4/gn/0/1/0/1/bb/8   Media Flowing: No
  Local Address/Port: 202.100.1.3/20000
  Remote Address/Port: 200.100.1.1/30000
  Status:              In Service
```

The following command lists the statistics for media flows collected on the DBE associated with a VRF vpn1:

```
Router# show sbc dmsbc-node9 dbc media-flow-stats summary/detail vrf vpn1 ipv4
88.88.110.100 port 20000
SBC Service 'dmsbc-node9'
Media Flow:
State of Media Flow: Active
Call Age: 3850390 ms
Call Priority: Routine
Reserved Bandwidth: 10 (kilobytes/second)
No media timeout remaining: 2741
Class of service: Any
Side A:
VRF Name: vpn1
Local Address: 88.88.110.100
Local Port: 20000
Remote Address: 200.200.200.172
Remote Port: 17488
RTP Packets Received: 140134
RTP Packets Sent: 140131
RTP Packets Discarded: 0
```

The following command lists the statistics about one or more media flows collected on the DBE for a port with an IPv4 address associated with a specific VRF instance:

```
Router# show sbc j dbc media-flow-stats detail vrf vpn1 ipv4 10.127.3.1 port 16526
SBC Service "j"
Media Flow:
State of Media Flow: Active
Call Priority:      Routine
ContextID:         12
StreamID:          49153
Reserved Bandwidth: 10500 (bytes/second)
No media timeout remaining: 30
Class of service:  Voice
Side A:
VRF Name:          vpn1
```

```

Local Address:          88.102.9.100
Local Port:            16384
Remote Address:        10.127.3.1
Remote Port:          16526
RTP Packets Received: 2119
RTP Packets Sent:     2096
RTP Packets Discarded: 0
RTP Data Received:    423800 (bytes)
RTP Data Sent:        419200 (bytes)
RTP Data Discarded:   0 (bytes)
End Point Packets Sent: Not known
End Point Packets Received: Not known
End Point Packets Lost: Not known
DTMF Interworking:    No
Media Flowing:        Yes
Affected by Routing Error: No
Unexpected SrcAddr Packets: No
Billing ID:           0x47B507DF2020202020202030302B3030303030300000
0018
Media directions allowed: sendrecv
Side B:
VRF Name:              vpn2
Local Address:         88.102.10.100
Local Port:            16384
Remote Address:        10.127.4.1
Remote Port:          19566
RTP Packets Received: 2096
RTP Packets Sent:     2119
RTP Packets Discarded: 0
RTP Data Received:    419200 (bytes)
RTP Data Sent:        423800 (bytes)
RTP Data Discarded:   0 (bytes)
End Point Packets Sent: Not known
End Point Packets Received: Not known
End Point Packets Lost: Not known
DTMF Interworking:    No
Media Flowing:        Yes
Affected by Routing Error: No
Unexpected SrcAddr Packets: No
Billing ID:           0x47B507DF2020202020202030302B3030303030300000
0017
Media directions allowed: sendrecv

```

Table 5 describes the significant fields shown in the display.

**Table 5** show sbc dbe media-flow-stats Field Descriptions

Field	Description
Context ID	The context ID to which the flow is associated.
Stream ID	Stream ID.

**Table 5** *show sbc dbe media-flow-stats Field Descriptions (continued)*

Field	Description
State of Media Flow	Flow (or Termination) state (Active, Allocated, or Unknown).  Active—The DBE has programmed the flow pair and media has started flowing in at least one direction.  Allocated—The DBE has programmed the flow pair, but no media has started to flow.  Unknown—The DBE has not yet been given enough information by the controller to be able to program the flow pair.
Call Established Time	Call established time in the format 23:51:29 UTC Jun 21 2007.
Flow Priority	Priority of the call (Routine or Urgent).
Side A	Information for the initiating side of the call.
Side B	Information for the terminating side of the call.
Name	Name of the flow.
Reserved Bandwidth	Bandwidth reserved for the call in bytes per second. (This value maps to the tman/sdr value.)
Status	Status is InService or OutofService.  InService—Flow on this side is in service.  OutofService—No media is forwarded.
VRF Name	Either the VRF name, or “Global” when there is no VRF.
VLAN Tags (Priorities)	VLAN tags and Ethernet priorities information.
Local Address	Local address on the DBE on which packets are received for this side of the call.
Local Port	Local port on the DBE on which packets are received for this side of the call.
Remote Address	Address of the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Port	Port on the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Source Address Mask	If specified, all packets matching the Remote Source Address Mask are classified as belonging to this flow rather than just those matching the full remote and port. (This value maps to the gm/sam value.)
Packets Received	Number of packets received from the remote endpoint.
Packets Sent	Number of packets forwarded to the remote endpoint.
Packets Discarded	Number of packets dropped (due to bandwidth policing, for example).
Data Received	Number of bytes of data received from the remote endpoint.
Data Sent	Number of bytes of data forwarded to the remote endpoint.

**Table 5** *show sbc dbe media-flow-stats Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Data Discarded	Number of bytes of data dropped (due to bandwidth policing, for example). (This value maps to the gm/sam value.)
GM Discarded Packets	This counter is always set to zero because it is not currently implemented. It will be the number of data packets received from the remote endpoint that have been discarded locally because of source address/port filtering.
Time To Recovery	The tsc/ttr value from Termination State Control (TSC) package, in milliseconds.
EndPoint Packets Sent	If there are EndPoint packets flowing in the call, the number of RTP packets (within the most recently received EndPoint) that the endpoint reports as being sent.
EndPoint Packets Received	If there are EndPoint packets flowing in the call, the number of RTP packets (within the most recently received EndPoint) that the endpoint reports as being received.
EndPoint Packets Lost	If there are EndPoint packets flowing in the call, the number of RTP packets (within the most recently received EndPoint) that the endpoint reports as being lost.
DTMF Interworking	Indicates whether DTMF interworking is in operation for the flow.
Media Flowing	Indicates whether packets are flowing from the endpoint.
Unexpected SrcAddr Packets	<p>If unexpected-source-alerting is switched on with the <b>unexpected-source-alerting</b> command, this counter records the number of alerts generated for the flow when media packets for a call are received from an unexpected source address and port.</p> <p>An unexpected source event happens when a packet is received, matched to a flow (but not by a full 5-tuple comparison), and found to have come from the wrong remote address.</p>
Billing ID	Signaling border element (SBE) billing ID for this side of the call.
Media directions allowed	Allowed directions of media flow for this side of the call (inactive, sendonly, recvonly, or sendrecv).
Max Burst size	The maximum burst size (tman/mbs) associated with the Tman package.
Delay variation tolerance	The delay variation tolerance (tman/dvt) associated with the Tman package. Defines the delay variation tolerance for the stream in tenths of microseconds when enforcing the PDR value in the first leaky bucket.
SDP string	The SDP string is that present on the H.248 ADD request to provision the call.
Graceful deactivation	Description to be added.

**Table 5** *show sbc dbe media-flow-stats Field Descriptions (continued)*

Field	Description
DiffServ Code Point	The Diffserv Code point is the (DSCP value) provided on the H.248 request to mark the media packets. This reflects the ds/dscp parameters.
Media Loss Event	Media Loss Event is “Yes” if the flow has the nt/qualert subscription.
NAT Latch Event	The NAT Latch Event is “Yes” if the flow has adr/rsac subscribed.

**Related Commands**

Command	Description
<b>show sbc dbe flow-stats</b>	Lists all flow statistics, both signaling and media flows, collected on the data border element (DBE).
<b>show sbc dbe addresses</b>	Displays the H.248 control addresses and media addresses configured on DBEs.
<b>show sbc dbe controllers</b>	Displays the media gateway controllers and the controller address configured on each DBE.
<b>show sbc dbe forwarder-stats</b>	Displays the global list of statistics for the DBE forwarding process.
<b>show sbc dbe media-stats</b>	Displays general DBE statistics. These statistics do not include data from active calls.
<b>show sbc dbe signaling-flow-stats</b>	Displays the statistics about one or more signaling flows collected on the DBE.
<b>unexpected-source-alerting</b>	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

# show sbc dbe media-stats (session border controller)

To list general data border element (DBE) statistics, use the **show sbc dbe media- stats** command in user EXEC or privileged EXEC mode.

**show sbc {sbc-name} dbe media-stats**

<b>Syntax Description</b>	<i>sbc-name</i> Name of the Session Border Controller (SBC) service.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	User EXEC (>)
	Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		Cisco IOS XE Release 2.1
	Cisco IOS XE Release 2.4	This command is supported in the unified model.
	Cisco IOS XE Release 3.2S	The output of the command was updated to include information about the transcoded calls.

**Usage Guidelines**

The **show sbc dbe media- stats** statistics do not include data from active calls. The global counters keep track of packets received and sent on calls that have already ended.

The Active Flows statistic counts the number of flows for which media has been observed within the media-timeout period, or where the call has failed over within the last media-timeout period and the Session Border Controller (SBC) has not yet had a chance to observe whether media is flowing or not.

The Unclassified Pkts statistic includes all packets received on the VLAN interface that are not matched to a valid media flow. This includes media packets not matched to a flow, signaling packets, and any other traffic.

**Examples**

The following example shows general DBE statistics on a DBE that is on an SBC called “mySbc.” These DBE statistics do not include data from active calls.

```
Router# show sbc mySbc dbe media-stats

SBC Service "MySBC"
  Available Bandwidth      = Unlimited
  Available Flows          = 131072
  Available Packet Rate    = Unlimited
  Active Media Flows       = 0
  Peak Media Flows         = 0
  Total Media Flows        = 0
  Active Transcoded Flows  = 1
```

```

Peak Transcoded Flows    = 1
Total Transcoded Flows  = 1
Active Signaling Flows  = 0
Peak Signaling Flows    = 0
Total Signaling Flows   = 0
SBC Packets Received    = 0
SBC Octets Received     = 0
SBC Packets Sent        = 0
SBC Octets Sent         = 0
SBC Packets Discarded   = 0
SBC Octets Discarded    = 0
No Media Count          = 0

```

Table 6 describes the significant fields shown in the display.

**Table 6** *show sbc dbe media-stats Field Descriptions*

Field	Description
Max Term per Context	Maximum number of terminations per context.
Available Bandwidth	Total amount of bandwidth available for new calls.
Available Flows	Total amount of flows available for new calls.
Available Packet Rate	Amount of media packets per second available to new calls.
Active Media Flows	Current number of active calls.
Peak Media Flows	Maximum number of concurrent calls recorded.
Total Media Flows	Total number of calls set up on the DBE since the statistics were last cleared.
Active Transcoded Flows	Current number of active transcoded calls.
Peak Transcoded Flows	Maximum number of transcoded calls recorded.
Total Transcoded Flows	Total number of transcoded calls on the DBE.
Active Signaling Flows	Current number of flows that are actively forwarding signaling traffic.
Peak Signaling Flows	Peak number of active signaling flows since the statistics were last reset.
Total Signaling Flows	Accumulated total number of signaling flows. This count contains both active signaling flows and signaling flows that were allocated but never connected.
SBC Packets Received	Total number of SBC packets received by the DBE for completed calls.
SBC Octets Received	Number of octets of SBC data received by the DBE for completed calls.
SBC Packets Sent	Total number of SBC packets sent by the DBE for completed calls.
SBC Octets Sent	Number of octets of SBC data sent by the DBE for completed calls.
SBC Packets Discarded	Number of SBC packets discarded on completed calls.

**Table 6** *show sbc dbe media-stats Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
SBC Octets Discarded	Number of SBC octets discarded on completed calls.
No Media Count	Number of calls that have been dropped because there was no media flowing on the call.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show sbc dbe addresses</b>	Displays the H.248 control addresses and media addresses configured on DBEs.
<b>show sbc dbe controllers</b>	Displays the media gateway controllers and the controller address configured on each DBE.
<b>show sbc dbe forwarder-stats</b>	Displays the global list of statistics for the DBE forwarding process.
<b>show sbc dbe media-flow-stats</b>	Displays the statistics about one or more media flows collected on the DBE.
<b>show sbc dbe signaling-flow-stats</b>	Displays the statistics about one or more signaling flows collected on the DBE.
<b>unexpected-source-alerting</b>	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.



# show sbc dbe signaling-flow-stats (session border controller)

To list the signaling flow statistics collected on the data border element (DBE), use the **show sbc dbe signaling-flow-stats** command in user EXEC or privileged EXEC mode.

```
show sbc {sbc-name} dbe signaling-flow-stats [{summary | detail} [vrf vrf-name] [{ipv4 A.B.C.D
| ipv6 ipv6-address} [port port-number]] [context {id}| termination {termination substring}]]
```

Syntax Description	
<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
summary	(Optional) Displays a summary of the signaling flow statistics, including pinhole flows, for the DBE.
detail	(Optional) Displays detailed signaling flow statistics, including pinhole flows, for the DBE.
vrf <i>vrf-name</i>	(Optional) Displays only signaling flows to or from the specified VPN routing and forwarding instance (VRF).
ipv4 <i>A.B.C.D</i>	(Optional) Displays only signaling flows to or from the specified IPv4 media IP address.
<b>ipv6</b> <i>ipv6-address</i>	(Optional) Displays only signaling flows to or from the specified IPv6 media IP address.
<b>port</b> <i>port-number</i>	(Optional) Displays only signaling flows to or from the specified port number.
context	(Optional) Shows summary or detailed display of all pinhole flows within the context ID.
id	(Optional) Specifies the context ID number.
termination	(Optional) Shows summary or detailed display of pinhole flows. that match the termination substring.
termination substring	(Optional) Specifies the termination substring number.

**Command Default** No default behavior or values are available.

**Command Modes** User EXEC (>)  
Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	The <b>context</b> and <b>termination</b> keywords were added. New fields (Max Burst size, Delay variation tolerance, SDP string, Graceful deactivation, DiffServ Code Point, Media Loss Event, and NAT Latch Event) were added to the output display.
	Cisco IOS XE Release 2.4	This command is supported in the unified model.

**Usage Guidelines**

When the “Media Flowing” field is reported as Yes, it either means that media has been observed flowing on the call within the media timeout period, or the call has failed over within the last media timeout period and the SBC has not yet had a chance to observe whether media is flowing or not.

**Examples**

The following example displays signaling and media flow pairs and additional fields added in Cisco IOS XE Release 2.2:

```
Router# show sbc global dbe signaling-flow-stats
SBC Service "global"
Media Flow:
Context ID:          6
Stream ID:           1
State of Signaling Flow: Allocated
Call Established Time: 16:53:58 UTC Feb 20 2008
Flow Priority:       Unspecified
Side A:
Name                 mycompany/sip4/gn/0/1/0/1/ac/1
Reserved Bandwidth:  0 (bytes/second)
Status               InService
VRF Name:            Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:       202.50.2.1
Local Port:          10000
Remote Address:      3.0.0.3
Remote Port:         5000
Packets Received:    0
Packets Sent:        0
Packets Discarded:   0
Data Received:       0 (bytes)
Data Sent:           0 (bytes)
Data Discarded:      0 (bytes)
GM Discarded Packets: 0
Time To Recovery:    Not known
Media Flowing:       No
Unexpected SrcAddr Packets: No
Max Burst size:      0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:          m=application $ udp 0
Graceful deactivation: No
DiffServ Code Point: 0
Media Loss Event:    No
NAT Latch Event:     No
Side B:
Name                 mycompany/sip4/gn/0/1/0/1/bb/2
Reserved Bandwidth:  0 (bytes/second)
Status               InService
VRF Name:            Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:       202.50.2.1
Local Port:          10001
Remote Address:      3.0.0.3
Remote Port:         5000
Packets Received:    0
Packets Sent:        0
Packets Discarded:   0
Data Received:       0 (bytes)
Data Sent:           0 (bytes)
Data Discarded:      0 (bytes)
GM Discarded Packets: 0
Time To Recovery:    Not known
Media Flowing:       No
```

<===== additional fields for Side A

```

Unexpected SrcAddr Packets: No
Max Burst size:                0 (bytes)                <===== additional fields for side B
Delay variation tolerance:      0 (microseconds)
SDP string:                     m=application $ udp 0
Graceful deactivation:         No
DiffServ Code Point:           B8
Media Loss Event:              No
NAT Latch Event:              No

```

The following example displays detailed statistics from an IPv4 signaling flow collected on the DBE:

```
Router# show sbc mySbc dbe signaling-flow-stats detail
```

```
SBC Service "mySbc"
```

```
Media Flow:
```

```

Context ID:                2
Stream ID:                 1
State of Signaling Flow:   Active
Call Established Time:      12:55:11 UTC Aug 11 2007
Flow Priority:              Routine

```

```
Side A:
```

```

Name                       abc/sip/gn/0/1/0/1/ac/1
Reserved Bandwidth:         43 (bytes/second)
Status                       InService
VRF Name:                   Global
VLAN Tags(Priorities):      0(0), 0(0)
Local Address:              202.50.255.110
Local Port:                 5000
Remote Address:             100.50.255.110
Remote Port:                5000
Remote Source Address Mask: 100.50.255.0/24
Packets Received:           1344
Packets Sent:               0
Packets Discarded:         444
Data Received:              885 (bytes)
Data Sent:                  0 (bytes)
Data Discarded:             292 (bytes)
GM Discarded Packets:       0
Time To Recovery:           Not known
Media Flowing:              Yes
Unexpected SrcAddr Packets: No
Max Burst size:             0 (bytes)                <===== additional fields for Side A
Delay variation tolerance:   0 (microseconds)
SDP string:                 m=application $ udp 0
Graceful deactivation:      No
DiffServ Code Point:        0
Media Loss Event:           No
NAT Latch Event:           No

```

```
Side B:
```

```

Name                       abc/sip/gn/0/1/0/1/bb/2
Reserved Bandwidth:         0 (bytes/second)
Status                       InService
VRF Name:                   Global
VLAN Tags(Priorities):      0(0), 0(0)
Local Address:              202.50.255.110
Local Port:                 5001
Remote Address:             200.50.255.110
Remote Port:                10000
Packets Received:           1335
Packets Sent:               900
Packets Discarded:         1335

```

```

Data Received:          880 (bytes)
Data Sent:              593 (bytes)
Data Discarded:        880 (bytes)
GM Discarded Packets:  0
Time To Recovery:      Not known
Media Flowing:         No
Unexpected SrcAddr Packets: No
Max Burst size:        0 (bytes)           <===== additional fields for side B
Delay variation tolerance: 0 (microseconds)
SDP string:            m=application $ udp 0
Graceful deactivation: No
DiffServ Code Point:  B8
Media Loss Event:     No
NAT Latch Event:      No

```

The following example displays detailed statistics from an IPv6 signaling flow collected on the DBE:

Router# **show sbc global dbe signaling-flow-stats detail**

```

SBC Service "global"
Media Flow:
Context ID:           2
Stream ID:            1
State of Signaling Flow: Allocated
Call Established Time: 12:55:11 UTC Aug 11 2007
Flow Priority:        Routine
Side A:
Name                  abc/sip/gn/0/1/0/1/ac/1
Reserved Bandwidth:   23 (bytes/second)
Status                InService
VRF Name:             Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:        1111:2222:3333:4444:5555:6666:7777:3331
Local Port:           5000
Remote Address:       Not known
Remote Port:          Not known
Remote Source Address Mask: 2222:1111:1111:2222:3333:4444:5555:7777/48
Packets Received:    0
Packets Sent:         0
Packets Discarded:   0
Data Received:       0 (bytes)
Data Sent:            0 (bytes)
Data Discarded:      0 (bytes)
GM Discarded Packets: Not known
Time To Recovery:    Not known
Media Flowing:       No
Unexpected SrcAddr Packets: No
Max Burst size:      0 (bytes)           <===== additional fields for side A
Delay variation tolerance: 0 (microseconds)
SDP string:          m=application $ udp 0
Graceful deactivation: No
DiffServ Code Point: B8
Media Loss Event:    No
NAT Latch Event:    No

Side B:
Name                  abc/sip/gn/0/1/0/1/bb/2
Reserved Bandwidth:   0 (bytes/second)
Status                InService
VRF Name:             Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address Mask:   2222:1111:1111:2222:3333:4444:5555:7777/48

```

```

Local Port:                0
Remote Address:            3333:1111:1111:2222:3333:4444:5555:7777
Remote Port:              10000
Packets Received:         0
Packets Sent:             0
Packets Discarded:        0
Data Received:            0 (bytes)
Data Sent:                0 (bytes)
Data Discarded:           0 (bytes)
GM Discarded Packets:     0
Time To Recovery:         Not known
Media Flowing:            No
Unexpected SrcAddr Packets: No
Max Burst size:           0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:               m=application $ udp 0
Graceful deactivation:    No
DiffServ Code Point:     B8
Media Loss Event:         No
NAT Latch Event:         No

```

<===== additional fields for side B

The following example shows summary statistics collected for signaling flows on the DBE:

```
Router# show sbc mySbc dbe signaling-flow-stats summary
```

```

SBC Service "mySbc"
Context ID 1                Stream ID 1
Side A:                    Name abc/sip6/gn/0/1/0/1/ac/1    Media Flowing: Yes
  Local Address/Port:      1:100:1:1:1:1:1:1/5060
  Remote Address/Port:     2:100:1:1:1:1:1:1/5000
  Status:                  In Service
Side B:                    Name abc/sip6/gn/0/1/0/1/bb/2    Media Flowing: Yes
  Local Address/Port:      2:100:1:1:1:1:1:1/5000
  Remote Address/Port:     3:100:1:1:1:1:1:1/5060
  Status:                  In Service
Context ID 2                Stream ID 1
Side A:                    Name abc/sip4/gn/0/1/0/1/ac/5    Media Flowing: Yes
  Local Address/Port:      202.100.1.1/5000
  Remote Address/Port:     100.100.1.1/5000
  Status:                  In Service
Side B:                    Name abcsip4/gn/0/1/0/1/bb/6    Media Flowing: Yes
  Local Address/Port:      202.100.1.1/5001
  Remote Address/Port:     200.100.1.1/5000
  Status:                  In Service

```

[Table 7](#) describes the significant fields shown in the display.

**Table 7** *show sbc dbe signaling-flow-stats Field Descriptions*

Field	Description
Context ID	Context ID to which the flow is associated.
Stream ID	Stream ID.

**Table 7** *show sbc dbe signaling-flow-stats Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
State of Signaling Flow	Flow state (Active, Allocated, or Unknown). <ul style="list-style-type: none"> <li>Active—DBE has programmed the flow pair and the media has started flowing in at least one direction.</li> <li>Allocated—DBE has programmed the flow pair, but no media has started to flow.</li> <li>Unknown—DBE has not yet been given enough information by the controller to be able to program the flow pair.</li> </ul>
Call Established Time	Call established time in the format 23:51:29 UTC Jun 21 2007.
Flow Priority	Priority of the call (Routine or Urgent).
Side A	Information for the initiating side of the call
Side B	Information for the terminating side of the call
Name	Name of the flow.
Reserved Bandwidth	Bandwidth reserved for the call in bytes per second.
Status	Status is InService or OutofService. InService—Flow on this side is in service. OutofService—No media is forwarded.
VRF Name	Either the VRF name, or “Global” when there is no VRF.
VLAN Tags (Priorities)	VLAN tags and Ethernet priority information.
Local Address	Local address on the DBE on which packets are received for this side of the call.
Local Port	Local port on the DBE on which packets are received for this side of the call.
Remote Address	Address of the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Port	Port on the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Source Address Mask	If specified, all packets matching the Remote Source Address Mask are classified as belonging to this flow rather than just those matching the full remote and port.
Packets Received	Number of packets received from the remote endpoint.
Packets Sent	Number of packets forwarded to the remote endpoint.
Packets Discarded	Number of packets dropped (due to bandwidth policing, for example).
Data Received	Number of bytes of data received from the remote endpoint.
Data Sent	Number of bytes of data forwarded to the remote endpoint.
Data Discarded	Number of bytes of data dropped (due to bandwidth policing, for example).

Table 7 show sbc dbe signaling-flow-stats Field Descriptions (continued)

Field	Description
GM Discarded Packets	This counter is always set to zero because it is not currently implemented. It will be the number of data packets received from the remote end point and discarded locally because of source address/port filtering.
Time To Recovery	The tsc/ttr value from Termination State Control (TSC) package, in milliseconds.
Media Flowing	Indicates whether packets are flowing from the endpoint.
Unexpected SrcAddr Packets	If unexpected-source-alerting is switched on with the <b>unexpected-source-alerting</b> command, this counter records the number of alerts generated for the flow when media packets for a call are received from an unexpected source address and port.  An unexpected source event happens when a packet is received, matched to a flow (but not by a full 5-tuple comparison), and found to have come from the wrong remote address.
Max Burst size	The maximum burst size (tman/mbs) associated with the Tman package.
Delay variation tolerance	The delay variation tolerance (tman/dvt) associated with the Tman package. Defines the delay variation tolerance for the stream in tenths of microseconds when enforcing the PDR value in the first leaky bucket.
SDP string	The SDP string is that present on the H.248 ADD request to provision the call.
Graceful deactivation	Description to be added.
DiffServ Code Point	The Diffserv Code point is the (DSCP value) provided on the H.248 request to mark the media packets. This reflects the ds/dscp parameters.
Media Loss Event	Media Loss Event is “Yes” if the flow has the nt/qualert subscription.
NAT Latch Event	The NAT Latch Event is “Yes” if the flow has adr/rsac subscribed.

**Related Commands**

Command	Description
<b>show sbc dbe flow-stats</b>	Lists all flow statistics, both signaling and media flows, collected on the data border element (DBE).
<b>show sbc dbe addresses</b>	Displays the H.248 control addresses and media addresses configured on DBEs.
<b>show sbc dbe controllers</b>	Displays the media gateway controllers and the controller address configured on each DBE.
<b>show sbc dbe forwarder-stats</b>	Displays the global list of statistics for the DBE forwarding process.

<b>Command</b>	<b>Description</b>
<b>show sbc dbe media-stats</b>	Displays general DBE statistics. These statistics do not include data from active calls.
<b>show sbc dbe media-flow-stats</b>	Displays the statistics about one or more media flows collected on the DBE.
<b>unexpected-source-alerting</b>	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.



## show sbc h248 bac

To display the H.248 Border Access Controller (BAC) configuration on the Session Border Controller (SBC), use the **show sbc h248 bac** command in the privileged EXEC mode.

```
show sbc h248 bac {adjacencies [adj-name]} | call contexts | iad {active-number | sessions
[filter] | [mid]} | trace-filter
```

Syntax Description		
<b>adjacencies</b>		Displays information pertaining to all the H.248 BAC adjacencies on the SBC or a specific H.248 BAC adjacency when the <i>adj-name</i> is configured.
<i>adj-name</i>		Specific name of an SBC H.248 BAC adjacency.
<b>call contexts</b>		Displays call information pertaining to the SBC H.248 BAC.
<b>iad</b>		Displays Integrated Access Device (IAD) information pertaining to the SBC H.248 BAC.
<b>active-number</b>		Displays the active number of the SBC H.248 BAC IAD.
<b>sessions</b>		Displays the SBC H.248 BAC IAD registry.
<b>filter</b>		Specifies the Message Identifier (MID) filter.
<b>mid</b>		Specifies the MID.
<b>trace-filter</b>		Displays the SBC H.248 BAC trace filter.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** There is no **no** form of this command.

**Examples**

The following is a sample output of the **show sbc h248 bac adjacencies** command:

```
H.248 Bac Service
  Name                               Type   State   Description
  -----
  core_spec2                         Core   Detached
  iad_80                             Access Detached
  iad_80_123                         Access Detached
```

Table 8 describes the significant fields shown in the display.

**Table 8** *show sbc h248 bac adjacencies Field Descriptions*

Field	Description
Name	Name of the H.248 adjacency.
Type	Type of the H.248 adjacency. The valid values are Core or Access.
State	State of the H.248 adjacency. The valid values are Attached or Detached.
Description	Description for the adjacency provided by customers.

The following is a sample output of the **show sbc h248 bac adjacencies core\_spec** command:

```
Adjacency core_spec2 (CORE)
  Status: Detached
  Control Address: 192.168.102.222
  Control Port Type: PORT-RANGE
  Control Port-Range Start: 2944
  Control Port-Range End: 2945
  Remote Address: 192.168.102.14
  Remote Port: 2944
  VRF: Global
  Reaml ID: 1
```

Table 9 describes the significant fields shown in the display.

**Table 9** *show sbc h248 bac adjacencies core\_spec Field Descriptions*

Field	Description
Status	State of the H.248 adjacency. The valid values are Attached or Detached.
Control Address	IP address assigned to the H.248 adjacency.
Control Port Type	Control port type of the H.248 adjacency. The valid values are Port Binding Type, Port for Static Binding, or Port Range for Dynamic Binding.
Control Port-Range Start	Start port number.
Control Port-Range End	End port number.
Remote Address	IP address of the Media Gateway Controller(MGC).
Remote Port	Listening port of the MGC.

**Table 9** show sbc h248 bac adjacencies core\_spec Field Descriptions (continued)

Field	Description
VRF	Virtual routing and forwarding (VRF) in which the adjacency resides.
Realm ID	ID for binding with the reserved IP address pool of media flow.

The following is a sample output of the **show sbc h248 bac adjacencies access\_spec** command:

```
Adjacency access (ACCESS)
  Status: Attached
  Control Address: 3.3.3.3
  Control Port Type: PORT
  Control Port: 2944
  VRF: Global
  Realm ID: 0
  Binding Core Adjacency: core
  H.248 BAC Domain Name: tt
  Heart Beat Terminate: 60
  Retry: 3
  Audit Interval: 60
  Audit: Auto (Default)
  Register Rate: 100
  Media Bypass: FALSE
  Media Down: FALSE
  NAT: Force-off (Default)
```

Table 10 describes the significant fields shown in the display.

**Table 10** show sbc h248 bac adjacencies access\_spec Field Descriptions

Field	Description
Status	State of the H.248 adjacency. The valid values are Attached or Detached.
Control Address	IP address assigned to the H.248 adjacency.
Control Port Type	Only PORT is supported for access adjacency.
Control Port	Port number assigned to the access adjacency.
VRF	VRF the adjacency resides in.
Realm ID	ID for binding with the reserved IP address pool of media flow.
Binding Core Adjacency	Core adjacency that the access adjacency binds.
H.248 BAC Domain Name	Domain name specified by customers.
Heart Beat Terminate	The terminate interval. BAC blocks the heartbeat from the endpoints within the terminate interval.
Retry	Retry number.
Audit Interval	Interval between BAC's endpoint audits.
Audit	Audit type for the H.248 adjacency. The valid values are Auto or Force.
Register Rate	Maximum register rate for the access adjacency.

**Table 10** *show sbc h248 bac adjacencies access\_spec Field Descriptions (continued)*

Field	Description
Media Bypass	Value shows whether media bypass is enabled or not.
Media Down	Value shows whether media down detection is enabled or not.
NAT	Value shows whether the endpoints reside behind the NAT device.

The following is a sample output of the **show sbc h248 bac call contexts** command:

```
Context ID: 51957
MGM correlator: 4
MPF correlator: 1
State: CONNECTED
RTP term id: RTP/00000
Access side RTP addr:
  src: 9.9.9.9/40000 VRF 0
  dst: 9.9.9.9/40000 VRF 0
Core side RTP addr:
  src: 8.8.8.8/40000 VRF 0
  dst: 192.168.102.81/4006 VRF 0
IAD mid: [192.168.102.80]:2944
-----
```

[Table 11](#) describes the significant fields shown in the display.

**Table 11** *show sbc h248 bac call contexts Field Descriptions*

Field	Description
Context ID	Context ID of the active call.
MGM correlator	ID of the MGM correlator.
MPF correlator	ID of the MPF correlator.
State	Call state. The valid values are IDLE, ALLOCATING, ALLOCATED, CONNECTED, MODIFYING, or DELETING.
RTP term id	RTP termination ID.
Access side RTP addr	Source or destination IP address, port, and VRF of media flow on the access side.
Core side RTP addr	Source or destination IP address, port, and VRF of media flow on the core side.
IAD mid	The MID for IAD.

The following is a sample output of the **show sbc h248 bac iad active-number 1** command:

```
H.248 bac active iad number: 1
H.248 bac active call context numbers: 47
```

[Table 12](#) describes the significant fields shown in the display.

**Table 12** *show sbc h248 bac iad active-number 1 Field Descriptions*

Field	Description
H.248 bac active iad number	Number of registered IADs.
H.248 bac active call context number	Number of active call contexts.

The following is a sample output of the **show sbc h248 bac iad sessions** command:

```
IAD Session:
  Access side remote address: 172.16.104.13 port 2944
  Core side local address: 172.16.104.178 port 3000
  IAD mid: [172.16.104.13]:2944
  BAC mid: [172.16.104.178]:2944
  IAD domain name:
```

[Table 13](#) describes the significant fields shown in the display.

**Table 13** *show sbc h248 bac iad sessions Field Descriptions*

Field	Description
Access side remote address	IP address and port number of the remote endpoint.
Core side local address	IP address and port number of the local core adjacency.
IAD mid	MID of the IAD.
BAC mid	MID of the BAC.
IAD domain name	Domain name of the IAD if the domain name is used for the MID.

# show sbc rg

To list the transport and statistical information pertaining to the Session Border Controller (SBC) redundancy group, use the **show sbc rg** command in Privileged EXEC mode.

**show sbc *sbc-name* rg {transport | statistics}**

Syntax Description	
<i>sbc-name</i>	The name of the SBC service.
<b>statistics</b>	Displays the SBC redundancy group statistics.
transport	Displays the SBC redundancy group transport information.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows the SBC redundancy group statistics:

```
Router# show sbc MySBC rg statistics
SBC HA B2B statistics
-----
Number of messages successfully queued           = 99901
Number of messages successfully requeued        = 3875
Number of messages successfully sent            = 99901
Number of IPS messages sent                     = 99628
Number of messages queue failures               = 0
Number of messages send throttles              = 0
Number of messages send full throttles         = 0
Number of messages requeue failures            = 0
Number of attempted-send message failures      = 45
Number of message header malloc failures       = 0
Number of no packet available failures         = 0
Number of high watermark of queued messages    = 43
Number of high watermark of recv messages      = 0

Number of messages received                     = 1621
Number of received IPS messages                 = 1389
Number of received messages discarded          = 0
Number of received messages dropped(no group)  = 0
Number of received large IPS messages         = 0
Number of large message send failures          = 0
Number of large message send total             = 0
Number of large message recv failures          = 0
Number of large message not sent, un supp by peer = 0
Slow start avoidance counter                   = 50/50
Send message size high watermark               = 7820
```

The following example shows the SBC redundancy group transport information:

```
Router# show sbc MySBC rg transport
SBC HA RG connection parameters for domain 2/2
```

```
-----
Application Type      1
Handler               8
My IP address         3.3.3.6
My L4 Port            4027
L3 Protocol           1
L4 Protocol           6
Peer IP address       3.3.3.8
Peer L4 Port          4027
My MTU                 16336
My L4 Offset          0
```

# show sbc rsrcmon

To show congestion states and statistics during switchover, use the **show sbc rsrcmon** command in the **Privileged EXEC mode**.

**show sbc *sbc-name* rsrcmon**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
<b>Command Default</b>	No default behavior or values are available.	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows the addresses that are configured on mySBC:

```
Router# show sbc test rsrcmon
Resource Monitoring           : Enabled
Congestion Status           : Normal
  CPU Congestion Status      : Normal
  Mem Congestion Status      : Normal
  Calls Rejected Due to Congestion : 0
  CPU Congestion Count       : 0
  Mem Congestion Count       : 0
CPU Congestion Threshold    : 91 %
CPU Congestion Clear Threshold : 80 %
Top Procs Frequency         : 200 ms
CPU Probe Duration during Congestion : 1000 ms
CPU Probe Duration during Normal Operation : 3000 ms
Avg CPU Utilization in last 500 msec : 0%(cpu0) 7%(cpu1)
                               1500 msec : 0%(cpu0) 10%(cpu1)
SBC Memory Allocation Limit : No Limit
  Current Allocation         : 78466149 bytes
  Peak Allocation            : 78466149 bytes
  Allocation Failure Count   : 0
  Buffer Pool Usage           : 67413 bytes
  CB Pool Usage              : 37464456 bytes
  Free Memory SBC Holding    : 40934280 bytes
  Memory Usage Ceiling       : 180000000 bytes
  Last Monitored Usage       : 37533189 bytes (20 %)
```

Here is info on malloc:

```
Total memory for dynamic memory allocation (arena) -- 440040 bytes
Number of ordinary blk not in use (ordblks) ----- 4
Number of small blk not in use (smlbks) ----- 0
Number of blks allocated w/ mmap (hblks) ----- 300
```



```
Sum of memory allocated with mmap (hblkhd) ----- 78798848 bytes
Space in small blks in use (usmblks) ----- 0 bytes
Space in free small blks (fsmblks) ----- 0 bytes
Space in ordinary blocks in use (uordblks) ----- 434736 bytes
Space in free ordinary blocks (fordblks) ----- 5304 bytes
keepcost ----- 5168
```

Here is OS memory info

```
Total = 844869632 bytes
Used = 470876160 bytes (321875968 bytes after minus buffers/cached)
Free = 373993472 bytes (522993664 bytes after adding buffers/cached)
Shared = 0 bytes
Buffers = 1130496 bytes
Cached = 147869696 bytes
```

# show sbc sbe aaa

To list the AAA status and configuration on each SBE, use the **show sbc sbe aaa** command in the **Privileged EXEC mode**.

```
show sbc sbc-name sbe aaa
```

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
<b>Command Default</b>	No default behavior or values are available.	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows the addresses that are configured on mySBC:

```
Router# show sbc sbe aaa

SBC Service "mySbc"
  AAA control address: 10.1.0.1
  Accounting server: 10.2.0.1
  Authentication server: 172.19.5.1
  Authentication server: 172.19.5.2
```

# show sbc sbe addresses

To list the addresses configured on SBEs, use the **show sbc sbe addresses** command in the **Privileged EXEC mode**.

**show sbc *sbc-name* sbe addresses**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	The command output was modified.

## Examples

The following example shows the addresses that are configured on mySBC:

```
Router# show sbc mySBC sbe addresses

SBC Service "mySbc"
  Control Addresses
    AAA control address:          10.1.0.1
    H.248 control address:        10.1.0.1

  Signaling Addresses
    H.323 adjacency h323ToIsp42:  10.1.0.2:1720, VRF vpn3
    SIP adjacency SipToIsp42:      10.1.0.2:5060, VRF vpn3
```

The following example shows the addresses that are configured on asr1:

```
Router# show sbc asr1 sbe addresses

SBC Service "asr1"
  Control Addresses
    AAA control address:          33.33.36.1
    No Media Gateway Controller Listen information found.

  Signaling Addresses
    No H323 adjacency information found.
    SIP adjacency UEV6: 2001:A401::33:33:36:1:4060
    SIP adjacency CCML34: 33.33.36.1:5060
    SIP adjacency CCML35: 33.33.36.1:5060
    SIP adjacency CCML36: 33.33.36.1:5060
    SIP adjacency CSPS23: 33.33.36.1:0
    SIP adjacency OpensipsV6: 2001:A401::33:33:36:1:7060
    SIP adjacency CCML35-IPv6: 2001:A401::33:33:36:1:5060
    SIP adjacency CCML35-vrfb: 10.190.7.97:5060, VRF h323-vrf-b
    SIP adjacency CCML36-IPv6: 2001:A401::33:33:36:1:5060
    SIP adjacency SIPP81-IPv6: 2001:A401::33:33:36:1:5060
```



# show sbc sbe adjacencies

To display the details of the adjacencies configured on the signaling border element (SBE), use the **show sbc sbe adjacencies** command in the privileged EXEC mode.

```
show sbc sbc-name sbe adjacencies {adjacency-name} [detail | authentication-realms | peers]
```

Syntax Description	
<i>sbc-name</i>	Name of the SBC.
<b>adjacency-name</b>	Name of the adjacency.
<b>detail</b>	Displays all the detailed field output pertaining to a specified Session Initiation Protocol (SIP) adjacency.
<b>authentication-realms</b>	Lists the configured authentication realms pertaining to a specified adjacency.
<b>peers</b>	Lists the peers configured for a specified adjacency.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.4.1	This command's output was modified to show whether an adjacency is configured to support the SIP method statistics.
	Cisco IOS XE Release 2.5	This command's output was modified to show the IP realm information, contact username information, IP-FQDN translation parameters, and 100rel interworking parameters.
	Cisco IOS XE Release 2.6	This command's output was modified to show the IPv6 details, and indicate whether TLS Mutual Authentication is enabled.
	Cisco IOS XE Release 3.1S	This command was modified. The <b>peers</b> keyword was added. The command output was modified to show IMS Rx information: <i>ims rx</i> , <i>ims realm</i> , <i>ims rx perf</i> , and <i>ims pani</i> . The <b>show sbc sbe adjacencies detail</b> command output was modified to show the peer status and the current peer index.
	Cisco IOS XE Release 3.2S	This command was modified. The output of the <b>show sbc sbe adjacencies detail</b> command was updated to include detailed information about the Multiple SBC Media Bypass feature.
	Cisco IOS XE Release 3.3S	This command was modified. The output of the <b>show sbc sbe adjacencies detail</b> command was updated to include detailed information about the H.225 messages, whether the contact username in a SIP REGISTER request is in a rewrite mode or passthrough mode, and the local jitter ratio.

Release	Modification
Cisco IOS XE Release 3.4S	This command was modified. The output of the <b>show sbc sbe adjacencies detail</b> command was updated to display the percentage of calls specified for use in the calculation of the Mean Opinion Score; Conversational Quality, Estimated (MOS-CQE) score and the value specified for the Advantage factor.
Cisco IOS XE Release 3.5S	This command was modified. The output of the <b>show sbc sbe adjacencies detail</b> command was updated to display information about the phone proxies associated with the adjacencies.
Cisco IOS XE Release 3.7S	This command was modified. The output of the <b>show sbc sbe adjacencies detail</b> command was updated to display information about value of the IMS Rf interface state for the adjacency.

### Usage Guidelines

The **statistics-setting** command must be configured in an adjacency before using the **show sbc sbe sip-method-stats** command to display the SIP method statistics. Use the **show sbc sbe adjacencies** command to verify that the **statistics-setting** command is configured in an adjacency.

### Examples

The following example shows how, in Cisco IOS XE Release 2.5 and later, the **show sbc sbe adjacencies detail** command lists the adjacency information, including the IP realm information, configured on an SBE:

```
Router# show sbc global sbe adjacencies Cisco-gw detail
SBC Service "global"
Adjacency Cisco-gw (SIP)
Status: Detached
Signaling address: 111.45.103.119:default
Signaling-peer: :5060 (Default)
Force next hop: No
Account:
Group: None
In header profile: Default
Out header profile: Default
In method profile: Default
Out method profile: Default
In body profile: None
Out body profile: None
In UA option prof: Default
Out UA option prof: Default
In proxy opt prof: Default
Out proxy opt prof: Default
Priority set name: None
Local-id: None
Rewrite REGISTER: Off
Target address: None
NAT Status: Auto Detect
Reg-min-expiry: 3000 seconds
Fast-register: Enabled
Fast-register-int: 30 seconds
Register aggregate: Disabled
Registration Required: Disabled
Register Out Interval: 0 seconds
Parse username params: Disabled
Supported timer insert:Disabled
Suppress Expires: Disabled
p-asserted-id header-value: not defined
p-assert-id assert: Disabled
```

```

Authenticated mode: None
Authenticated realm: None
Auth. nonce life time: 300 seconds
IMS visited NetID: None
Inherit profile: Default
Force next hop: No
Home network Id: None
UnEncrypt key data: None
SIPI passthrough: No
Passthrough headers:
Media passthrough: No
Client authentication: No
Incoming 100rel strip: No
Incoming 100rel supp: No
Out 100rel supp add: No
Out 100rel req add: No
Parse TGID parms: No
IP-FQDN inbound:
IP-FQDN outbound:
FQDN-IP inbound:
FQDN-IP outbound:
Outbound Flood Rate: None
Hunting Triggers: Global Triggers
Add transport=tls param: Disabled
Redirect mode: Pass-through
Security: Untrusted-Unencrypted
Ping: Disabled
Ping Interval: 32 seconds
Ping Life Time: 32 seconds
Ping Peer Fail Count: 3
Ping Trap sending: Enabled
Ping Peer Status: Not Tested
Rewrite Request-uri: Disabled
Registration Monitor: Disabled
DTMF SIP NOTIFY Relay: Enabled
DTMF SIP NOTIFY Interval: 2000
DTMF SIP default duration: 200
DTMF Preferred Method: SIP NOTIFY
Realm : cisco.com
Statistics setting: Disabled

```

The following example shows how, in Cisco IOS XE Release 2.5 and later, the **show sbc sbe adjacencies detail** command displays the Register contact username information:

```

Router# show sbc test sbe adjacencies SIP1Reg detail
SBC Service "test"
  Adjacency SIP1Reg (SIP)
    Status: Attached
    Signaling address: 10.10.100.140:default
    Signaling-peer: 10.10.100.12:7068
    Force next hop: No
    Account:
    Group: SIP1Reg
    .
    .
    .
Rewrite REGISTER: Off
  Register contact username: Rewrite
    Target address: 10.10.100.12:7068
    NAT Status: Auto Detect
    Reg-min-expiry: 3000 seconds
    Fast-register: Enabled
    Fast-register-int: 30 seconds

```

```
Register aggregate: Disabled
Registration Required: Disabled
Register Out Interval: 0 seconds
..
```

The following example shows how, in Cisco IOS XE Release 3.1.0S and later, the **show sbc sbe adjacencies detail** command lists peer information, including the current peer index, configured on an SBE:

```
Router# show sbc mat sbe adjacencies SIPPA detail
SBC Service "mat"
Adjacency SIPPA (SIP)
  Status: Attached
  Signaling address: 1.0.0.10:5068
  IPsec server port: 0
  Signaling-peer: 1.0.0.3:5068
  Signaling-peer status: Down
  Signaling-peer priority: 6
  Signaling-peer switch: on-fail
  Peer status: Down
  Current peer index: 0
  Force next hop: Yes
  Force next hop select: Out-of-dialog
  Account:
  Group: None
  In header profile: Default
  Out header profile: Default
  In method profile: Default
  Out method profile: Default
  Out error profile: Default
  In body profile: None
  Out body profile: None
  In UA option prof: Default
  Out UA option prof: Default
  In proxy opt prof: Default
  Out proxy opt prof: Default
  Priority set name: None
  Local-id: None
  Rewrite REGISTER: On
  Register contact username: Rewrite
  Target address: 1.0.0.3:5068
  NAT Status: Auto Detect
  Reg-min-expiry: 3000 seconds
  Fast-register: Enabled
  Fast-register-int: 30 seconds
  Register aggregate: Disabled
  Registration Required: Disabled
  Register Out Interval: 0 seconds
  Parse username params: Disabled
  Supported timer insert: Disabled
  Suppress Expires: Disabled
  p-asserted-id header-value: not defined
  p-assert-id assert: Disabled
  Authenticated mode: None
  Authenticated realm: None
```

In Cisco IOS XE Release 3.2S, the output of the **show sbc sbe adjacency detail** command was updated to include details about multiple SBC media bypass:

```
Router# show sbc MySBC sbe adjacencies ADJ1 detail
SBC Service MySBC
Adjacency ADJ1 (SIP)
  Status: Attached
```



```

Signaling address: 192.0.2.36.1:5060, VRF sidd_sipp1
IPsec server port: 0
Signaling-peer: 192.0.2.37.1:5060 (Default)

```

```

.
.
.

```

```

Media Bypass Tag List:
Tag 1: tag1
Tag 2: tag2
Media Bypass Max Out Data Length: 1024
Register unencrypted covert: Enabled

```

In Cisco IOS XE Release 3.3S, the output of the **show sbc sbe adjacency detail** command was updated to include details about the H.225 messages, whether the contact username in a SIP REGISTER request is in a rewrite mode or passthrough mode, and the local jitter ratio:

```

Router# show sbc MySBC sbe adjacencies ADJ1 detail
SBC Service "MySBC"
Adjacency h323adj (H.323)
Status: Detached
Signaling address: 0.0.0.0:1720 (default)
Signaling-peer: 0.0.0.0:1720 (default)
Admin Domain: None
Account:
Media passthrough: Yes
Group:
Hunting triggers: Global Triggers
Hunting mode: Global Mode
Techology Prefix:
H245 Tunnelling: Enabled
Fast-Slow Interworking: None
Trust-level: Untrusted
Call-security: Insecure
Realm: None
Warrant Match-Order: None
Local Jitter Ratio: 0/1000
H225 address block: Enabled
H225 address usage: h323id (default)
.
.
.
Rewrite REGISTER: Off
Register contact username: Rewrite as userid and digits
Target address: None
NAT Status: Auto Detect
Reg-min-expiry: 3000 seconds
Local Jitter Ratio: 0/1000
.
.
.

```

The following example shows the adjacencies that are configured on the SBE:

```

Router# show sbc mysbc sbe adjacencies

SBC Service ''mysbc''
Name Type State Description
-----
h323-7206-CG H.323 Attached
h323-ixvoice H.323 Attached
sip-60 SIP Attached
7600-phonel SIP Attached

```

```
7600-phone2 SIP Attached
sip-ixvoice SIP Attached
sip-7206-CG- SIP Attached
```

The following example shows the detailed output for the SoftSwitch adjacency, in which softswitch shielding is enabled. The Register Out Timer: field shows the time interval, in seconds, at which the SBC forwards the next REGISTER messages to the softswitch.

```
Router# show sbc mySbc sbe adjacencies SoftSwitch detail
SBC Service "mySbc"
Adjacency SoftSwitch (SIP)
  Status: Attached
  Signaling address: 100.100.100.100:5060, VRF Admin
  Signaling-peer: 10.10.51.10:5060
  Force next hop: No
  Account:
  Group: None
  In header profile: Default
  Out header profile: Default
  In method profile: Default
  Out method profile: Default
  In UA option prof: Default
  Out UA option prof: Default
  In proxy opt prof: Default
  Out proxy opt prof: Default
  Priority set name: None
  Local-id: None
  Rewrite REGISTER: Off
  Target address: None
  Register Out Timer: 36000 seconds
  Register Aggregate: Disabled
  NAT Status: Auto Detect
  Reg-min-expiry: 30 seconds
  Fast-register: Enabled
  Fast-register-int: 30 seconds
  Authenticated mode: None
  Authenticated realm: None
  Auth. nonce life time: 300 seconds
  IMS visited NetID: None
  Inherit profile: Default
  Force next hop: No
  Home network Id: None
  UnEncrypt key data: None
  SIPI passthrough: No
  Rewrite from domain: Yes
  Rewrite to header: Yes
  Media passthrough: No
  Preferred transport: UDP
  Hunting Triggers: Global Triggers
  Redirect mode: Pass-through
  Security: Untrusted
  Outbound-flood-rate: None
  Ping-enabled: No
  Signaling Peer Status: Not Tested
```

The following example displays the detailed output for the Cary-IP-PBX adjacency, including the Register Aggregate: field, which shows that aggregate registration is enabled:

```
Router# show sbc mySbc sbe adjacencies Cary-IP-PBX detail
SBC Service "mySBC"
Adjacency Cary-IP-PBX (SIP)
  Status: Attached
  Signaling address: 100.100.100.100:5060, VRF Admin
```

```

Signaling-peer:      10.10.51.10:5060
Force next hop:      No
Account:
Group:               None
In header profile:   Default
Out header profile:  Default
In method profile:   Default
Out method profile:  Default
In UA option prof:   Default
Out UA option prof:  Default
In proxy opt prof:   Default
Out proxy opt prof:  Default
Priority set name:    None
Local-id:            None
Rewrite REGISTER:    Off
Target address:      None
Register Out Timer:  1800 seconds
Register Aggregate: Enabled
NAT Status:          Auto Detect
Reg-min-expiry:      30 seconds
Fast-register:       Enabled
Fast-register-int:   30 seconds
Authenticated mode:  None
Authenticated realm: None
Auth. nonce life time: 300 seconds
IMS visited NetID:   None
Inherit profile:     Default
Force next hop:      No
Home network Id:     None
UnEncrypt key data:  None
SIPI passthrough:    No
Rewrite from domain: Yes
Rewrite to header:   Yes
Media passthrough:   No
Preferred transport: UDP
Hunting Triggers:    Global Triggers
Redirect mode:        Pass-through
Security:             Untrusted
Outbound-flood-rate: None
Ping-enabled:         No
Signaling Peer Status: Not Tested
Rewrite Request-uri: Enabled
Registration Monitor: Disabled

```

The following example displays the detailed output for the Cary-IP-PBX adjacency, including the Registration Monitor: field, which shows that registration monitoring is enabled:

```

Router# show sbc mySBC sbe adjacencies Cary-IP-PBX detail
SBC Service "mySbc"
Adjacency Cary-IP-PBX (SIP)
Status:                Attached
Signaling address:     100.100.100.100:5060, VRF Admin
Signaling-peer:        10.10.51.10:5060
Force next hop:        No
Account:
Group:                 None
In header profile:     Default
Out header profile:    Default
In method profile:     Default
Out method profile:    Default
In UA option prof:     Default
Out UA option prof:    Default
In proxy opt prof:     Default
Out proxy opt prof:    Default

```

```

Priority set name:      None
Local-id:              None
Rewrite REGISTER:     Off
Target address:        None
Register Out Timer:    1800 seconds
Register Aggregate:    Enabled
NAT Status:            Auto Detect
Reg-min-expiry:        30 seconds
Fast-register:         Enabled
Fast-register-int:     30 seconds
Authenticated mode:    None
Authenticated realm:   None
Auth. nonce life time: 300 seconds
IMS visited NetID:     None
Inherit profile:       Default
Force next hop:        No
Home network Id:       None
UnEncrypt key data:    None
SIPI passthrough:     No
Rewrite from domain:   Yes
Rewrite to header:     Yes
Media passthrough:     No
Preferred transport:   UDP
Hunting Triggers:     Global Triggers
Redirect mode:         Pass-through
Security:              Untrusted
Outbound-flood-rate:  None
Ping-enabled:          No
Signaling Peer Status: Not Tested
Rewrite Request-uri:   Disabled
Registration Monitor: Enabled

```

The following example displays the detailed output for the CCM135-IPV6 adjacency. This example also contains a new field, TLS Mutual Authentication, to indicate whether TLS Mutual Authentication is enabled on the adjacency.

```

Router# show sbc asr1 sbe adjacencies CCM135-IPV6 detail
SBC Service "asr1"
Adjacency CCM135-IPV6 (SIP)
  Status: Attached
  Signaling address: 2001:A401::33:33:36:1:5060
  Signaling-peer: 2001::10:0:50:135:5060 (Default)
  Force next hop: Yes
  Account:
  Group: v6
  In header profile: ccmpf1
  Out header profile: ccmpf1
  In method profile: cmmethod2
  Out method profile: cmmethod2
  In body profile: None
  Out body profile: None
  In UA option prof: Default
  Out UA option prof: Default
  In proxy opt prof: Default
  Out proxy opt prof: Default
  Priority set name: None
  Local-id: None
  Rewrite REGISTER: Off
  Register contact username: Rewrite
  Target address: None
  NAT Status: Force off
  Reg-min-expiry: 3000 seconds
  Fast-register: Enabled
  Fast-register-int: 30 seconds

```

```

Register aggregate:      Disabled
Registration Required:  Disabled
Register Out Interval:  0 seconds
Parse username params:  Disabled
Supported timer insert: Disabled
Suppress Expires:       Disabled
p-asserted-id header-value: not defined
p-assert-id assert:     Disabled
Authenticated mode:     None
Authenticated realm:    None
Auth. nonce life time:  300 seconds
IMS visited NetID:      None
Inherit profile:        Default
Force next hop:         Yes
Home network Id:        None
UnEncrypt key data:     None
SIPI passthrough:      No
Passthrough headers:   No
Media passthrough:     No
Preferred transport:    UDP
Incoming 100rel strip:  No
Incoming 100rel supp:  No
Out 100rel supp add:   No
Out 100rel req add:    No
Parse TGID parms:      No
IP-FQDN inbound:       No
IP-FQDN outbound:      No
FQDN-IP inbound:       No
FQDN-IP outbound:     No
Outbound Flood Rate:   None
Hunting Triggers:      Global Triggers
Add transport=tls param: Disabled
Redirect mode:          Pass-through
Security:                Untrusted-Unencrypted
TLS mutual authentication: No
Ping:                   Disabled
Ping Interval:          32 seconds
Ping Life Time:         32 seconds
Ping Peer Fail Count:   3
Ping Trap sending:      Enabled
Ping Peer Status:       Not Tested
Rewrite Request-uri:    Disabled
Registration Monitor:    Disabled
DTMF SIP NOTIFY Relay:  Enabled
DTMF SIP NOTIFY Interval: 2000
DTMF SIP default duration: 200
DTMF Preferred Method:  SIP NOTIFY
Realm :                 None
Statistics setting:     Summary

```

The following example shows the output of the **show sbc sbe adjacencies peers** command. The command lists all the peers configured on the SBEs for a specified adjacency:

```

Router# show sbc mat sbe adjacencies SIPPA peers
Configured peers
-----

```

Index	Priority	Status	Address:Port	Network
1	2	Down	5.5.5.5:5060	5.5.5.5/32
2	3	Down	22.22.22.22:2222	22.22.22.22/32

The following example shows the output of the **show sbc sbe adjacencies detail** command for an adjacency with IMX Rx settings:

```
Router# show sbc mySBC sbe adjacencies A_1 detail
```

```
SBC Service "mySBC"
Adjacency A_1 (SIP)
  Status: Detached
  Signaling address: 0.0.0.0:default
  IPsec server port: 0
  Signaling-peer: :5060 (Default)
  Signaling-peer status: Not Tested
  Signaling-peer priority: 2147483647
  Signaling-peer switch: always
  Peer status: Not Tested
  Force next hop: No
  Force next hop select: Out-of-dialog
  Account:
  Group: None
  In header profile: Default
  Out header profile: Default
  In method profile: Default
  Out method profile: Default
  Out error profile: Default
  In body profile: None
  Out body profile: None
  In UA option prof: Default
  Out UA option prof: Default
  In proxy opt prof: Default
  Out proxy opt prof: Default
  Priority set name: None
  Local-id: None
  Rewrite REGISTER: Off
  Register contact username: Rewrite
  Target address: None
  NAT Status: Auto Detect
  Reg-min-expiry: 3000 seconds
  Fast-register: Enabled
  Fast-register-int: 30 seconds
  Register aggregate: Disabled
  Registration Required: Disabled
  Register Out Interval: 0 seconds
  Parse username params: Disabled
  Supported timer insert: Disabled
  Suppress Expires: Disabled
  p-asserted-id header-value: not defined
  p-assert-id assert: Disabled
  Authenticated mode: None
  Authenticated realm: None
  Auth. nonce life time: 300 seconds
  IMS visited NetID: None
  Inherit profile: Default
  Force next hop: No
  Home network Id: None
  UnEncrypt key data: None
  SIPI passthrough: No
  Passthrough headers:
  Media passthrough: Yes
  Incoming 100rel strip: No
  Incoming 100rel supp: No
  Out 100rel supp add: No
  Out 100rel req add: No
  Parse TGID parms: No
```

```

IP-FQDN inbound:
IP-FQDN outbound:
FQDN-IP inbound:
FQDN-IP outbound:
Outbound Flood Rate:  None
Hunting Triggers:     Global Triggers
Add transport=tls param:  Disabled
Redirect mode:        Pass-through
Security:             Untrusted-Unencrypted
TLS mutual authentication: No
Ping:                 Disabled
Ping Interval:        32 seconds
Ping Life Time:       32 seconds
Ping Peer Fail Count: 3
Ping Trap sending:    Enabled
Ping Peer Status:     Not Tested
Rewrite Request-uri: Disabled
Registration Monitor: Disabled
DTMF SIP INFO Relay:  Auto_detect
DTMF SIP NOTIFY Relay: Enabled
DTMF SIP NOTIFY Interval: 2000
DTMF SIP default duration: 200
DTMF Preferred Method: SIP NOTIFY
Realm:                None
Statistics setting:   Summary
IMS Rx:                Enabled
IMS Rx pcrf host:     None
IMS Nass:              Disabled
IMS realm name:       Realm_1
PANI:
Warrant Match-Order:  None

```

The following example shows how, in Cisco IOS XE Release 3.4S and later, the output of the **show sbc sbe adjacencies detail** command includes the percentage of calls that has been set for use in the calculation of the MOS-CQE score. The output also includes the value that has been set for the Advantage factor.

```
Router# show sbc mySbc sbe adjacencies adj1 detail
```

```

SBC Service "mySbc"
Adjacency adj1 (H.323)
Status: Attached
Signaling address: 1.0.0.3:1720 (default)
Signaling-peer: 40.40.40.4:1720 (default)
Admin Domain: None
Account:
Media passthrough: Yes
Group:
Hunting triggers: Global Triggers
Hunting mode: Global Mode
Technology Prefix:
H245 Tunnelling: Enabled
Fast-Slow Interworking: None
Trust-level: Untrusted
Call-security: Insecure
Realm: None
Warrant Match-Order: None
Local Jitter Ratio: 1000/1000
Calc Moscq: 305/1000
G107A factor: 10
H225 address block: Disabled (default)
H225 address usage: h323id (default)

```

The following is a sample output of the **show sbc asr sbe adjacency mySBC detail** command in Cisco IOS XE Release 3.7S and later:

```
Router# show sbc asr sbe adjacency mySBC detail

Ims rf:           Enabled
```

Table 14 describes the significant field shown in the display.

**Table 14** *show sbc asr sbe adj mySBC detail Field Descriptions*

Field	Description
Ims rf	Value of the IMS Rf interface state for the adjacency. The valid values are Enabled or Disabled.

**Related Commands**

Command	Description
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
<b>g107a-factor</b>	Sets the Advantage (A) factor.
<b>g107 bpl</b>	Set the Packet-Loss Robustness (Bpl) factor.
<b>g107 ie</b>	Sets the Equipment Impairment (Ie) factor.
<b>local-jitter-ratio</b>	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
<b>show sbc sbe sip-method-stats</b>	Displays either a summary of statistics or detailed statistics pertaining to a SIP method.
<b>statistics-setting</b>	Configures an adjacency to support the SIP method statistics.
<b>tls mutual-authentication</b>	Enables TLS Mutual Authentication on an adjacency.



# show sbc sbe adjacencies authentication-realms

To display authentication realm on the specified adjacency, use the **show sbc sbe adjacencies authentication-realms** command in Privileged EXEC mode.

*show sbc sbc-name sbe adjacencies adjacency-name authentication-realms*

Syntax Description	Parameter	Description
	<i>sbc-name</i>	Specifies the name of the SBC service.
	<i>adjacency-name</i>	The name of the SIP adjacency whose details are to be displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to display all currently configured authentication-realms for all SIP adjacencies:

```
Router# show sbc mysbc sbe adjacencies sipAdjacency authentication-realms

Configured authentication realms
-----
Domain Username Password
abcdef.com abc abc
```

# show sbc sbe admin-domain

To list the administrative domains on the Session Border Controller (SBC) and per adjacency, use the **show sbc sbe admin-domain** command in the Privileged EXEC mode.

**show sbc *sbc-name* sbe admin-domain [adjacency]**

Syntax Description	
<i>sbc-name</i>	The name of the SBC service.
<b>adjacency</b>	Displays a list of the administrative domains on an adjacency.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows a list of the administrative domains on an SBC:

```
Router# show sbc mySBC sbe admin-domain
SBC Service "mySBC"
Global cac-policy-set:                2
Default call-policy-set/priority:    1/6

Administrative Domain      cac      call-policy-set/priority
                           policy-set  inbound-na  routing  outbound-na
-----
DOMAIN1                    2        2/1        2/1        2/1
```

The following example shows a list of the administrative domains on the adjacency:

```
Router# show sbc mySBC sbe admin-domain adjacency
SBC Service "mySBC"
Adjacency Name             Type  State  Admin-domain
-----
SIPP1A                     SIP   Attached  DOMAIN1
```

Related Commands	Command	Description
	<b>admin-domain</b>	Configures an administrative domain.
	<b>cac-policy-set global</b>	Activates the global CAC policy set within an SBE entity.
	<b>cac-policy-set (admin-domain)</b>	Configures the call admission control (CAC) policy set for an administrative domain.

---

<b>call-policy-set (admin-domain)</b>	Configures the inbound and outbound number analysis and routing policy set for an administrative domain.
<b>call-policy set default</b>	Configures a default policy set on the signaling border element (SBE) entity.

---

# show sbc sbe all-authentication-realms

To display all currently configured authentication-realms for all SIP adjacencies, use the **show sbc sbe all-authentication-realms** command in Privileged EXEC mode.

```
show sbc sbe all-authentication-realms
```

**Syntax Description** *.This command has no arguments or keywords*

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to display all currently configured authentication realms for all SIP adjacencies:

```
Router# show sbc mySbc sbe all-authentication-realms
```

```
Configured authentication realms
```

```
-----
```

```
Adjacency: SipToIsp42
```

```
Domain Username Password
```

```
Example.com usersbc passwordsbc
```

# show sbc sbe all-peers

To display peer information of all the adjacencies on an SBE, use the **show sbc sbe all-peers** command in privileged EXEC mode.

**show sbc *sbc-name* sbe all-peers**

## Syntax Description

<i>sbc-name</i>	The name of the SBC service.
-----------------	------------------------------

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how the **show sbc sbe all-peers** command displays peer information of all the adjacencies on an SBE:

```
Router# show sbc mat sbe all-peers
```

```
Configured peers
```

```
-----
```

```
Adjacency: SIPPA
```

Index	Priority	Status	Address:Port	Network
1	2	Down	5.5.5.5:5060	5.5.5.5/32
2	3	Down	22.22.22.22:2222	22.22.22.22/32

```
Adjacency: SIPPB
```

```
No peers specified for this adjacency.
```

```
Adjacency: server
```

```
No peers specified for this adjacency.
```

# show sbc sbe billing

To display the remote billing configuration, use the **show sbc sbe billing** command in Privileged EXEC mode.

```
show sbc sbc-name sbe billing instance [instance-index] [rf { realms [realm-name current5mins]
| cdfs cdf-name}]
```

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
<b>instance</b>	Displays the billing details for a specific sbe instance.
<i>instance-index</i>	Method for instance. Range: 0 to 7.
<b>rf</b>	Displays the Rf information.
<b>realms</b>	Displays all the Rf billing realms configurations, or a specific Rf billing realm configuration if the <i>realm-name</i> is configured.
<i>realm-name</i>	Name of the realm.
<b>current5mins</b>	Displays the stats for current 5-minute interval.
<b>cdfs</b>	Displays all the Rf billing Charging Data Function (CDF) configurations, or a specific Rf billing CDF configuration if the <i>cdf-name</i> is configured.
<i>cdf-name</i>	Name of the CDF.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.7S	This command was modified to display the billing information for an Rf billing instance.

## Examples

The following shows how to display the billing information for a packetcable billing instance:

```
Router# show sbc mySBC sbe billing instance
```

```
Billing Manager Information:
  Local IP address:      172.18.53.179
  LDR check time:       0:0
  Method                 packetcable-em
  Method                 packetcable-li
  Admin Status:         DOWN
  Operation Status:     DOWN
  Cache path:           usb0:billing_cache/
  Cache max size:       0 Kilobytes
  Cache minor-alarm:    97656 Kilobytes
  Cache major-alarm:    488281 Kilobytes
```

```
Cache critical-alarm:      976562 Kilobytes
Retry-interval:           20 secs
CDR Media-Info:           Not Included
CDR Endpoint-Info:       Addressing
```

```
Billing Methods:
  Radius client name:      ssss
  Instance:                 0
  Type:                     PACKET-CABLE
  Transport Mechanism Status: DOWN
  Active Calls Billed:     0
  Local IP Address:        172.18.53.179
  Deact-mode:              abort
  Admin Status:            DOWN
  Operation Status:        DOWN
  LDR check time:          0 :0
  Batch size:              0
  Batch time:              1000 ms
```

The following shows how to display the billing information for an Rf billing instance:

```
Router# show sbc asr sbe billing instance
```

```
Billing Manager Information:
Local IP address: 0.0.0.0
LDR check time: 0 :0
Method rf
Admin Status: UP
Operation Status: UP

Billing Methods:
Instance: 1
Type: 3GPP-RF
Transport Mechanism Status: UP
Active Calls Billed: 0
Local IP Address: 0.0.0.0
Deact-mode: abort
Admin Status: UP
Operation Status: UP
LDR check time: 24:0
Origin Host: yfasr.open-ims.test
Origin Realm: open-ims.test
```

Table 15 describes the significant fields shown in the display.

**Table 15** *show sbc asr sbe billing instance Field Descriptions*

Field	Description
Local IP address	IP address of the local billing manager.
LDR check time	Check time for LDR.
Operation Status	Operation status of the billing manager: UP or DOWN.
Instance	Instance for billing configuration.
Type	Billing type.
Transport Mechanism Status	Transport mechanism status of the billing methods: UP or DOWN.
Active Calls Billed	Active calls for billing.
Local IP Address	IP address of the local billing host.

**Table 15** *show sbc asr sbe billing instance Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Deact-mode	Deactive mode of the billing method.
Admin Status	Administrator status of the billing methods: UP or DOWN.
Operation Status	Operation status of the billing methods: UP or DOWN.
LDR check time	Check time for Long Duration Check (LDR).
Origin Host	DNS address or IP address of the origin host.
Origin Realm	DNS address or IP address of the origin realm.



## show sbc sbe blacklist

To list the limits in force for a particular source, whether from defaults or explicitly configured, in a form in which they can be entered into the command, use the **show sbc sbe blacklist** command in Privileged EXEC mode.

```
show sbc sbc-name sbe blacklist [source] {ipv4 IP address | ipv6 IP address}
```

Syntax Description		
<i>sbc-name</i>		Specifies the name of the SBC.
source		Specifies the source for which you want to display blacklisting information. This source is one of the following values: <ul style="list-style-type: none"> <li>VPN ID (Only VPN ID is permitted in the present implementation.)</li> </ul>
<i>ipv4</i> IP address		Shows configured blacklisting for a single IPv4 address.
<i>ipv6</i> IP address		Shows configured blacklisting for a single IPv6 address.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	The <i>ipv6</i> keyword was added.

**Usage Guidelines** Also listed are any defaults for a smaller scope configured at this address. Values not explicitly configured and, therefore, inherited from other defaults, are bracketed.

**Examples** The following example shows how to list blacklisting information for a specific VPN with a valid IPv4 address:

```
Router# show sbc mySbc sbe blacklist vpn3 ipv4 172.19.12.12
```

```
SBC Service mySbc SBE dynamic blacklist vpn3 172.19.12.12
```

```
vpn3 172.19.12.12
```

```
=====
```

Reason	Trigger Size	Trigger Period	Blacklisting Period
Authentication	(20)	10 ms	(1 hour)
Bad address	(20)	10 ms	(1 hour)
Routing	(20)	10 ms	(1 hour)
Registration	(5)	100 ms	(10 hours)
Policy	(20)	10 ms	(1 day)

```
Corrupt          40          10 ms          (1 hour)
Spam             2           10 secs         1 mins
```

Default for ports of vpn3 172.19.12.12

```
=====
Reason          Trigger          Trigger          Blacklisting
                Size            Period           Period
-----
Authentication   20             1 sec           1 hour
Bad address      20             1 sec           1 hour
Routing          20             1 sec           1 hour
Registration     5              30 sec          10 hours
Policy           20             1 sec           1 day
Corrupt          20             100 ms          1 hour
Spam             2              10 secs         1 mins
```

The following example shows the blacklist information for an IPv6 address:

```
Router# show sbc asr1 sbe blacklist ipv6 2001::10:0:0:1
SBC Service "asr1"
```

VRF: 2001::10:0:0:1

```
=====
Reason          Trigger          Trigger          Blacklisting
                Size            Period           Period
-----
Authentication   (4)             (100 ms)         (10 mins)
Bad-Address      (4)             (100 ms)         (10 mins)
Routing          (4)             (100 ms)         (10 mins)
Registration     (4)             (100 ms)         (10 mins)
Policy           (4)             (100 ms)         (10 mins)
Corruption       65535           1 mins           (10 mins)
Spam             (30)            (100 ms)         (10 mins)
```

Default for all ports of 2001::10:0:0:1

```
=====
Reason          Trigger          Trigger          Blacklisting
                Size            Period           Period
```

**Related Commands**

Command	Description
<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.
<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# show sbc sbe blacklist configured-limits

To list the explicitly configured limits, showing only the configured sources, use the **show sbc sbe blacklist configured-limits** command in Privileged EXEC mode.

Values that are not explicitly configured and therefore inherited from other defaults, are within brackets.

```
show sbc sbc-name sbe blacklist configured-limits
```

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC.
<b>Command Default</b>	No default behavior or values are available.	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	The output of this command was updated to include the blacklist alerts.

## Examples

The following command displays explicitly configured limits, displaying only the sources. Nonexplicitly configured values are displayed withing brackets:

```
Router(config-sbc-sbe)# show sbc mySbc sbe blacklist configured-limits
SBC Service "mySBC"
```

```
Blacklist Defaults
```

```
=====
```

Reason	Trigger Size	Trigger Period	Blacklisting Period	Minor Alert	Major Alert	Critical Alert
Auth-failure	(4)	(100 ms)	(10 mins)	not set	not set	not set
Bad-address	(4)	(100 ms)	(10 mins)	not set	not set	not set
RTG-policy-rejection	(4)	(100 ms)	(10 mins)	not set	not set	not set
Endpoint-registration	(4)	(100 ms)	(10 mins)	not set	not set	not set
CAC-policy-rejection	(4)	(100 ms)	(10 mins)	not set	not set	not set
Corrupt-message	(4)	(100 ms)	(10 mins)	not set	not set	not set
Spam	(30)	(100 ms)	(10 mins)	not set	not set	not set
NA-policy-rejection	(4)	(100 ms)	(10 mins)	not set	not set	not set

```
-----
```

```
VRF: 172.18.53.56
```

```
=====
```

Reason	Trigger Size	Trigger Period	Blacklisting Period	Minor Alert	Major Alert	Critical Alert
NA-policy-rejection	(4)	(100 ms)	(10 mins)	2	not set	not set

```
-----
```

Related Commands	Command	Description
	<b>critical-alert-size</b>	Configures the number of specified events that must occur before a critical alert is triggered.
	<b>major-alert-size</b>	Configures the number of specified events that must occur before a major alert is triggered.
	<b>minor-alert-size</b>	Configures the number of specified events that must occur before a minor alert is triggered.
	<b>reason</b>	Enables the entry of a user into a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, and global address space).
	<b>trigger-size</b>	Defines the number of specified events from the specified source that are allowed before blacklisting is triggered, and blocks all the packets from the source.
	<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the <b>trigger-size</b> command.
	<b>timeout</b>	Defines the length of time for which packets from the source are blocked, should the limit be exceeded.
	<b>show sbc sbe blacklist</b>	Lists the limits in force for a particular source (whether they are from defaults or are explicitly configured) in a form in which they can be entered in the CLI. Also listed are any defaults for a smaller scope configured at this address.
	<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits that cause sources to be blacklisted.

# show sbc sbe blacklist critical

To show all configured critical blacklists for IPv4 and IPv6 addresses, use the **show sbc sbe blacklist critical** command in Privileged EXEC mode.

```
show sbc sbc-name sbe blacklist [ critical ] { WORD } ipv4 addr [ tcp tcp-port | udp udp-port ]
```

```
show sbc sbc-name sbe blacklist critical { ipv4 addr | ipv6 addr } [ tcp tcp-port | udp udp-port ]
```

Syntax Description		
	<i>sbc-name</i>	Specifies the name of the SBC.
	<b>WORD</b>	Specifies the VPN ID for which you want to display critical blacklisting information.
	<i>ipv4</i>	Shows configured critical blacklisting for a single IPv4 address.
	<i>ipv6</i>	Shows configured critical blacklisting for a single IPv6 address.
	<i>addr</i>	IPv4 or IPv6 address.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	The <i>ipv6</i> keyword was added.

**Examples** The following example shows critical blacklist information for VPN ID 600 for a specific IPv4 address:

```
Router# show sbc test sbe blacklist critical 600 ipv4 10.0.120.12
SBC Service "test"
600 10.0.120.12
=====
Reason Trigger Trigger Blacklisting
Size Period Period
-----
Authentication (4) (100 ms) (10 mins)
Bad-Address (4) (100 ms) (10 mins)
Routing (4) (100 ms) (10 mins)
Registration (4) (100 ms) (10 mins)
Policy (4) (100 ms) (10 mins)
Corruption 2 1 secs (10 mins)
Spam 2 1 secs (10 mins)
Default for all ports of 600 10.0.120.12
=====
Reason Trigger Trigger Blacklisting
Size Period Period
-----
Authentication (4) (100 ms) (10 mins)
```

```
Bad-Address (4) (100 ms) (10 mins)
Routing (4) (100 ms) (10 mins)
Registration (4) (100 ms) (10 mins)
Policy (4) (100 ms) (10 mins)
Corruption (4) (100 ms) (10 mins)
Spam (30) (100 ms) (10 mins)
```

The following example shows critical blacklist information for a specific IPv6 address:

```
Router# show sbc asr1 sbe blacklist critical ipv6 2001::10:0:0:1
SBC Service "asr1"
```

```
VRF: 2001::10:0:0:1
=====
Reason          Trigger          Trigger          Blacklisting
                Size            Period           Period
Authentication  65535            1 mins           (10 mins)
```

```
-----
Default for all ports of 2001::10:0:0:1
=====
Reason          Trigger          Trigger          Blacklisting
                Size            Period           Period
```

**Related Commands**

Command	Description
<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.
<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# show sbc sbe blacklist critical configured-limits

To show all configured blacklisting limits for critical blacklists, use the **show sbc sbe blacklist critical configured-limits** command in Privileged EXEC mode.

```
show sbc sbc-name sbe blacklist critical configured-limits
```

Syntax Description		
	<i>sbc-name</i>	Specifies the name of the SBC.
	configured-limits	Shows all configured blacklisting limits for critical blacklists.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows the configured blacklisting limits for critical blacklists:

```
Router# show sbc test sbe blacklist critical configured-limits
```

Related Commands	Command	Description
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
	<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
	<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
	<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
	<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.
	<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# show sbc sbe blacklist critical current-blacklisting

To show all currently blacklisted addresses for critical blacklists, use the **show sbc sbe blacklist critical** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe blacklist critical current-blacklisting**

Syntax Description	
<i>sbc-name</i>	Specifies the name of the SBC.
current-blacklisting	Shows the currently blacklisted addresses for critical blacklists.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows the currently blacklisted addresses for critical blacklists:

```
Router# show sbc test sbe blacklist critical current-blacklisting
SBC Service "test" SBE dynamic blacklist current members
VRF: 600
=====
Source Source Blacklist Time
Address Port Reason Remaining
-----
10.0.120.12 All Corruption 585 secs
```

Related Commands	Command	Description
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
	<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
	<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
	<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.



<b>Command</b>	<b>Description</b>
<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.
<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# show sbc sbe blacklist current-blacklisting

To list the limit causing sources to be blacklisted, use the **show sbc sbe blacklist current-blacklisting** command in the Privileged EXEC mode.

**show sbc *sbc-name* sbe blacklist current-blacklisting**

<b>Syntax Description</b>	<i>sbc-name</i>	Defines the name of the service.
---------------------------	-----------------	----------------------------------

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows the current blacklisting information for the SBC:

```
Router# show sbc mySbc sbe blacklist current-blacklisting
```

```
SBC Service mySbc SBE dynamic blacklist current members
```

```
Global addresses
```

```
=====
```

Source Address	Source Port	Blacklist Reason	Time Remaining
125.125.111.123	All	Authentication	15 mins
125.125.111.253	UDP 85	Registration	10 secs
144.12.12.4	TCP 80	Corruption	Never ends
192.169.0.9	All	Spam	49 secs

```
VRF: vpn3
```

```
=====
```

Source Address	Source Port	Blacklist Reason	Time Remaining
132.15.1.2	TCP 285	Registration	112 secs
172.23.22.2	All	Policy	10 hours
192.169.0.9	All	Spam	49 secs

Related Commands	Command	Description
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
	<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
	<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
	<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
	<b>show sbc sbe blacklist</b>	Lists the limits in force for a particular source (whether they are from defaults or explicitly configured) in a form in which they can be entered into the CLI. Also listed are any defaults for a smaller scope configured at this address.
	<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.

# show sbc sbe cac-policy-set

To list detailed information pertaining to a given entry in a call admission control (CAC) policy table, use the **show sbc sbe cac-policy-set** command in the privileged EXEC mode.

```
show sbc name sbe cac-policy-set [id [table name [entry id]] | global [table name [entry id]]]
[detail]
```

## Syntax Description

<i>name</i>	Name of the Session Border Controller (SBC) service.
<i>id</i>	CAC policy set ID, that is, the numeric identifier of the CAC policy set to which the table belongs. Valid range is 1 through 2147483647.
<b>table</b> <i>name</i>	<b>table</b> specifies the table in a CAC policy set.  <i>name</i> is the name of a table.
<b>entry</b> <i>id</i>	<b>entry</b> specifies the numeric identifier of the CAC entry you want to display. It displays the output in detail.  <i>id</i> is the CAC entry ID.
<b>global</b>	Displays the global CAC policy sets.
<b>detail</b>	Displays information pertaining to the CAC policy sets in detail format.

## Command Default

Brief output format is the default.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command was modified. Callee Bandwidth-Field and Caller Bandwidth-Field were added to the output.
Cisco IOS XE Release 2.5.1	This command was modified. The output of this command was modified to show the caller and callee media capabilities and extra terminal capability exchange message capabilities.
Cisco IOS XE Release 2.6	This command was modified. The output of this command was modified to show IPv6 call type and the caller and callee secure media.
Cisco IOS XE Release 3.1S	This command was modified. The command output was modified to display: <ul style="list-style-type: none"> <li>IMS Rx information: Ims rx preliminary-aar</li> <li>Ims media-service</li> <li>Asymmetric payload types that are allowed or disallowed</li> </ul>

Release	Modification
Cisco IOS XE Release 3.2S	This command was modified. The <b>active</b> keyword was replaced with the <b>global</b> keyword. The output of the <b>show sbc sbe cac-policy-set table entry detail</b> command was updated to include details about multiple SBC media bypass.
Cisco IOS XE Release 3.3S	This command was modified. The output of the <b>show sbc sbe cac-policy-set</b> command was updated to include information about the billing filter and the rejection counts of the failed CAC policies.
Cisco IOS XE Release 3.5S	This command was modified. The output of the <b>show sbc sbe cac-policy-set</b> command was updated to include information about the <b>branch</b> command settings.

### Usage Guidelines

There are two output formats, brief (default) and detail. The brief version displays important high-level information for each entry on a single line. The detail version displays the policy sets, tables, and entry values in detail.

This command allows filters according to the policy set IDs, the active policy sets, table names, and entry IDs. The default displays all the policy sets, tables, and entries.

If the entry option is specified, the information is displayed in the detail format.

### Examples

The following example shows the output of the **show sbc sbe cac-policy-set table entry** command that was updated in Cisco IOS XE Release 3.3S to include information about the billing filter and the rejection counts of the failed CAC policies:

```
Router# show sbc mySBC sbe cac-policy-set 1 table t1 entry 1

SBC Service "mySBC"
CAC Averaging period 1: 60 sec
CAC Averaging period 2: 0 sec

CAC Policy Set 1
  Global policy set: Yes
  Description:
  First CAC table: t1
  First CAC scope: global

Table name: t1
  Description:
  Table type: policy-set
  Total call setup failures (due to non-media limits): 0

Entry 1
  CAC scope:
  CAC scope prefix length: 0
  Action: CAC complete
  Number of call setup failures (due to non-media limits): 0
  No. of registrations rejected (due to registration limits): 0

Max calls per scope:                               Unlimited
No. of events rejected due to Max Call Limit:      0

Max reg. per scope:                                 Unlimited
No. of events rejected due to Max Reg limit:       0

Max channels per scope:                             Unlimited
```

```
Max updates per scope: Unlimited
Max bandwidth per scope: Unlimited
```

```

                                     Averaging-period 1      Averaging-period
2
Max call rate per scope:              Unlimited            Unlimited
No. of events rejected due to Max call rate: 0                0

Max reg. rate per scope:              Unlimited            Unlimited
No. of events rejected due to Max reg rate: 0                0

Max in-call message rate:            Unlimited            Unlimited
No. of events rejected due to Max in-call rate: 0            0

Max out-call message rate:           Unlimited            Unlimited
No. of events rejected due to Max Out call rate: 0            0

```

Timestamp when the rejection counts were last reset: 2011/03/07 04:38:24

```

.....
media bandwidth policing:            Degrade
Media policy limit:                  mp1
IPsec maximum registers:             10
IPsec maximum calls:                 5
Billing filter :                   enable
Billing filter methods:          xml

```

The following example shows the output of the **show sbc sbe cac-policy-set table entry detail** command that was updated in Cisco IOS XE Release 3.2S to include details about multiple SBC media bypass:

```

Router# show sbc asr8 sbe cac-policy-set 1 table table1 entry 1 detail
SBC Service "asr8"

CAC Policy Set 1
Active policy set: No
Description:
Averaging period: 60 sec
First CAC table:
First CAC scope: global

Table name: table1
Description:
Table type: policy-set

Entry 1
Action: CAC Complete
...
Media Bypass Type: Full Partial
Caller Media Bypass: Enabled
Callee Media Bypass: Enabled

```

In Cisco IOS XE Release 2.6, the command output was modified to show the caller and callee media capabilities and extra TCS message capabilities, and the caller and callee sides configured with granular secure media:

```

Router# show sbc mySBC sbe cac-policy-set 2 table table2 entry 1
SBC Service "mySBC"

CAC Policy Set 2

```

```

Active policy set: No
Description:
Averaging period: 60 sec
First CAC table: 1
First CAC scope: global
First CAC prefix length: 4294967256

Table name: table2
Description:
Table type: policy-set
Total call setup failures (due to non-media limits): 0

Entry 1
CAC scope:
CAC scope prefix length: 0
Action: CAC complete
Number of call setup failures (due to non-media limits): 0
Max calls per scope:      Unlimited      Max call rate per scope: Unlimited
Max in-call rate:        Unlimited      Max out-call rate:      Unlimited
Max reg. per scope:      Unlimited      Max reg. rate per scope: Unlimited
Max channels per scope:  Unlimited      Max updates per scope:  Unlimited
Early media:             Allowed      Early media direction:  Both
Early media timeout:     None      Transcoder per scope:   Allowed
Callee Bandwidth-Field: None      Caller Bandwidth-Field: None
Media bypass:             Allowed
Renegotiate Strategy:    Delta
Max bandwidth per scope: Unlimited

...

Caller media capabilities:      <codec-list-name>
Callee media capabilities:    <codec-list-name>
Extra TCS capabilities:       <codec-list-name>

Caller unsignaled secure media: Allowed
Callee unsignaled secure media: Allowed
Caller tel-event payload type: Default
Callee tel-event payload type: Default
Media flag:
  Ignore bandwidth-fields (b=), Telephone Event Interworking
Restrict codecs to list:      Default
Restrict caller codecs to list: Default
Restrict callee codecs to list: Default
Maximum Call Duration:       Unlimited

```

The following example displays in detail format the output for CAC policy set 10, table 10, and entry 1 with the IPv6 details included in Cisco IOS XE Release 2.6:

```
Router# show sbc asr1 sbe cac-policy-set 10 table table10 entry 1 detail
```

```

SBC Service "asr1"

CAC Policy Set 10
Active policy set: Yes
Description:
Averaging period: 60 sec
First CAC table: table10
First CAC scope: global

Table name: table10
Description:
Table type: limit dst-adjacency
Total call setup failures (due to non-media limits): 0

```

```

Entry 1
Match value: CCM135-IPV6
Match prefix length: 0
Action: CAC complete
Number of call setup failures (due to non-media limits): 0
Max calls per scope:      Unlimited      Max call rate per scope: Unlimited
Max in-call message rate: Unlimited      Max out-call message rate: Unlimited
Max reg. per scope:      Unlimited      Max reg. rate per scope: Unlimited
Max channels per scope: Unlimited      Max updates per scope:  Unlimited
Early media:             Allowed        Early media direction:  Both
Early media timeout:     None          Transcoder per scope:  Allowed
Callee Bandwidth-Field: None          Caller Bandwidth-Field: None
Media bypass:            Allowed
Renegotiate Strategy:   Delta
Max bandwidth per scope: Unlimited
SRTP Transport:         Trusted-Only (by default)
Caller hold setting:     Standard
Callee hold setting:    Standard
Caller privacy setting:  Never hide
Callee privacy setting: Never hide
Caller voice QoS profile: Default
Callee voice QoS profile: Default
Caller video QoS profile: Default
Callee video QoS profile: Default
Caller sig QoS profile:  Default
Callee sig QoS profile: Default
Caller inbound SDP policy: None
Callee inbound SDP policy: None
Caller outbound SDP policy: None
Callee outbound SDP policy: None
SDP Media Profile      : None
Caller media disabled:  None
Callee media disabled: None
Caller un signaled secure media: Not Allowed
Callee un signaled secure media: Not Allowed
Caller tel-event payload type: Default
Callee tel-event payload type: Default
Media flag:            None

Restrict codecs to list:      Default
Restrict caller codecs to list: Default
Restrict callee codecs to list: Default
Caller media caps list:      None
Callee media caps list:     None
TCS extra codec list:        None
Caller media-type:           Inherit (default)
Callee media-type:         IPv6
Maximum Call Duration:       Unlimited

```

The following example displays in detail format the output for CAC policy set 1, table 1, and entry 1, including the Callee Bandwidth-Field and Caller Bandwidth-Field introduced in Cisco IOS XE Release 2.5:

```

Router# show sbc SBC1 sbe cac-policy-set 1 table 1 entry 1
SBC Service "SBC1"

CAC Policy Set 1
Active policy set: No
Description: This is a description for cac-policy-set 1
Averaging period: 60 sec
First CAC table: 1
First CAC scope: call

```



```

Table name: 1
Description:
Table type: policy-set                               Total call failures: 0

Entry 1
CAC scope: call
Action: CAC complete                                Number of calls rejected: 0
Max calls per scope:      Unlimited                 Max call rate per scope: Unlimited
Max in-call rate:        Unlimited                 Max out-call rate:      Unlimited
Max reg. per scope:      Unlimited                 Max reg. rate per scope: Unlimited
Max channels per scope:  Unlimited                 Max updates per scope:  1
Early media:             Allowed                   Early media direction: Both
Early media timeout:     None                      Transcoder per scope:  Allowed
Callee Bandwidth-Field: TIAS-to-AS               Caller Bandwidth-Field: AS-to-TIAS
Media bypass:            Allowed
Media flag:              Not Set
Renegotiate Strategy:   Delta
Max bandwidth per scope: Unlimited
SRTP Transport:         Trusted-Only (by default)
Caller hold setting:    Standard
Callee hold setting:   Standard
Caller privacy setting: Never hide
Callee privacy setting: Never hide
Caller voice QoS profile: Default
Caller video QoS profile: Default
Caller sig QoS profile: Default
Callee voice QoS profile: Default
Callee video QoS profile: Default
Callee sig QoS profile: Default
Restrict codecs to list: Default
Restrict caller codecs to list: Default
Restrict callee codecs to list: Default
Caller inbound SDP policy: None
Caller outbound SDP policy: None
Callee inbound SDP policy: None
Callee outbound SDP policy: None

```

The following example displays in brief format the information pertaining to global CAC policy set 6:

```

Router# show sbc SBC1 sbe cac-policy-set global
SBC Service "SBC1"

CAC Policy Set 6
Global policy set: Yes
First CAC table: white-list1
First CAC scope: category

Table name: white-list1
Table type: limit category                               Total call failures: 0
Entry  Match value                                     Action              Failures
-----  -----
2       non-emergency                                   white-list2         0

Table name: white-list2
Table type: policy-set                               Total call failures: 0
Entry  Scope                                           Action              Failures
-----  -----
1       call                                               Complete            0

```

The following example displays the detailed output for global CAC policy set 2:

```
Router# show sbc mySBC sbe cac-policy-set global detail
```

```

SBC Service "mySBC"
CAC Averaging period 1: 100 sec
CAC Averaging period 2: 1500 sec

CAC Policy Set 2
Global policy set: Yes
Description:
First CAC table: 1
First CAC scope: src-adjacency

Table name: 1
Description:
Table type: limit adjacency
Total call setup failures (due to non-media limits): 0

Entry 1
Match value: SIP1A
Match prefix length: 0
Action: CAC complete
Number of call setup failures (due to non-media limits): 0

Max calls per scope:      1                Max reg. per scope:      Unlimited
Max channels per scope:  Unlimited          Max updates per scope:  Unlimited
Max bandwidth per scope: Unlimited

Max call rate per scope:      Averaging-period 1    Averaging-period 2
Max reg. rate per scope:      Unlimited              Unlimited
Max in-call message rate:     Unlimited              Unlimited
Max out-call message rate:    Unlimited              Unlimited

Early media:                Allowed              Early media direction: Both
Early media timeout:         None                 Transcoder per scope:  Allowed
Callee Bandwidth-Field:     None                 Caller Bandwidth-Field: None
Media bypass:                Allowed              Asymmetric Payload Type: Not Set
Renegotiate Strategy:       Delta
SRTP Transport:              Trusted-Only (by default)
Caller hold setting:         Standard
Callee hold setting:        Standard
Caller limited-privacy-service: Never hide identity
Callee limited-privacy-service: Never hide identity
Caller privacy-service:      Not set
Callee privacy-service:     Not set
Caller edit-privacy-request: Not set
Callee edit-privacy-request: Not set
Caller edit-privacy-request sip strip: Not set
Callee edit-privacy-request sip strip: Not set
Caller edit-privacy-request sip insert: Not set
Callee edit-privacy-request sip insert: Not set
Caller voice QoS profile:    Default
Callee voice QoS profile:   Default
Caller video QoS profile:    Default
Callee video QoS profile:   Default
Caller sig QoS profile:      Default
Callee sig QoS profile:     Default
Caller inbound SDP policy:   None
Callee inbound SDP policy:  None
Caller outbound SDP policy:  None
Callee outbound SDP policy: None
SDP Media Profile           :   None
Caller media disabled:       None
Callee media disabled:      None
Caller unsignaled secure media: Not Allowed
Callee unsignaled secure media: Not Allowed
Caller response downgrade support: No

```

```

Callee response downgrade support: No
Caller retry rtp support: No
Callee retry rtp support: No
Resend sdp answer in 200ok: No
Caller tel-event payload type: Default
Callee tel-event payload type: Default
Media flag: None
Restrict codecs to list: Default
Restrict caller codecs to list: Default
Restrict callee codecs to list: Default
Codec preference list: Default
Caller Codec profile: None
Callee Codec profile: None
Caller media caps list: None
Callee media caps list: None
TCS extra codec list: None
Caller media-type: Inherit (default)
Callee media-type: Inherit (default)
Caller Media Bypass: Inherit (default)
Callee Media Bypass: Inherit (default)
Media Bypass Type: Not set
Callee local transfer support: Inherit (default)
Maximum Call Duration: Unlimited
Caller SRTP support: Inherit (default)
Callee SRTP support: Inherit (default)
SRTP Interworking: Inherit (default)
SRTP media Interworking: Inherit (default)
Ims rx preliminary-aar: Disabled(default)
Ims media-service: None(default)
media bandwidth policing: Inherit(default)
Caller ptime: None (default)
Callee ptime: None (default)
Caller codec variant conversion: Disabled (default)
Callee codec variant conversion: Disabled (default)
Caller inband DTMF mode: Inherit(default)
Callee inband DTMF mode: Inherit(default)
Caller Port Range Tag: Inherit (default)
Callee Port Range Tag: Inherit (default)
Session refresh renegotiation: Inherit(default)

Entry 2
Match value: SIPPlB
Match prefix length: 0
Action: CAC complete
Number of call setup failures (due to non-media limits): 0

Max calls per scope: 4 Max reg. per scope: Unlimited
Max channels per scope: Unlimited Max updates per scope: Unlimited
Max bandwidth per scope: Unlimited
Max call rate per scope: Unlimited Averaging-period 1 Averaging-period 2
Max reg. rate per scope: Unlimited Unlimited
Max in-call message rate: Unlimited Unlimited
Max out-call message rate: Unlimited Unlimited

Early media: Allowed Early media direction: Both
Early media timeout: None Transcoder per scope: Allowed
Callee Bandwidth-Field: None Caller Bandwidth-Field: None
Media bypass: Allowed Asymmetric Payload Type: Not Set
Renegotiate Strategy: Delta
SRTP Transport: Trusted-Only (by default)
Caller hold setting: Standard
Callee hold setting: Standard
Caller limited-privacy-service: Never hide identity

```

```

Callee limited-privacy-service: Never hide identity
Caller privacy-service: Not set
Callee privacy-service: Not set
Caller edit-privacy-request: Not set
Callee edit-privacy-request: Not set
Caller edit-privacy-request sip strip: Not set
Callee edit-privacy-request sip strip: Not set
Caller edit-privacy-request sip insert: Not set
Callee edit-privacy-request sip insert: Not set
Caller voice QoS profile: Default
Callee voice QoS profile: Default
Caller video QoS profile: Default
Callee video QoS profile: Default
Caller sig QoS profile: Default
Callee sig QoS profile: Default
Caller inbound SDP policy: None
Callee inbound SDP policy: None
Caller outbound SDP policy: None
Callee outbound SDP policy: None
SDP Media Profile : None
Caller media disabled: None
Callee media disabled: None
Caller unsignaled secure media: Not Allowed
Callee unsignaled secure media: Not Allowed
Caller response downgrade support: No
Callee response downgrade support: No
Caller retry rtp support: No
Callee retry rtp support: No
Resend sdp answer in 200ok: No
Caller tel-event payload type: Default
Callee tel-event payload type: Default
Media flag: None
Restrict codecs to list: Default
Restrict caller codecs to list: Default
Restrict callee codecs to list: Default
Codec preference list: Default
Caller Codec profile: None
Callee Codec profile: None
Caller media caps list: None
Callee media caps list: None
TCS extra codec list: None
Caller media-type: Inherit (default)
Callee media-type: Inherit (default)
Caller Media Bypass: Inherit (default)
Callee Media Bypass: Inherit (default)
Media Bypass Type: Not set
Callee local transfer support: Inherit (default)
Maximum Call Duration: Unlimited
Caller SRTP support: Inherit (default)
Callee SRTP support: Inherit (default)
SRTP Interworking: Inherit (default)
SRTP media Interworking: Inherit (default)
Ims rx preliminary-aar: Disabled(default)
Ims media-service: None(default)
media bandwidth policing: Inherit(default)
Callerptime: None (default)
Calleeptime: None (default)
Caller codec variant conversion: Disabled (default)
Callee codec variant conversion: Disabled (default)
Caller inband DTMF mode: Inherit(default)
Callee inband DTMF mode: Inherit(default)
Caller Port Range Tag: Inherit (default)
Callee Port Range Tag: Inherit (default)
Session refresh renegotiation: Inherit(default)

```

The following command output shows that the SBC is configured to allow Asymmetric Payload Types:

```
Router(config)# show sbc RAND sbe cac-policy-set 1 TAB1

SBC Service "RAND"

CAC Policy Set 1
  Active policy set: Yes
  Description:
  Averaging period: 60 sec
  First CAC table: TAB1
  First CAC scope: global

Table name: TAB1
  Description:
  Table type: policy-set
  Total call setup failures (due to non-media limits): 0

Entry 1
  CAC scope:
  CAC scope prefix length: 0
  Action: CAC complete
  Number of call setup failures (due to non-media limits): 0
  Max calls per scope:           Unlimited           Max call rate per scope:           Unlimited
  Max in-call message rate:      Unlimited           Max out-call message rate:         Unlimited
  Max reg. per scope:            Unlimited           Max reg. rate per scope:           Unlimited
  Max channels per scope:        Unlimited           Max updates per scope:             Unlimited
  Early media:                   Allowed           Early media direction:             Both
  Early media timeout:           None             Transcoder per scope:              Allowed
  Callee Bandwidth-Field:        AS-to-TIAS      Caller Bandwidth-Field:            None
  Asymmetric Payload Types: Allowed           Media bypass:                       Allowed
  Renegotiate Strategy:         Delta
  Max bandwidth per scope:      Unlimited
  SRTP Transport:               Trusted-Only (by default)
  Caller hold setting:          Standard
  Callee hold setting:          Standard
  Caller privacy setting:       Never hide
  Callee privacy setting:       Never hide
  Caller voice QoS profile:     Default
  Callee voice QoS profile:     Default
  Caller video QoS profile:     Default
  Callee video QoS profile:     Default
  Caller sig QoS profile:       Default
  Callee sig QoS profile:       Default
  Caller inbound SDP policy:    None
  Callee inbound SDP policy:    None
  Caller outbound SDP policy:   None
  Callee outbound SDP policy:   None
  SDP Media Profile             :           None
  Caller media disabled:        None
  Callee media disabled:        None
  Caller unsignaled secure media: Not Allowed
  Callee unsignaled secure media: Not Allowed
  Caller tel-event payload type: Default
  Callee tel-event payload type: Default
  Media flag:                   None

Restrict codecs to list:       Default
Restrict caller codecs to list: Default
Restrict callee codecs to list: Default
Caller media-type:             Inherit (default)
Callee media-type:             Inherit (default)
```

Maximum Call Duration: Unlimited

The following example shows the output of the **show sbc sbe cac-policy-set detail** command that was updated in Cisco IOS XE Release 3.5S to include information about the **branch** command settings:

Router# **show sbc SBC2 sbe cac-policy-set 1 detail**

SBC Service "SBC2"  
CAC Averaging period 1: 60 sec  
CAC Averaging period 2: 0 sec

CAC Policy Set 1  
Global policy set: Yes  
Description:  
First CAC table: 1  
First CAC scope: global

Table name: 1  
Description:  
Table type: policy-set  
Total call setup failures (due to non-media limits): 0

Entry 1  
CAC scope:  
CAC scope prefix length: 0  
Action: CAC complete  
Number of call setup failures (due to non-media limits): 0  
No. of registrations rejected (due to registration limits): 0

Max calls per scope: Unlimited  
No. of events rejected due to Max Call Limit: 0

Max reg. per scope: Unlimited  
No. of events rejected due to Max Reg limit: 0

Max channels per scope: Unlimited  
Max updates per scope: Unlimited  
Max bandwidth per scope: Unlimited

2 Averaging-period 1 Averaging-period

Max call rate per scope: Unlimited Unlimited  
No. of events rejected due to Max call rate: 0 0

Max reg. rate per scope: Unlimited Unlimited  
No. of events rejected due to Max reg rate: 0 0

Max in-call message rate: Unlimited Unlimited  
No. of events rejected due to Max in-call rate: 0 0

Max out-call message rate: Unlimited Unlimited  
No. of events rejected due to Max Out call rate: 0 0

Timestamp when the rejection counts were last reset: 2011/10/11 04:40:42

Early media: Allowed Early media direction: Both  
Early media timeout: None Transcoder per scope: Allowed  
Callee Bandwidth-Field: None Caller Bandwidth-Field: None  
Branch Bandwidth-Field: None  
Media bypass: Allowed Asymmetric Payload Type: Not Set  
Renegotiate Strategy: Delta

```

SRTP Transport:                               Trusted-Only (by default)
Caller hold setting:                           Standard
Callee hold setting:                           Standard
Branch hold setting:                           Standard
Caller limited-privacy-service:                 Never hide identity
Callee limited-privacy-service:                 Never hide identity
Caller privacy-service:                         Not set
Callee privacy-service:                         Not set
Branch privacy-service:                         Not set
Caller edit-privacy-request:                     Not set
Callee edit-privacy-request:                     Not set
Branch edit-privacy-request:                     Not set
Caller edit-privacy-request sip strip:           Not set
Callee edit-privacy-request sip strip:           Not set
Branch edit-privacy-request sip strip:           Not set
Caller edit-privacy-request sip insert:          Not set
Callee edit-privacy-request sip insert:          Not set
Branch edit-privacy-request sip insert:          Not set
Caller voice QoS profile:                       Default
Callee voice QoS profile:                       Default
Branch voice QoS profile:                       Default
Caller video QoS profile:                       Default
Callee video QoS profile:                       Default
Branch video QoS profile:                       Default
Caller sig QoS profile:                         Default
Callee sig QoS profile:                         Default
Branch sig QoS profile:                         Default
Caller inbound SDP policy:                       None
Callee inbound SDP policy:                       None
Branch inbound SDP policy:                       None
Caller outbound SDP policy:                       None
Callee outbound SDP policy:                       None
Branch outbound SDP policy:                       None
SDP Media Profile                               :       None
Caller Generic Stream:                           Default
Callee Generic Stream:                           Default
Branch Generic Stream:                           Default
Caller media disabled:                           None
Callee media disabled:                           None
Branch media disabled:                           None
Caller unsignaled secure media:                   Not Allowed
Callee unsignaled secure media:                   Not Allowed
Branch unsignaled secure media:                   Not Allowed
Caller response downgrade support:                 No
Callee response downgrade support:                 No
Branch response downgrade support:                 No
Caller retry rtp support:                           No
Callee retry rtp support:                           No
Branch retry rtp support:                           No
Resend sdp answer in 200ok:                       No
Caller tel-event payload type:                     Default
Callee tel-event payload type:                     Default
Branch tel-event payload type:                     Default
Media flag:                                         None
Restrict codecs to list:                           Default
Restrict caller codecs to list:                     Default
Restrict callee codecs to list:                     Default
Restrict branch codecs to list:                     Default
Codec preference list:                             Default
Caller Codec profile:                             None
Callee Codec profile:                             None
Branch Codec profile:                             None
Caller media caps list:                             None
Callee media caps list:                             None

```

```

Branch media caps list:          None
TCS extra codec list:          None
Caller media-type:              Inherit (default)
Callee media-type:             Inherit (default)
Branch media-type:              Inherit (default)
Caller Media Bypass:            Inherit (default)
Callee Media Bypass:           Disabled
Branch Media Bypass:            Inherit (default)
Media Bypass Type:              All (Hairpin, Partial, Full)
Callee local transfer support: Inherit (default)
Maximum Call Duration:          Unlimited
Caller SRTP support:            Inherit (default)
Callee SRTP support:           Inherit (default)
Branch SRTP support:            Inherit (default)
SRTP Interworking:              Inherit (default)
SRTP media Interworking:        Inherit (default)
Ims rx preliminary-aar:         Disabled(default)
Ims media-service:              None(default)
media bandwidth policing:       Inherit(default)
Billing filter:                  Inherit(default)
Caller ptime:                    None (default)
Callee ptime:                   None (default)
Branch ptime:                     None (default)
Caller codec variant conversion: Disabled (default)
Callee codec variant conversion: Disabled (default)
Branch codec variant conversion: Disabled (default)
Caller inband DTMF mode:         Inherit(default)
Callee inband DTMF mode:        Inherit(default)
Branch inband DTMF mode:         Inherit(default)
Media policy limit table name:   None
IPsec maximum registers:         Unlimited (default)
IPsec maximum calls:             Unlimited (default)
Caller Port Range Tag:           Inherit (default)
Callee Port Range Tag:          Inherit (default)
Branch Port Range Tag:           Inherit (default)
Session refresh renegotiation:   Inherit(default)

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>cac-policy-set</b>	Creates a new CAC policy set, copies an existing complete policy set, swaps the references of a complete policy set to another policy set, or sets the averaging period for rate calculations in a CAC policy set.
<b>cac-policy-set global</b>	Activates the global CAC policy set within an SBE entity.



# show sbc sbe call-policy-set

To show the properties associated with a given policy set, use the **show sbc sbe call-policy-set** command in Privileged EXEC mode.

```
show sbc sbc-name sbe call-policy-set {Routing-policy-set-ID {detail | number-analysis-tables
{detail} | routing-tables {detail} | table table-name {detail | entry entry-id detail}} | default
{detail | number-analysis-tables {detail} | routing-tables {detail} | table table-name {detail
| entry entry-id detail}} | detail}
```

Syntax Description		
	<i>sbc-name</i>	The name of the Session Border Controller (SBC) service.
	<i>Routing-policy-set-ID</i>	ID of the routing-policy-set.
	<b>detail</b>	Shows the detailed information for call policy set.
	<b>number-analysis-tables</b>	Shows all number analysis tables.
	<b>routing-tables</b>	Shows all routing policy tables.
	<b>table</b>	Filters based on the call table.
	<i>table-name</i>	Name of the call table to be displayed.
	<b>entry</b>	Filters based on the call-table-entry ID.
	<i>entry-id</i>	Entry ID of the call table.
	<b>default</b>	Shows the default call policy set.
	<b>detail</b>	Shows details of all the call-policy-sets.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The output was updated with information about the first outbound number analysis table and the first inbound number analysis table. This command provides two forms of outputs: the brief (default) and the detailed. The brief version displays important high-level information for each entry on a single line. The detail version displays the entire policy-set, table, and entry values in detail.

**Examples** The following example shows a sample output of the **show sbc sbe call-policy-set** command:

```
Router# show sbc mySBC sbe call-policy-set
SBC Service "mySBC"

Policy set 1
  Default policy set          : No
```

```

First inbound NA table      :
First call routing table    : TAB1
First reg routing table     : TAB2
First outbound NA table     :
    
```

```

Table Name                  : TAB1
Class                       : Routing
Table type                  : rtg-src-adj
Total Call-policy Failures : 0 (0 *)
Entry      Match Value      Destination Adjacency  Action
-----
1          SIPPIA           SIPPIB                 Routing complete
2          SIPPIB           SIPPIA                 Routing complete
    
```

```

Table Name                  : TAB2
Class                       : Routing
Table type                  : rtg-src-adj
Total Call-policy Failures : 0 (0 *)
Entry      Match Value      Destination Adjacency  Action
-----
1          SIPPIA           Registrar              Routing complete
2          SIPPIB           Registrar              Routing complete
    
```

```

Policy set 2
Default policy set         : Yes (priority 1)
First inbound NA table     :
First call routing table   : TAB1
First reg routing table    : TAB2
First outbound NA table    :
    
```

```

Table Name                  : TAB1
Class                       : Routing
Table type                  : rtg-src-adj
Total Call-policy Failures : 0 (0 *)
Entry      Match Value      Destination Adjacency  Action
-----
1          SIPPIA           SIPPIB                 Routing complete
2          SIPPIB           SIPPIA                 Routing complete
    
```

```

Table Name                  : TAB2
Class                       : Routing
Table type                  : rtg-src-adj
Total Call-policy Failures : 0 (0 *)
Entry      Match Value      Destination Adjacency  Action
-----
1          SIPPIA           Registrar              Routing complete
2          SIPPIB           Registrar              Routing complete
    
```

```

Policy set 21
Default policy set         : No
First inbound NA table     :
First call routing table   : TAB1
First reg routing table    : TAB2
First outbound NA table    :
    
```

```

Table Name                  : TAB1
Class                       : Routing
Table type                  : rtg-src-adj
Total Call-policy Failures : 0 (0 *)
Entry      Match Value      Destination Adjacency  Action
-----
1          SIPPIA           SIPPIB                 Routing complete
2          SIPPIB           SIPPIA                 Routing complete
    
```

```

Table Name           : TAB2
Class                : Routing
Table type           : rtg-src-adj
Total Call-policy Failures : 0 (0 *)
Entry      Match Value      Destination Adjacency  Action
-----
1          SIP1A             Registrar             Routing complete
2          SIP1B             Registrar             Routing complete

```

## Policy set 25

```

Default policy set      : No
First inbound NA table  : ADMINTable
First call routing table :
First reg routing table :
First outbound NA table : OutTable

```

## Policy set 27

```

Default policy set      : No
First inbound NA table  :
First call routing table :
First reg routing table :
First outbound NA table :

```

## Policy set 35

```

Default policy set      : No
First inbound NA table  :
First call routing table :
First reg routing table :
First outbound NA table :

```

\* Numbers in brackets refer to a call being rejected by a routing or number analysis table because there were no matching entries in the table. This is also included in the total figure.

---

**Related Commands**

Command	Description
<b>call-policy-set</b>	Creates a new policy set on the Session Border Controller (SBC).
<b>call-policy set default</b>	Configures a default policy set on the signaling border element (SBE) entity.
<b>first-inbound-na-table</b>	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
<b>first-outbound-na-table</b>	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
<b>rtg-dst-address-table</b>	Configures the name of the first policy table to be processed when performing the number analysis stage of a policy.

# show sbc sbe call-policy-sets

To list all of the routing policy sets on the SBE, use the **show sbc sbe call-policy-sets** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe call-policy-sets**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to list the routing policy sets on the SBE with a configuration that has one call-policy-set:

```
Router# show sbc test sbe call-policy-sets
```

```
SBC Service ''test''
Policy Set Description
```

```
-----
1
Active policy set = 1
```

The following example shows how to list all of the routing policy sets on the SBE with multiple call-policy-sets with descriptions:

```
Router# show sbc a sbe call-policy-sets
```

```
SBC Service "a"
Policy Set      Description
```

```
-----
1          Call policy set for navtel
2          Call policy set for number analysis
3          Call policy set for h323
Active policy set = 1
Router#
```

# show sbc sbe call-policy-set default

To display the summary of the default policy set, use the **show sbc sbe call-policy-set default** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe call-policy-set default**

Syntax Description		
<i>sbc-name</i>	The name of the SBC service.	
<b>adjacency</b>	Displays the list of administrative domains on the adjacency.	

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	This command was modified. The <b>active</b> keyword was replaced with the <b>default</b> keyword.

**Examples** The following example shows how to display a summary of the default call policy set:

```
Router# show sbc mySBC sbe call-policy-set default
SBC Service "mySBC"

Policy set 1
  Default policy set      : Yes (priority 6)
  First inbound NA table :
  First call routing table : TAB1
  First reg routing table : TAB2
  First outbound NA table :

  Table Name              : TAB1
  Class                   : Routing
  Table type              : rtg-src-adj
  Total Call-policy Failures : 0 (0 *)
  Entry   Match Value      Destination Adjacency  Action
  ----   -
  1       SIPP1A           SIPP1B                Routing complete
  2       SIPP1B           SIPP1A                Routing complete

  Table Name              : TAB2
  Class                   : Routing
  Table type              : rtg-src-adj
  Total Call-policy Failures : 0 (0 *)
  Entry   Match Value      Destination Adjacency  Action
  ----   -
  1       SIPP1A           Registrar              Routing complete
  2       SIPP1B           Registrar              Routing complete
```

\* Numbers in brackets refer to a call being rejected by a routing or number analysis table because there were no matching entries in the table. This is also included in the total figure.

Related Commands	Command	Description
	<b>call-policy-set</b>	Creates a new policy set on the Session Border Controller (SBC).
	<b>call-policy set default</b>	Configures a default policy set on the signaling border element (SBE) entity.
	<b>first-inbound-na-table</b>	Configures the name of the first inbound policy table to be processed when performing the number analysis stage of a policy.
	<b>first-outbound-na-table</b>	Configures the name of the first outbound policy table to be processed when performing the number analysis stage of a policy.
	<b>show sbc sbe call-policy-set</b>	Lists the details of the policy sets configured on the SBC.

# show sbc sbe call-policy-set (enum)

To display configuration and status information about call policy sets, use the **show sbc sbe call-policy-set** command in privileged EXEC mode.

```
show sbc sbc-name sbe call-policy-set [active] [detail] [rps-id]
```

Syntax Description	active	(Optional) Displays configuration information for active call policy sets.
	<b>detail</b>	(Optional) Displays detailed configuration and status information for call policy sets.
	<i>rps-id</i>	(Optional) Displays information for the specified routing policy set ID number. The range is 1 to 2147483647.

**Command Default** If no parameters are given, information for all policies is displayed.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to display information about call policy sets:

## Example 1: Active

```
Router# show sbc test sbe call-policy-set default
```

```
SBC Service "test"
```

```
Policy set 1
```

```
Active policy set           : Yes
First Number Analysis table :
First call routing table    : rt1
First reg routing table     :
```

```
Table Name                  : rt1
Class                       : Routing
Table type                   : rtg-src-adj
Total Call-policy Failures  : 0 (0 *)
```

Entry	Match Value	Destination Adjacency	Action
1	sip1		Next dal
2	sip2		Routing complete

**Example 2: Active with Detail**

A number in parentheses indicates the number of calls being rejected by a routing table or by a number analysis table because no matching entries were found in the table. These rejected calls are included in the total number as well.

Router# **show sbc test sbe call-policy-set default detail**

```
SBC Service "test"

Policy set 1
  Description                :
  Active policy set          : Yes
  First Number Analysis table :
  First call routing table   : rtl
  First reg routing table    :

Table Name                   : rtl
  Description                 :
  Class                       : Routing
  Table type                  : rtg-src-adj
  Total Call-policy Failures : 0 (0)
  Entry : 1
    Match adjacency          sip1
    Action                   Next-table da1
    ENUM ID                  1
    ENUM entry               default-enum
    Failures                 0
  Entry : 2
    Match adjacency          sip2
    Action                   Routing complete
    ENUM ID                  1
    ENUM entry               cisco-enum
    Failures                 0
```

**Related Commands**

Command	Description
<b>activate</b>	Activates ENUM client.
<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.



<b>Command</b>	<b>Description</b>
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

# show sbc sbe call-policy-set tables

To list a summary of the call policy tables associated with the given policy set, use the **show sbc sbe call-policy-set tables** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe call-policy-set *policy-set tables***

Syntax Description	
<i>sbc name</i>	This is the name of the SBC service.
<b>policy-set</b>	The numeric identifier of the call policy set whose tables are to be displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to display a summary of the routing policy tables associated with the given policy set:

```
Router# show sbc a sbe call-policy-set 2 tables

SBC Service "a"
Policy set 2 tables
Table name      Match type      Description      Total Failures
-----
start-table     rtg-src-adj           0 (0 *)
na-table        na-dst-num           0 (0 *)
* Numbers in brackets refer to a call being rejected by a
routing or number analysis table because there were no
matching entries in the table. This is also included in
the total figure.
```

# show sbc sbe call-policy-set table entries

To display a summary of the entries associated with a given table, use the **show sbc sbe call-policy-set table entries** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe call-policy-set *id* table *name* entries**

Syntax Description	<i>id</i>	Specifies the numeric identifier of the routing policy set to which the table belongs.
	<i>sbc name</i>	This is the name of the SBC service.
	<i>name</i>	Specifies the table whose entries are to be displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to display a summary of the entries associated with the given table:

```
Router# show sbc a sbe call-policy-set 1 table start-table entries

SBC Service 'a'
Policy set 1 table start-table entries
Table class Entry Match Value
-----
Routing entry 1 navtel2
Routing entry 2 navtell
Router#
```

# show sbc sbe call-policy-set table entry

To display detailed information for a given entry in a CAC policy table, use the **show sbc sbe call-policy-set table entry** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe call-policy-set *id* table *name* entry**

Syntax Description		
<i>id</i>	Specifies the numeric identifier of the routing policy set to which the table belongs.	
<i>name</i>	Specifies the table whose entries are to be displayed.	
<i>sbc name</i>	This is the name of the SBC service.	
<b>entry</b>	Specifies the entry index of the table.	

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to display a summary of the entries associated with the given table:

```
Router# show sbc mySbc sbe call-policy-set 1 table rtgTable entry 1
SBC Service 'mySbc'
Policy set 1 table rtgTable entry 1
Routing table entry
Match adjacency sipOrig
Action Routing complete
Dest Adjacency h323Term
Failures 0
```

## show sbc sbe call-rate-stats

To list all of the current rate of attempted call setups per second over a short period of time (default to 3 seconds), use the **show sbc sbe call-rate-stats** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe call-rate-stats**

<b>Syntax Description</b>	<i>sbc name</i> This is the name of the SBC service.				
<b>Command Default</b>	Default value is 3 seconds.				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

**Examples** The following example shows how to list all of the current rate of attempted call setups per second:

```
Router# show sbc sbc-1 sbe call-rate-stats
Calls Per Second:
-----
Current CPS 10
Maximum CPS 80
Minimum CPS 1
Average CPS 0
```

## show sbc sbe call-stats

To display the statistics pertaining to all the calls on the SBE, use the **show sbc sbe call-stats** command in the privileged EXEC mode.

```
show sbc sbc-name sbe call-stats {all | global | per-adjacency adjacency-name | src-account name
| dst-account name | src-adjacency name | dst-adjacency name} period
```

```
show sbc sbc-name sbe call-stats {reject-threshold}
```

```
show sbc sbc-name sbe call-stats failures {detail | summary} period
```

```
show sbc sbc-name sbe call-stats {global | adjacency adjacency-name} emergence
```

Syntax	Description
<i>sbc-name</i>	Name of the SBC service.
name	Name of the account for which you want the statistics to be displayed. The maximum length of this value is 30 characters.
<i>period</i>	Interval at which the statistics are displayed. The possible values are: <ul style="list-style-type: none"> <li><i>current5mins</i>—Shows the statistics pertaining to the current 5-minute interval.</li> <li><i>previous5mins</i>—Shows the statistics pertaining to the previous 5-minute interval.</li> <li><i>current15mins</i>—Shows the statistics pertaining to the current 5-minute interval and the previous two 5-minute intervals.</li> <li><i>previous15mins</i>—Shows the statistics pertaining to the previous 5-minute interval and the previous two 5-minute intervals.</li> <li><i>currenthour</i>—Shows the statistics pertaining to the current 5-minute interval and the previous eleven 5-minute intervals.</li> <li><i>previoushour</i>—Shows the statistics pertaining to the previous 5-minute interval and the previous eleven 5-minute intervals.</li> <li><i>currentday</i>—Shows the statistics pertaining to the current 5-minute interval and the previous two hundred eighty seven 5-minute intervals.</li> <li><i>previousday</i>—Shows the statistics pertaining to the previous 5-minute interval and the previous two hundred eighty seven 5-minute intervals.</li> <li><i>currentindefinite</i>—Shows the statistics pertaining to the period since the last explicit reset.</li> </ul>
<b>global</b>	Displays the emergency call statistics globally for the entire SBC.
<b>adjacency</b>	Displays the emergency calls statistics for calls received and sent for the specified adjacency name.
<i>adjacency-name</i>	Name of the adjacency for which emergency calls belonging to that adjacency should be displayed.
<b>emergence</b>	<i>Displays the emergency call statistics for the entire SBC or for a specific adjacency name.</i>
failures	Displays the incremental failure counters of failed calls.

<b>detail</b>	Displays the detailed output of all the statistics containing incremental failure counters for the specified period.
<b>summary</b>	Displays the summary of all the statistics containing incremental failure counters for the specified period.
<b>per-adjacency</b>	Displays the QoS-related statistics for a single adjacency.
<b>dst-adjacency</b>	Displays the statistics for the destination adjacency.
<b>src-adjacency</b>	Displays the statistics for the source adjacency.
<b>reject-threshold</b>	Displays the rejection threshold statistics.
<b>src-account</b>	Displays the statistics for the source account.
<b>dst-account</b>	Displays the statistics for the destination account.

**Command Default**

No default behavior or values are available.

**Command Modes**

Privileged EXEC (#)

**Command History**

<b>Release</b>	<b>Modification</b>
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers, and failure statistics were added to the output.
Cisco IOS XE Release 2.5	This command was modified. New parameters were added to the command to list the statistics for all the policy failures.
Cisco IOS XE Release 2.6	The output of this command was modified to include the number of active IPv6 calls.
Cisco IOS XE Release 3.1S	The output of this command was modified to show Internet Mail Service (IMS) Rx statistics and Secure Real-Time Transport Protocol (SRTP) statistics. <b>The reject-threshold and failures keywords were added.</b>
Cisco IOS XE Release 3.2S	The command was modified. The <b>adjacency</b> keyword and the <i>adjacency-name</i> parameter were added to the <b>show sbc sbe call-stats</b> command. The <b>emergence</b> keyword was added to display the emergency call statistics globally or for a specified adjacency name. The output of the command was updated to list the count of the active transcoded and transrated calls.
Cisco IOS XE Release 3.3S	This command was modified. The <b>per-adjacency</b> keyword and the <i>currentindefinite</i> parameter were added to the command.
Cisco IOS XE Release 3.4S	The output of this command was modified to include the values of the QoS statistics and the current alert levels of the statistics.

**Usage Guidelines**

The statistics are collected at 5-minute intervals past the hour (that is, 0, 5, 10, 15, and so on). The system keeps a bucket that collects each of the over 5-minutes counts. Each bucket is started at 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, and 55-minutes past the hour according to the system clock. The **show sbc sbe call-stats** command then combines a number of these buckets and displays the sum of these buckets.

For example, if the current time is 12:34, *currenthour* will apply to the statistics collected since 11:35, and *current15mins* will apply to the statistics collected since 12:20. In this example, *previoushour* is 10:35 to 11:35, and *previous15mins* is 12:05 to 12:20.

**Note**

Call statistics for rejection of calls based on the memory threshold is not tracked based on time intervals.

**Cisco IOS XE Release 3.2S**

To display the emergency call statistics for calls belonging to a particular category and assigned a priority number globally, execute the **show sbc *sbc-name* sbe call-stats global emergence** command from the privileged EXEC mode. The command output displays the global call statistics for the entire SBC.

To display the emergency call statistics for calls belonging to a particular adjacency, run the **show sbc *sbc-name* sbe call-stats adjacency *adjacency-name* emergence** command. The command output displays the call statistics for calls that are both received and sent on the specified adjacency.

**Examples**

The following example shows how to list the complete call statistics for the current day:

```
Router# show sbc global sbe call-stats all currentday
```

```
statistics for the current day for global counters
```

```
Call count totals:
```

```
Total call attempts = 0
Total active calls = 0
Total active IPv6 calls = 0
Total activating calls = 0
Total de-activating calls = 0
Total active emergency calls = 0
Total active e2 emergency calls = 0
Total IMS rx active calls = 0
Total IMS rx call renegotiation attempts = 0
Total SRTP-RTP interworked calls = 0
Total active calls not using SRTP = 0
Total active transcoded calls = 0
Total active transrated calls = 0
Total calls completed = 0
```

```
General call failure counters:
```

```
Total call setup failures = 0
Total active call failures = 0
Total failed call attempts = 0
Total failed calls due to update failure = 0
Total failed calls due to resource failure = 0
Total failed calls due to congestion = 0
Total failed calls due to media failure = 0
Total failed calls due to signaling failure = 0
Total failed calls due to IMS rx setup failure = 0
Total failed calls due to IMS rx renegotiation failure = 0
Total failed calls due to RTP disallowed on call leg = 0
Total failed calls due to SRTP disallowed on call leg = 0
```

```
Policy control failures:
```

```
Call setups failed due to NA = 0
Call setups failed due to RTG = 0
Call setups failed due to CAC = 0
CAC fails due to number of calls limit = 0
CAC fails due to call rate limit = 0
CAC fails due to bandwidth limit = 0
```



```

CAC fails due to number of media channels limit =          0
CAC fails due to number of media update limit =          0
CAC message drops due to mid call message rate limit =    0
CAC message drops due to out of call message rate limit = 0

```

Stats Reset Timestamp:

```
Timestamp when stats for this summary period were reset = 2010/10/21 20:30:21
```

Table 16 provides the descriptions for the important fields in the displayed example.

**Table 16** *show sbc sbe call-stats Field Descriptions*

Field	Description
Active calls	If the period being queried is “current5mins”, this is the number of calls (IPv4 and IPv6) currently active at the instant that the query is issued. Otherwise, this is the average number of calls that have been active for the entire period. A call must have been active for at least half of the period in order to count as having been active on an average for the entire period. Therefore, this statistic is effectively a count of the number of calls that have been active for half the period or more.
Active Ipv6 calls	If the period being queried is “current5mins”, this is the number of IPv6 calls active at the instant the query is issued. Otherwise, this is the average number of calls that have been active for the entire period. A call must have been active for at least half of the period in order to count as having been active on an average for the entire period. Therefore, this statistic is effectively a count of the number of calls that have been active for half the period or more.
Activating calls	If the period being queried is “current5mins”, this is the number of calls currently activating at the instant that the query is issued. Otherwise, this is the average number of calls that have been activating for the entire period. A call must have been activating for at least half of the period in order to count as having been activating on average for the entire period. Therefore this statistic is effectively a count of the number of calls that have been activating for half the period or more.
Deactivating calls	If the period being queried is “current5mins,” this is the number of calls that are undergoing deactivation at the instant that the query is issued. Otherwise, this is the average number of calls that have been undergoing deactivation for the entire period. A call must have been undergoing deactivation for at least half of the period in order to count as having been undergoing deactivation on average for the entire period. Therefore, this statistic is effectively a count of the number of calls that have been undergoing deactivation for half the period or more.

**Table 16** *show sbc sbe call-stats Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Total call attempts	Call establishment attempts made. A call attempt may have failed in a later summary period. This counter may include failed calls which are not included in the failed call attempt count.
Failed call attempts	Indicates the calls that have failed to establish a successful call. A failed call attempt may result from a call that was started during a previous summary period. This counter may include call attempts that are not included in the total call attempt count.
Successful call attempts	Total call attempts minus failed call attempts.
Call routing failed	Call establishment attempts failed due to a routing failure.
Call resources failed	Call establishment attempts failed due to a resource failure.
Call media failed	Call establishment attempts failed due to a media failure.
Call signaling failed	Call establishment attempts failed due to a signaling failure.
Active call failures	Calls failed from an active state. This count includes all deactivation causes other than normal release.
Congestion failures	Call establishment attempts failed due to system congestion.
Total call setup failures	Total number of call setup failures due to Number Analysis, Routing, and Multiple CAC policies.
Total call update failures	Total number of call update failures due to Multiple CAC policies.
Call setup failed due to NA	Total number of call setup failures due to Number Analysis policies.
Call setup failed due to rtg	Total number of call setup failures due to routing policies.
Call setup failed due to CAC	Total number of call setup failures due to Multiple CAC policies.
CAC fails due to num call lim	Total number of call setup failures due to CAC call limit.
CAC fails due to call rate lim	Total number of call setup failures due to CAC call rate limit.
CAC fails due to num media channels lim	Total number of call setup failures due to CAC number of media channels limit.
CAC fails due to num media updates lim	Total number of call setup failures due to CAC number of media updates limit.
CAC fails due to bandwidth lim	Total number of call setup failures due to CAC Bandwidth limit.
CAC fails due to in-call rate lim	Total number of failures due to the CAC limit on the rate of in-call messages.
CAC fails due to out-call rate lim	Total number of failures due to the CAC limit on the rate of out-of-call requests.

The following is an example of the **show** command output for reject threshold:

```
Router# show sbc mySBC sbe call-stats reject-threshold
```

```

Level      Memory Trigger  Action
-----
minor     < 25 percent    0 in 10 calls dropped
major     < 20 percent    4 in 10 calls dropped
critical  < 15 percent    9 in 10 calls dropped
halt      < 10 percent    10 in 10 calls dropped

Current level: NORMAL
Total calls rejected due to low memory threshold: 0

```

The following example shows the emergency call statistics globally for the entire SBC:

```

Router# show sbc mySBC sbe call-stats global emergence
SBC Service "md"
Emergence call statistics for global counters
Call count totals:
  Category ABCEMERGENCY active calls = 1
  Category ABCEMERGENCY unaudit calls = 0
  Category ABCHIGHPRIORITY active calls = 2
  Category ABCHIGHPRIORITY unaudit calls = 0
  Priority unspecified active calls = 3
  Priority unspecified unaudit calls = 0

```

The following example shows the emergency call statistics for calls belonging to a specified adjacency. The following **show** command output displays the per-adjacency count for calls received and sent on a specified adjacency name:

```

Router# show sbc mySBC sbe call-stats adjacency govt-adj emergence
Statistics for the current hour for source adjacency govt-adj
Call count totals:
  Total active calls =                200
  Category govtcalls incoming calls =    90
  Category govtcalls outgoing calls =    90
  Category sipheader incoming calls =    80
  Category sipheader outgoing calls =    80
  Priority routing incoming calls =      80
  Priority routing outgoing calls =      80
  Unaudited calles =                  100

```

The following example shows an output of the **show sbc sbe call-stats global current5min** command that lists the count of the active transcoded and transrated calls.

```

Router# show sbc mySBC sbe call-stats global current5min
SBC Service "mySBC"
Statistics for the current 5 mins for global counters
Call count totals:
  Total call attempts =                0
  Total active calls =                  1
  Total active IPv6 calls =             0
  Total activating calls =              0
  Total de-activating calls =           0
  Total active emergency calls =         0
  Total active e2 emergency calls =     0
  Total IMS rx active calls =           0
  Total IMS rx call renegotiation attempts = 0
  Total SRTP-RTP interworked calls =    0
  Total active calls not using SRTP =    1
  Total active transcoded calls =        1
  Total active transrated calls =        0
General call failure counters:
  Total call setup failures =           0
  Total active call failures =          0
  Total failed call attempts =          0
  Total failed calls due to update failure = 0

```

```
Total failed calls due to resource failure = 0
Total failed calls due to congestion = 0
Total failed calls due to media failure = 0
Total failed calls due to signaling failure = 0
Total failed calls due to IMS rx setup failure = 0
Total failed calls due to IMS rx renegotiation failure = 0
Total failed calls due to RTP disallowed on call leg = 0
Total failed calls due to SRTP disallowed on call leg = 0
```

The following example shows how, in Release 3.4S and later, the output of the **show sbc sbe call-stats per-adjacency currentindefinite** command was modified to include the values of the QoS statistics and the current alert levels of the statistics:

```
Router# show sbc Mysbc sbe call-stats per-adjacency adj1 currentindefinite
...
Statistics for the current hour for adjacency adj1

Stats Reset Timestamp:
Timestamp when stats for this summary period were reset = 2011/04/08 04:05:09
Current count of Media Packets Lost = 0
Current count of Media Packets Dropped = 1
Current count of Media Packets Sent = 116
Current count of Media Packets Received = 116
Current count of RTCP Packets Sent = 0
Current count of RTCP Packets Received = 0
Average Call Duration = 21 secs 16 ms
Average of the Unanswered Call Ratio per thousand call = 0
Average of the Round Trip Delay = 0 ms
Average of the locally calculated jitter = 77 ms
Average of the remotely calculated jitter = 0 ms
Average of the received media dropped per thousand pkts = 8
Average of the sent media lost per thousand pkts = 0
Average of Mean Opinion Score = 20
Current alert level of the Unanswer Seizure Ratio = NONE
Current alert level of the Round Trip Delay = NORMAL
Current alert level of the locally calculated Jitter = MINOR
Current alert level of the remotely calculated Jitter = NORMAL
Current alert level of the media packet dropped = MAJOR
Current alert level of the sent packets lost = NORMAL
Current alert level of the Media Opinion Score = MINOR
```

**Related Commands**

Command	Description
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
<b>reject-threshold</b>	Configures the memory threshold and reject rate for new calls.
<b>show sbc sbe call-rate-stats</b>	Lists all the calls on the SBE.

# show sbc sbe calls

To list all the calls on the signaling border element (SBEs), use the **show sbc sbe calls** command in privileged EXEC mode.

```
show sbc sbc-name sbe calls [ipv6 | media-detail | srtp | srtp-iw]
```

Syntax Description	
<i>sbc name</i>	Name of the Session Border Controller (SBC) service.
<b>ipv6</b>	Displays the details of the IPv6 calls on the SBE.
<b>media-detail</b>	Displays details of the calls, including their media information.
<b>srtp</b>	Displays details of the calls with Secure Real-Time Transport Protocol (SRTP) media on the SBE.
<b>srtp-iw</b>	Displays details of the calls performing SRTP-to-Real-Time Transport Protocol interworking.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	This command's output was modified to provide details of IPv6 calls.
	Cisco IOS XE Release 3.1S	The <b>media-detail</b> , <b>srtp-iw</b> , and <b>srtp</b> optional keywords were added.

**Examples** The following examples show how to display the call statistics for the current hour:

### Example 1: Default

```
Router# show sbc a sbe calls
```

```
SBC Service 'a'
Call State Type Src Adjacency Dest Adjacency
-----
393 Activating Audio navtel1 navtel2
394 Activating Audio navtel1 navtel2
```

### Example 2: IPv6 Details

```
Router# show sbc test sbe calls ipv6
```

```
SBC Service "test"
Call          State          Src Adjacency      Dest Adjacency
-----
923752        Active         CCM135             CCM136-IpV6
```

**Example 3: Media Detail**

```
Router# show sbc b2b1 sbe calls media-detail
SBC Service "b2b1"
Call          State          Src Adjacency      Dest Adjacency
-----
1             Active          7200-1             7200-2
Context ID 1Stream ID 49153
Side A:      Media Flowing: Yes
Local Address/Port: 10.2.0.10/16384
Remote Address/Port: 2.0.0.3/6000
Side B:      Media Flowing: Yes
Local Address/Port: 10.2.0.10/16386
Remote Address/Port: 3.0.0.3/7000
```

**Example 4: SRTP**

```
Router# show sbc b2b1 sbe calls srtp
SBC Service "SBC1"
Call          State          Src Adjacency      Dest Adjacency
-----
5             Active          UAS                 UAC
```

**Example 5: SRTP-to-RTP Interworking**

```
Router# show sbc global sbe calls srtp-iv
SBC Service "global"
Call          State          Src Adjacency      Dest Adjacency
-----
1             Active          Customer            CORE
```

**Related Commands**

Command	Description
<b>srtp caller</b>	Configures SRTP for a caller in a CAC policy.
<b>srtp callee</b>	Configures SRTP for a callee in a CAC policy.
<b>srtp media interworking</b>	Configures SRTP-to-RTP media interworking in a CAC policy.
<b>srtp interworking</b>	Configures SRTP-to-RTP interworking in a CAC policy.
<b>srtp retry rtp</b>	Configures the SBC to retry and enable SRTP-to-RTP interworking after it has rejected an SRTP offer.
<b>srtp response downgrade</b>	Configures a SIP endpoint to support a nonstandard offer/answer SRTP downgrade.

# show sbc sbe call branches

To show all the branches on the specified call on SBEs, use the **show sbc sbe call branches** command in Privileged EXEC mode.

**show sbc sbe call *call-num* branches**

<b>Syntax Description</b>	<i>call-num</i> Specifies the call to display information about.				
<b>Command Default</b>	No default behavior or values are available.				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

## Examples

The following example shows how to display the branches associated with call 2:

```
Router# show sbc mySbc sbe call 2 branches
```

```
SBC Service "mySbc"
Call: 2
State: active
Type: video
```

```
Branch Calling Number Called Number Billing ID
1      102 789 767      -          DAB3C4D153624C7124E1234
2      -                05 659 896
```

# show sbc sbe codec-list

To show information about the codec lists that are configured on the SBE, use the **show sbc sbe codec-list** command in Privileged EXEC mode.

```
show sbc sbc-name sbe codec-list list-name
```

Syntax Description		
	<i>sbc name</i>	This is the name of the SBC service.
	<i>list-name</i>	Specifies the name of the codec list.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to display information about the codec list named my\_codecs.

```
Router# show sbc mySbc sbe codec-list my_codecs

SBC Service "mySbc"

Codec list "my_codecs" (Legitimate codecs)
  Codec Name           Min Packetization Period
  =====
  PCMU                 20ms
  G729                 10ms
```



# show sbc sbe codecs

To view the codecs included in the Session Border Controller (SBC) and the codecs dynamically configured on the SBC, use the **show sbc sbe codecs** command in the Privileged EXEC configuration mode.

```
show sbc sbcname sbe codecs [[base | user | modified] | [name] codec-name | variant [profiles]]
```

Syntax Description	
<i>sbcname</i>	The name of the SBC.
<b>base</b>	Displays codecs that have not been modified.
<b>user</b>	Displays the codecs defined by a user.
<b>modified</b>	Displays the codecs that have been modified.
<b>name</b>	Displays information about a specific codec.
<i>codec-name</i>	The unique name of a codec.
<b>variant</b>	Displays information about codec variants.
<b>profiles</b>	Displays information about codec variant profiles.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.2S	The command was modified. The <b>variant</b> and <b>profiles</b> keywords were added to this command.

**Usage Guidelines** To use this command, you must be in the correct configuration mode.

**Examples** The following example shows how to display all the codecs on the *mySBC* SBC:

```
Router# show sbc mySBC sbe codecs
Codec Name: CN
Type           = Fixed Rate
Clock Rate     = 8000 Hz
Packet time    = 20 sec
Bandwidth      = 1
Sample Size    = 0
Number Channels = 0
Max Frames Per Pkt = 0
Media Type     = Audio
Options        = Transcode
Configured State = base
```

```
Codec Name: DV
-----
Type           = Variable Bitrate
Clock Rate     = 10000 Hz
Packet_Time    = 10
Bandwidth      = 1
Sample Size    = 0
Number Channels = 0
Max Frames Per Pkt = 0
Media Type     = Video
Options        = None
Configured State = modified
```

The following example shows how to display the details of a specific codec:

Router# **show sbc mySBC sbe codecs name gsm-efr**

```
Codec Name: GSM-EFR
-----
Type           = Fixed
Clock Rate     = 8000 Hz
Packet_Time    = 20
Bandwidth      = 1
Sample Size    = 0
Number Channels = 0
Max Frames Per Pkt = 65535
Media Type     = Audio
Options        = Transcode
Configured State = user defined
```

The following example shows how to display information about the codec variants:

Router# **show sbc mySBC sbe codecs variant**

```
Codec Variant Table:
**Note: base variants begin with '#'.

Variant Name       = #CCD
Variant Encoded name = CCD
Standard Codec Name = CLEARMODE
FMTP String        =
Referenced Pofiles =
-----
Variant Name       = #NSE
Variant Encoded name = NSE
Standard Codec Name = X-NSE
FMTP String        =
Referenced Pofiles =
-----
Variant Name       = #NTE
Variant Encoded name = NTE
Standard Codec Name = telephone-event
FMTP String        =
Referenced Pofiles =
-----
.
.
.
```

The following example shows how to display information about the codec variant profiles:

```
Router# show sbc MySBC sbe codecs variant profiles
```

```
Profile          Variant[s]
codec_profile1   g711a
                  #G.722
codec_profile2   #G.729
                  g711a
```

# show sbc sbe diameter

To display the configuration information for the Diameter protocol, use the **show sbc sbe diameter** command in privileged EXEC mode.

**show sbc *sbc-name* sbe diameter**

Syntax Description	sbc-name	Name of the SBC service.
--------------------	----------	--------------------------

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to display the configuration information for the Diameter protocol.

```
Router# show sbc MySBC sbe diameter
```

```
SBC Service "MySBC"
Diameter information:
  Origin Realm:          Realm1
  Origin Host:           Cisco.com
  Admin Status:         DOWN
  Operation Status:     DOWN
```

Related Commands	Command	Description
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.
	<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
	<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
	<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
	<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.

<b>Command</b>	<b>Description</b>
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# show sbc sbe diameter peers

To display the configuration information for IMS peers, use the **show sbc sbe diameter peers** command in privileged EXEC mode.

**show sbc *sbc-name* sbe diameter peers *peer-name***

## Syntax Description

<b>sbc-name</b>	Name of the SBC service.
<b>peer-name</b>	Name of the IMS peer.

## Command Default

If no peer name is given, brief information for all peers is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to display the configuration information for an IMS peer.

```
Router# show sbc MySBC sbe diameter peers Peer1
```

```
Diameter peer Peer1:
  State:          Closed
  DWR State:      Initial
  Origin:         Static
  VRF Name:       None
  Local Address:  0.0.0.0
  Local Port:     0
  Peer Address:   10.10.10.10
  Peer Port:      0
  Peer FQDN:
```

## Related Commands

Command	Description
<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
<b>origin-realm</b>	Configures the domain name of an IMS local realm.
<b>origin-host</b>	Configures the domain name of an IMS local host.

<b>Command</b>	<b>Description</b>
<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# show sbc sbe diameter stats

To display the transport statistics for an IMS peer, use the **show sbc sbe diameter stats** command in privileged EXEC mode.

**show sbc *sbc-name* sbe diameter stats**

<b>Syntax Description</b>	sbc-name	Name of the SBC service.
---------------------------	----------	--------------------------

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to display the transport statistics for an IMS peer.
-----------------	--

```
Router# show sbc MySBC sbe diameter stats

Diameter statistics:
  Diameter up time:                0 seconds
  Diameter packets sent:           0
  Diameter packets received:       0
  Diameter malformed packets received: 0
  Diameter unknown identifier answer messages received: 0
  Diameter protocol error answer messages received: 0
  Diameter unknown command code packets received: 0
  Diameter requests transient failures: 0
  Diameter requests permanent failures: 0
  Diameter requests unexpected transport failures: 0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>diameter</b>	Enables the Diameter protocol on a node and enter the Diameter configuration mode.
	<b>origin-realm</b>	Configures the domain name of an IMS local realm.
	<b>origin-host</b>	Configures the domain name of an IMS local host.



<b>Command</b>	<b>Description</b>
<b>peer</b>	Creates an IMS peer and configure the name and IPv4 address of the peer.
<b>realm (diameter)</b>	Configures a peer and assign the peer to a realm.
<b>show sbc sbe diameter</b>	Displays the configuration information for the Diameter protocol.
<b>show sbc sbe diameter peers</b>	Displays the configuration information for IMS peers.
<b>show sbc sbe diameter stats</b>	Displays the transport statistics for an IMS peer.
<b>ims rx</b>	Configures an IMS Rx interface for access adjacency
<b>ims pani</b>	Configures the P-Access-Network-Info (PANI) header process preference for an adjacency.
<b>ims realm</b>	Configures an IMS realm for use by an IMS Rx interface.
<b>ims rx preliminary-aar-forbid</b>	Prevents preliminary AAR messages from being sent in an IMS Rx session.
<b>ims media-service</b>	Configures a CAC table to allow the use of media resources and 3rd party transcoding resources as well as Rx resources.

# show sbc sbe editors

To display a list of all the editors registered on the SBC, use the **show sbc sbe editors** command in the privileged EXEC mode.

**show sbc *sbc-name* sbe editors**

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
-----------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

There are no specific usage guidelines for using the **show sbc sbe editors** command. Note that the **clear sbc sbe script-set-stats** command can be used to clear the stored statistics from which the **show sbc sbe editors** command draws data.

## Examples

In the following example, the **show sbc sbe editors** command is used to display a list of all the editors registered on the SBC:

```
Router# show sbc mySbc sbe editors
```

Editor	Script-set	Type	Total executions
my_body_editor	n/a	profile	0
preset-call-tag	n/a	profile	0
my_header_editor	n/a	profile	0
my_method_editor	n/a	profile	0
my_option_editor	n/a	profile	0
preset-acc-in-hdr	n/a	profile	0
preset-acc-in-mth	n/a	profile	0
preset-acc-in-opt	n/a	profile	0
preset-std-in-hdr	n/a	profile	0
preset-std-in-mth	n/a	profile	0
preset-std-in-opt	n/a	profile	0
preset-acc-out-hdr	n/a	profile	0
preset-acc-out-mth	n/a	profile	0
preset-acc-out-opt	n/a	profile	0

preset-core-in-hdr	n/a	profile	0
preset-core-in-mth	n/a	profile	0
preset-core-in-opt	n/a	profile	0
preset-std-out-hdr	n/a	profile	0
preset-std-out-mth	n/a	profile	0
preset-std-out-opt	n/a	profile	0
default-body-editor	n/a	profile	0
preset-core-out-hdr	n/a	profile	0
preset-core-out-mth	n/a	profile	0
preset-core-out-opt	n/a	profile	0
preset-ipsec-in-hdr	n/a	profile	0
preset-ipsec-in-mth	n/a	profile	0
preset-ipsec-in-opt	n/a	profile	0
preset-ipsec-out-hdr	n/a	profile	0
preset-ipsec-out-mth	n/a	profile	0
preset-ipsec-out-opt	n/a	profile	0
default-header-editor	n/a	profile	36
default-method-editor	n/a	profile	36
default-option-editor	n/a	profile	36
preset-ibcf-ext-in-hdr	n/a	profile	0
preset-ibcf-ext-in-mth	n/a	profile	0
preset-ibcf-ext-in-opt	n/a	profile	0
preset-ibcf-int-in-hdr	n/a	profile	0
preset-ibcf-int-in-mth	n/a	profile	0
preset-ibcf-int-in-opt	n/a	profile	0
preset-ibcf-utr-in-hdr	n/a	profile	0
preset-ibcf-utr-in-mth	n/a	profile	0
preset-ibcf-utr-in-opt	n/a	profile	0
preset-ibcf-ext-out-hdr	n/a	profile	0
preset-ibcf-ext-out-mth	n/a	profile	0
preset-ibcf-ext-out-opt	n/a	profile	0
preset-ibcf-int-out-hdr	n/a	profile	0
preset-ibcf-int-out-mth	n/a	profile	0
preset-ibcf-int-out-opt	n/a	profile	0
preset-ibcf-utr-out-hdr	n/a	profile	0
preset-ibcf-utr-out-mth	n/a	profile	0
preset-ibcf-utr-out-opt	n/a	profile	0
preset-std-block-in-hdr	n/a	profile	0
preset-std-block-in-mth	n/a	profile	0
preset-std-block-in-opt	n/a	profile	0
preset-std-block-out-hdr	n/a	profile	0
preset-std-block-out-mth	n/a	profile	0
preset-std-block-out-opt	n/a	profile	0
lcl_addr	2	script	0
monitor_packetization	3	script	0

Table 17 describes the significant fields in the output of the **show sbc sbe editors** command.

**Table 17** *show sbc sbe editors Field Descriptions*

Field	Description
Editor	Name of the editor.
Script-set	Number of the script set in which the editor has been configured.

**Table 17** *show sbc sbe editors Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Type	Type of editor. The type can be profile or script.
Total executions	Number of times the editor has been applied. The counter for tracking the number of times the editor has been applied is incremented even when a message that does not meet the criteria for applying the editor is processed.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>active-script-set</b>	Activates a script set,
<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
<b>editor</b>	Specifies the order in which a particular editor must be applied.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# show sbc sbe enum

To display the configuration information about an ENUM client, use the **show sbc sbe enum** command in privileged EXEC mode.

```
show sbc sbc-name sbe enum enum-id
```

## Syntax Description

<i>sbc-name</i>	Name of the SBC service.
<i>enum-id</i>	ENUM client ID number. Currently, only the number 1 is allowed.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to display the configuration information about all currently configured ENUM Supplementary Routing Services (SRS):

```
Router# show sbc MySBC sbe enum 1

SBC Service enum
 Enum 1
  Supplementary routing service id      : 1
  Max recursive depth                   : 6
  Max responses                          : 6
  Request timeout                       : 60
  Status                                : Up
 entry enum
   Enum Server IPV4 Address             : 20.21.28.125
   Enum Server VPN ID                   : 5
   Dial plan suffix string              : enum.com
 entry default
   Enum Server IPV4 Address             : 20.21.28.125
   Enum Server VPN ID                   : 0
   Dial plan suffix string              : e164.arpa
```

Related Commands	Command	Description
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
	<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
	<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
	<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
	<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
	<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
	<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
	<b>req-timeout</b>	Configures the ENUM request timeout period.
	<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
	<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
	<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
	<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
	<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

# show sbc sbe enum entry

To display the contents of an ENUM client entry, use the **show sbc sbe enum entry** command in privileged EXEC mode.

```
show sbc sbc-name sbe enum enum-id entry entry-name
```

## Syntax Description

<i>sbc-name</i>	Name of the SBC service.
<i>enum-id</i>	ENUM client ID number. Currently, only the number 1 is allowed.
<i>entry-name</i>	ENUM client entry name.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure display the contents of an ENUM client entry:

```
Router# show sbc MySBC sbe enum 1 entry MyEntry
SBC Service MySBC
  entry MyEntry
    Enum Server IPV4 Address      : 10.10.10.10
    Enum Server VPN ID           : 0
    Dial plan suffix string      : e164.arpa
```

## Related Commands

Command	Description
<b>activate</b>	Activates ENUM client.
<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.

<b>Command</b>	<b>Description</b>
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe</b> <b>call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum</b> <b>entry</b>	Displays the contents of an ENUM client entry.



# show sbc sbe h323 timers

To display a list of H.323 timer configuration, use the **show sbc sbe h323** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe h323 timers**

<b>Syntax Description</b>	<i>sbc name</i> This is the name of the SBC service.				
<b>Command Default</b>	No default behavior or values are available.				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

**Examples** The following example shows how the **show sbc sbe h323 timers** command is used to display a list of H.323 timer configuration:

```
Router# show sbc test sbe h323 timers
```

```
SBC Service 'test'
H.323 Timers
Global scope
adjacency retry timeout 30000
h225 timeout setup 4000
h225 timeout proceeding 10000
h225 timeout establishment 180000
ras rrq ttl 60
ras rrq keepalive 45000
ras retry count (arq) 2
ras timeout (arq) 5000
ras retry count (brq) 2
ras timeout (brq) 3000
ras retry count (drq) 2
ras timeout (drq) 3000
ras retry count (grq) 2
ras timeout (grq) 5000
ras retry count (rrq) 2
ras timeout (rrq) 3000
ras retry count (urq) 1
ras timeout (urq) 3000
```

```
Adjacency tekOrig
H225 Timeout Setup 4000
H225 Timeout Proceeding 10000
H225 Timeout Establishment 180000
RAS RRQ TTL 60
RAS RRQ Keepalive 45000
```

```
RAS Retry Count (arq) 2
RAS Timeout (arq) 5000
RAS Retry Count (brq) 2
RAS Timeout (brq) 3000
RAS Retry Count (drq) 2
RAS Timeout (drq) 3000
RAS Retry Count (grq) 2
RAS Timeout (grq) 5000
RAS Retry Count (rrq) 2
RAS Timeout (rrq) 3000
RAS Retry Count (urq) 1
RAS Timeout (urq) 3000
```

# show sbc sbe hold-media-timeout

To show the configured duration of the media timeout timer for on-hold calls, use the **show sbc sbe hold-media-timeout** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe hold-media-timeout**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the SBC service.
<b>Command Default</b>	No default behavior or values are available.	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows sample data for the media timeout timer for on-hold calls:

```
Router# show sbc mysbc sbe hold-media-timeout

SBC Service "mysbc"

SBE On-hold media timeout duration is: 10 seconds
Router#
```

# show sbc sbe hunting-trigger

To show the H.323 or SIP hunting triggers at the global level, use the **show sbc sbe hunting-trigger** command in Privileged EXEC mode.

```
show sbc sbc-name sbe {h323 | sip} hunting-trigger
```

Syntax Description	Parameter	Description
	<i>sbc-name</i>	Specifies the SBC service.
	<b>h323</b>	Specifies H.323 hunting-trigger.
	<b>sip</b>	Specifies SIP hunting-trigger.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows sample data for the media timeout timer for on-hold calls:

```
Router# show sbc uut105-1 sbe h323 hunting-trigger
```

```
H.323 Hunting Triggers
-----
noBandwidth
unreachableDestination
destinationrejection
noPermission
badFormatAddress
securityDenied
```

Related Commands	Command	Description
	<b>hunting-trigger</b>	Configures failure return codes to trigger hunting.

# show sbc sbe media-gateway-associations

To list all the media gateways associated with this SBE and statistics associated with the media gateway, use the **show sbc sbe media-gateway-associations** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe media-gateway-associations**

## Syntax Description

<i>sbc-name</i>	Specifies the SBC service.
-----------------	----------------------------

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to list all the media gateways associated with this SBE and statistics associated with the media gateway:

```
Router# show sbc test sbe media-gateway-associations
```

```
SBC Service 'test'
Media gateway 200.200.207.101:2944
Gateway Protocol = megaco
Transport Protocol = UDP
Local Address = 88.104.1.3:2944
```

```
Sent Received Failed Retried
Requests 3687 1 0 0
Replies 1 3686 - 0
```

# show sbc sbe media-gateway-policy

To display the details of a media gateway policy, use the **show sbc sbe media-gateway-policy** command in the privileged EXEC mode.

```
show sbc sbc-name sbe media-gateway-policy [stats | type {default | local | remote {ipv4 | ipv6}
ip-address [port port-number]]
```

Syntax Description		
	<i>sbc-name</i>	Name of the SBC.
	<b>stats</b>	Specifies that the media gateway policy statistics must be displayed.
	<b>type</b>	Specifies that the configuration and status of the specified media gateway policy type must be displayed. The type can be <b>default</b> , <b>local</b> , or <b>remote</b> .
	<b>default</b>	Specifies that the configuration and status of the default media gateway policy must be displayed.
	<b>local</b>	Specifies that the configuration and status of the local media gateway policy must be displayed.
	<b>remote</b>	Specifies that the configuration and status of the remote media gateway policy must be displayed.
	<b>ipv4</b>	Specifies that the remote media gateway has an IPv4 IP address.
	<b>ipv6</b>	Specifies that the remote media gateway has an IPv6 IP address.
	<i>ip-address</i>	IP address of the remote media gateway. The IP address can be in the IPv4 format or IPv6 format.
	<b>port</b>	Specifies the port number of the remote media gateway.
	<i>port-number</i>	Port number of the remote media gateway.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following command shows the output of the **show sbc sbe media-gateway-policy type** command for a remote type media gateway policy:

```
Router# show sbc mySbc sbe media-gateway-policy type remote ipv4 192.0.2.26 port 6886

Gateway Policy Type           =      REMOTE
-----
Remote vpn                     =      0
```

```

Remote address type      =    IPV4
Remote address          =    192.0.2.26
Remote Port             =    6886
Media Limit Table       =
Transcode Audio Cost    =    10
Transrate Audio Cost    =    6
    
```

**Related Commands**

Command	Description
<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
<b>media-gateway policy type</b>	Configures a media gateway policy.
<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
<b>media-policy</b>	Configures a media policy.
<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
<b>show sbc sbe media-policy</b>	Displays the details of media policies.
<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.



# show sbc sbe media-gateways

To list the gateway configuration and attachment status on SBE, use the **show sbc sbe media-gateways** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe media-gateways**

<b>Syntax Description</b>	<i>sbc-name</i> Specifies the SBC service.				
<b>Command Default</b>	No default behavior or values are available.				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

**Examples**

The following example shows how to list the gateway configuration and attachment status on SBEs:

```
Router# show sbc mySbc sbe media-gateways

SBC Service "mySbc"
  Configured Gateway 10.0.0.1
  Configured Gateway 100.1.0.1
  Configured Gateway 172.3.4.9
```

# show sbc sbe media-policy

To display the details of media policies, use the **show sbc sbe media-policy** command in the privileged EXEC mode.

**show sbc *sbc-name* sbe media-policy [*policy-name*]**

Syntax Description	
<i>sbc-name</i>	Name of the SBC.
<i>policy-name</i>	Name of the media policy. If you do not enter the name of a media policy, the command displays details of all media policies configured on the SBC.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** In the following example, the **show sbc sbe media-policy** command is used to display the details of the my\_media\_policy media policy:

```
Router# show sbc mySbc sbe media-policy my_media_policy
```

```
Policy Name: my_media_policy
```

```
-----
Type = gateway
Audio transcode limit = 30
Audio transrate limit = 30
Video transcode limit = 30
Inband-dtmf-iw limit = 10
SRTP-iw limit = 20
Total resource limit = 40
```

Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.

<b>Command</b>	<b>Description</b>
<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
<b>media-gateway policy type</b>	Configures a media gateway policy.
<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
<b>media-policy</b>	Configures a media policy.
<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
<b>show sbc sbe media-policy</b>	Displays the details of media policies.
<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.



# show sbc sbe policy-failure-stats

To list the statistics for all of the policy failures on a specific SBE, use the **show sbc sbe policy-failure-stats** command in Privileged EXEC mode.

```
show sbc sbc-name sbe policy-failure-stats period
```

Syntax Description	
<i>sbc-name</i>	Specifies the SBC service.
<i>period</i>	Specifies the time period for the statistics that you want to display. The time period can be one of the following: <ul style="list-style-type: none"> <li>• <b>current15mins</b>—Displays statistics in 15 minute intervals starting from the current minute.</li> <li>• <b>current5mins</b>—Displays statistics in 5 minute intervals starting from the current minute.</li> <li>• <b>currentday</b>—Displays statistics for the current day starting midnight of the same day.</li> <li>• <b>currenthour</b>—Displays statistics for the current hour.</li> <li>• <b>previous15mins</b>—Displays statistics from previous 15 minute intervals.</li> <li>• <b>previous5mins</b>—Displays statistics from previous 5 minute intervals.</li> <li>• <b>previousday</b>—Displays statistics from the previous day.</li> <li>• <b>previoushour</b>—Displays statistics from the previous hour.</li> </ul>

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	This command is obsolete in Cisco IOS XE Release 2.5.

**Usage Guidelines** The statistics are collected at 5 minute intervals past the hour (that is, at 0, 5, 10, 15 minutes, and so on past the hour). For example, the periods covered by the various buckets at 12:43 would be as follows:

- current five minutes: 12:40-12:43
- previous five minutes: 12:35-12:40
- current 15 minutes: 12:30-12:43
- previous 15 minutes: 12:15-12:30

- current hour: 12:00-12:43
- last hour: 11:00-12:00
- current day: 00:00-12:43
- last day: 00:00-24h - 00:00.

**Examples**

The following example shows the complete policy failure statistics for source adjacency glophone and source account 200 for the current day:

```
Router# show sbc global sbe policy-failure-stats currentday

SBC Service ''global''
Policy failure statistics for the current day for source adjacency glophone:
  Total call setup failures:          8
  Call setups failed due to NA:       0
  Call setups failed due to rtg:      8
  Call setups failed due to CAC:      0
  CAC fails due to num call lim:      0
  CAC fails due to rate call lim:     0
  CAC fails due to num channels lim:  0
  CAC fails due to bandwidth lim:     0

Policy failure statistics for the current day for source account 200
  Total call setup failures:          8
  Call setups failed due to NA:       0
  Call setups failed due to rtg:      8
  Call setups failed due to CAC:      0
  CAC fails due to num call lim:      0
  CAC fails due to rate call lim:     0
  CAC fails due to num channels lim:  0
  CAC fails due to bandwidth lim:     0
```

Table 1 describes the important fields shown in the output of the command.

**Table 1** show sbc sbe policy-failure-stats Field Descriptions

Field	Description
Total call setup failures	Total number of call setup failures due to Number Analysis, Routing, and CAC Policies.
Call setups failed due to NA	Total number of call setup failures due to Number Analysis policies.
Call setups failed due to rtg	Total number of call setup failures due to routing policies.
Call setups failed due to CAC	Total number of call setup failures due to CAC policies.
CAC fails due to num call lim	Total number of call setup failures due to CAC call limits.
CAC fails due to call rate lim	Total number of call setup failures due to CAC call rate limits.
CAC fails due to num media channels lim	Total number of call setup failures due to CAC number of media channels limits.
CAC fails due to num media updates lim	Total number of call setup failures due to CAC number of media updates limits.
CAC fails due to bandwidth lim	Total number of call setup failures due to CAC Bandwidth Limits.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear sbc sbe policy-rejection-stats</b>	Clears all the policy rejection statistics by the SBE.
	<b>show sbc sbe policy-failure-stats src-adjacency</b>	Lists the statistics for all the policy failures on the specified SBE.
	<b>show sbc sbe policy-failure-stats dst-adjacency</b>	Lists the statistics for the policy failures for calls with the adjacency.
	<b>show sbc sbe policy-failure-stats src-account</b>	Lists the statistics for the policy failures for calls with the account.
	<b>show sbc sbe policy-failure-stats dst-account</b>	Lists the statistics for the policy failures for calls with the account.

# show sbc sbe policy-failure-stats dst-account

To list policy failure statistics for a specified target account for a specified time period, use the **show sbc sbe policy-failure-stats dst-account** command in Privileged EXEC mode.

**show sbc** *sbc-name* **sbe policy-failure-stats dst-account** *name* **period** *time-period*

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
<i>name</i>	Specifies the name of the account for which you would like to display statistics. The maximum length of this value is 30 characters.
<b>period</b> <i>time-period</i>	Specifies the time period to which the statistics apply. Choose one of the following time intervals: <ul style="list-style-type: none"> <li>• <b>current15mins</b>—Displays statistics in 15 minute intervals starting from the current minute.</li> <li>• <b>current5mins</b>—Displays statistics in 5 minute intervals starting from the current minute.</li> <li>• <b>currentday</b>—Displays statistics for the current day starting midnight of the same day.</li> <li>• <b>currenthour</b>—Displays statistics for the current hour.</li> <li>• <b>previous15mins</b>—Displays statistics from previous 15 minute intervals.</li> <li>• <b>previous5mins</b>—Displays statistics from previous 5 minute intervals.</li> <li>• <b>previousday</b>—Displays statistics from the previous day.</li> <li>• <b>previoushour</b>—Displays statistics from the previous hour.</li> </ul>

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command is obsolete in Cisco IOS XE Release 2.5.

## Usage Guidelines

The statistics are collected at 5 minute intervals past the hour (that is, at 0, 5, 10, 15 minutes, and so on past the hour). For example, the periods covered by the various buckets at 12:43 would be as follows:

- current five minutes: 12:40-12:43
- previous five minutes: 12:35-12:40
- current 15 minutes: 12:30-12:43



- previous 15 minutes: 12:15-12:30
- current hour: 12:00-12:43
- last hour: 11:00-12:00
- current day: 00:00-12:43
- last day: 00:00-24h - 00:00.

## Examples

The following example lists the policy failure statistics for an adjacent account named AA for the current hour:

```
Router# show sbc mysbc sbe policy-failure-stats dst-account AA period currenthour

SBC Service "mysbc"
Policy failure statistics for the current hour for source adjacency AA

Total call setup failures: 10
Call setups failed due to NA: 5
Call setups failed due to rtg: 3
Call setups failed due to CAC: 2
CAC fails due to num call lim: 1
CAC fails due to rate call lim: 0
CAC fails due to num channels lim: 0
CAC fails due to bandwidth lim: 1
```

[Table 2](#) describes the important fields shown in the output of the command.

**Table 2** *show sbc sbe policy-failure-stats dst-account Field Descriptions*

Field	Description
Total call setup failures	Total number of call setup failures due to Number Analysis, Routing, and CAC Policies.
Call setups failed due to NA	Total number of call setup failures due to Number Analysis policies.
Call setups failed due to rtg	Total number of call setup failures due to routing policies.
Call setups failed due to CAC	Total number of call setup failures due to CAC policies.
CAC fails due to num call lim	Total number of call setup failures due to CAC call limits.
CAC fails due to call rate lim	Total number of call setup failures due to CAC call rate limits.
CAC fails due to num media channels lim	Total number of call setup failures due to CAC number of media channels limits.
CAC fails due to num media updates lim	Total number of call setup failures due to CAC number of media updates limits.
CAC fails due to bandwidth lim	Total number of call setup failures due to CAC Bandwidth Limits.

Related Commands	Command	Description
	<b>show sbc sbe policy-failure-stats dst-adjacency</b>	Lists policy failure statistics for calls within the specified target adjacency for the specified time period.
	<b>show sbc sbe policy-failure-stats src-account</b>	Lists policy failure statistics for calls within the specified source account for the specified time period.
	<b>show sbc sbe policy-failure-stats src-adjacency</b>	Lists policy failure statistics for calls within the specified source adjacency for the specified time period.

# show sbc sbe policy-failure-stats dst-adjacency

To list policy failure statistics for a specified target adjacency for a specified time period **use the show sbc sbe policy-failure-stats dst-adjacency command in Privileged EXEC mode.**

**show sbc** *sbc-name* **sbe policy-failure-stats dst-adjacency** *name* **period** *time-period*

Syntax Description	
<i>sbc-name</i>	Specifies the name of the SBC service.
<i>name</i>	Specifies the name of the adjacency for which you would like to display statistics. The maximum length of this value is 30 characters.
<b>period</b> <i>time-period</i>	Specifies the time period to which the statistics apply. Choose one of the following time intervals: <ul style="list-style-type: none"> <li>• <b>current15mins</b>—Displays statistics in 15 minute intervals starting from the current minute.</li> <li>• <b>current5mins</b>—Displays statistics in 5 minute intervals starting from the current minute.</li> <li>• <b>currentday</b>—Displays statistics for the current day starting midnight of the same day.</li> <li>• <b>currenthour</b>—Displays statistics for the current hour.</li> <li>• <b>previous15mins</b>—Displays statistics from previous 15 minute intervals.</li> <li>• <b>previous5mins</b>—Displays statistics from previous 5 minute intervals.</li> <li>• <b>previousday</b>—Displays statistics from the previous day.</li> <li>• <b>previoushour</b>—Displays statistics from the previous hour.</li> </ul>

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	This command is obsolete in Cisco IOS XE Release 2.5.

**Usage Guidelines** The statistics are collected at 5 minute intervals past the hour (that is, at 0, 5, 10, 15 minutes, and so on past the hour). For example, the periods covered by the various buckets at 12:43 would be as follows:

- current five minutes: 12:40-12:43
- previous five minutes: 12:35-12:40
- current 15 minutes: 12:30-12:43

- previous 15 minutes: 12:15-12:30
- current hour: 12:00-12:43
- last hour: 11:00-12:00
- current day: 00:00-12:43
- last day: 00:00-24h - 00:00.

**Examples**

The following example shows the policy failure statistics for an adjacency named ZZ for the current hour:

```
Router# show sbc mysbc sbe policy-failure-stats dst-adjacency ZZ period currenthour

SBC Service "mysbc"
Policy failure statistics for the current hour for source adjacency ZZ

Total call setup failures: 10
Call setups failed due to NA: 5
Call setups failed due to rtg: 3
Call setups failed due to CAC: 2
CAC fails due to num call lim: 1
CAC fails due to rate call lim: 0
CAC fails due to num channels lim: 0
CAC fails due to bandwidth lim: 1
```

Table 3 describes the important fields shown in the output of the command.

**Table 3** show sbc sbe policy-failure-stats dst-adjacency Field Descriptions

Field	Description
Total call setup failures	Total number of call setup failures due to Number Analysis, Routing, and CAC Policies.
Call setups failed due to NA	Total number of call setup failures due to Number Analysis policies.
Call setups failed due to rtg	Total number of call setup failures due to routing policies.
Call setups failed due to CAC	Total number of call setup failures due to CAC policies.
CAC fails due to num call lim	Total number of call setup failures due to CAC call limits.
CAC fails due to call rate lim	Total number of call setup failures due to CAC call rate limits.
CAC fails due to num media channels lim	Total number of call setup failures due to CAC number of media channels limits.
CAC fails due to num media updates lim	Total number of call setup failures due to CAC number of media updates limits.
CAC fails due to bandwidth lim	Total number of call setup failures due to CAC Bandwidth Limits.

Related Commands	Command	Description
	<b>show sbc sbe policy-failure-stats dst-account</b>	Lists policy failure statistics for calls within the specified target account for the specified time period.
	<b>show sbc sbe policy-failure-stats src-account</b>	Lists policy failure statistics for calls within the specified source account for the specified time period.
	<b>show sbc sbe policy-failure-stats src-adjacency</b>	Lists policy failure statistics for calls within the specified source adjacency for the specified time period.

# show sbc sbe policy-failure-stats src-account

To list policy failure statistics for a specified source account for a specified time period use the **show sbc sbe policy-failure-stats src-account** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe policy-failure-stats src-account *name* period *time-period***

## Syntax Description

<b>sbc-name</b>	Specifies the name of the SBC service.
<b><i>name</i></b>	Specifies the name of the account for which you would like to display statistics. The maximum length of this value is 30 characters.
<b>period <i>time-period</i></b>	Specifies the time period to which the statistics apply. Choose one of the following time intervals: <ul style="list-style-type: none"> <li>• <b>current15mins</b>—Displays statistics in 15 minute intervals starting from the current minute.</li> <li>• <b>current5mins</b>—Displays statistics in 5 minute intervals starting from the current minute.</li> <li>• <b>currentday</b>—Displays statistics for the current day starting midnight of the same day.</li> <li>• <b>currenthour</b>—Displays statistics for the current hour.</li> <li>• <b>previous15mins</b>—Displays statistics from previous 15 minute intervals.</li> <li>• <b>previous5mins</b>—Displays statistics from previous 5 minute intervals.</li> <li>• <b>previousday</b>—Displays statistics from the previous day.</li> <li>• <b>previoushour</b>—Displays statistics from the previous hour.</li> </ul>

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command is obsolete in Cisco IOS XE Release 2.5.

## Usage Guidelines

The statistics are collected at 5 minute intervals past the hour (that is, at 0, 5, 10, 15 minutes, and so on past the hour). For example, the periods covered by the various buckets at 12:43 would be as follows:

- current five minutes: 12:40-12:43
- previous five minutes: 12:35-12:40
- current 15 minutes: 12:30-12:43

- previous 15 minutes: 12:15-12:30
- current hour: 12:00-12:43
- last hour: 11:00-12:00
- current day: 00:00-12:43
- last day: 00:00-24h - 00:00.

## Examples

The following example shows the policy failure statistics for a source account named BB for the current hour:

```
Router# show sbc mysbc sbe policy-failure-stats src-account BB period currenthour

SBC Service "mysbc"
Policy failure statistics for the current hour for source adjacency BB

Total call setup failures: 10
Call setups failed due to NA: 5
Call setups failed due to rtg: 3
Call setups failed due to CAC: 2
CAC fails due to num call lim: 1
CAC fails due to rate call lim: 0
CAC fails due to num channels lim: 0
CAC fails due to bandwidth lim: 1
```

[Table 4](#) describes the important fields shown in the output of the command.

**Table 4** *show sbc sbe policy-failure-stats src-account Field Descriptions*

Field	Description
Total call setup failures	Total number of call setup failures due to Number Analysis, Routing, and CAC Policies.
Call setups failed due to NA	Total number of call setup failures due to Number Analysis policies.
Call setups failed due to rtg	Total number of call setup failures due to routing policies.
Call setups failed due to CAC	Total number of call setup failures due to CAC policies.
CAC fails due to num call lim	Total number of call setup failures due to CAC call limits.
CAC fails due to call rate lim	Total number of call setup failures due to CAC call rate limits.
CAC fails due to num media channels lim	Total number of call setup failures due to CAC number of media channels limits.
CAC fails due to num media updates lim	Total number of call setup failures due to CAC number of media updates limits.
CAC fails due to bandwidth lim	Total number of call setup failures due to CAC Bandwidth Limits.

Related Commands	Command	Description
	<b>show sbc sbe policy-failure-stats dst-adjacency</b>	Lists policy failure statistics for calls within the specified target adjacency for the specified time period.
	<b>show sbc sbe policy-failure-stats dst-account</b>	Lists policy failure statistics for calls within the specified target account for the specified time period.
	<b>show sbc sbe policy-failure-stats src-adjacency</b>	Lists policy failure statistics for calls within the specified source adjacency for the specified time period.



# show sbc sbe policy-failure-stats src-adjacency

To list policy failure statistics for a specified source adjacency for a specified time period **use the show sbc sbe policy-failure-stats src-adjacency command in Privileged EXEC mode.**

**show sbc** *sbc-name* **sbe policy-failure-stats src-adjacency** *name* **period** *time-period*

## Syntax Description

<b>sbc-name</b>	Specifies the name of the SBC service.
<i>name</i>	Specifies the name of the adjacency for which you would like to display statistics. The maximum name length is 30 characters.
<b>period</b> <i>time-period</i>	Specifies the time period to which the statistics apply. Choose one of the following time intervals: <ul style="list-style-type: none"> <li>• <b>current15mins</b>—Displays statistics in 15 minute intervals starting from the current minute.</li> <li>• <b>current5mins</b>—Displays statistics in 5 minute intervals starting from the current minute.</li> <li>• <b>currentday</b>—Displays statistics for the current day starting midnight of the same day.</li> <li>• <b>currenthour</b>—Displays statistics for the current hour.</li> <li>• <b>previous15mins</b>—Displays statistics from previous 15 minute intervals.</li> <li>• <b>previous5mins</b>—Displays statistics from previous 5 minute intervals.</li> <li>• <b>previousday</b>—Displays statistics from the previous day.</li> <li>• <b>previoushour</b>—Displays statistics from the previous hour.</li> </ul>

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command is obsolete in Cisco IOS XE Release 2.5.

## Usage Guidelines

The statistics are collected at 5 minute intervals past the hour (that is, at 0, 5, 10, 15 minutes, and so on past the hour). For example, the periods covered by the various buckets at 12:43 would be as follows:

- current five minutes: 12:40-12:43
- previous five minutes: 12:35-12:40
- current 15 minutes: 12:30-12:43

- previous 15 minutes: 12:15-12:30
- current hour: 12:00-12:43
- last hour: 11:00-12:00
- current day: 00:00-12:43
- last day: 00:00-24h - 00:00.

**Examples**

The following example displays policy failure statistics for a source adjacency named YY for the current hour:

```
Router# show sbc test sbe policy-failure-stats src-adjacency Acct1
period current15mins

SBC Service ''test''
Policy failure statistics for the current 15 mins for source adjacency Acct1
Total call setup failures: 0
Call setups failed due to NA: 0
Call setups failed due to rtg: 0
Call setups failed due to CAC: 0
CAC fails due to num call lim: 0
CAC fails due to rate call lim: 0
CAC fails due to num channels lim: 0
CAC fails due to bandwidth lim: 0
```

Table 5 describes the important fields shown in the output of the command.

**Table 5** show sbc sbe policy-failure-stats src-adjacency Field Descriptions

Field	Description
Total call setup failures	Total number of call setup failures due to Number Analysis, Routing, and CAC Policies.
Call setups failed due to NA	Total number of call setup failures due to Number Analysis policies.
Call setups failed due to rtg	Total number of call setup failures due to routing policies.
Call setups failed due to CAC	Total number of call setup failures due to CAC policies.
CAC fails due to num call lim	Total number of call setup failures due to CAC call limits.
CAC fails due to call rate lim	Total number of call setup failures due to CAC call rate limits.
CAC fails due to num media channels lim	Total number of call setup failures due to CAC number of media channels limits.
CAC fails due to num media updates lim	Total number of call setup failures due to CAC number of media updates limits.
CAC fails due to bandwidth lim	Total number of call setup failures due to CAC Bandwidth Limits.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc sbe policy-failure-stats dst-adjacency</b>	Lists policy failure statistics for calls within the specified target adjacency for the specified time period.
	<b>show sbc sbe policy-failure-stats src-account</b>	Lists policy failure statistics for calls within the specified source account for the specified time period.
	<b>show sbc sbe policy-failure-stats dst-account</b>	Lists policy failure statistics for calls within the specified target account for the specified time period.

# show sbc sbe qos-profiles

To list all QoS profiles, use the **show sbc sbe qos-profiles** command in Privileged EXEC mode.

```
show sbc sbc-name sbe qos-profiles [profile-name]
```

## Syntax Description

sbc-name	Specifies the name of the SBC service.
profile-name	(Optional) Specifies the profile name.
	If you specify a QoS profile, the details of that profile are shown.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to list all of the QoS profiles on the SBE:

```
Router# show sbc test sbe qos-profiles
```

```
SBC Service ''test''
profile name Class
-----
default Voice
profile6 Voice
residential Voice
default Video
profile3 Video
profile5 Video
profile7 Video
profile9 Video
default Fax
default Signaling
profile2 Signaling
profile4 Signaling
profile8 Signaling 7
```

The **show sbc test sbe qos-profiles** command is invalid when displaying one profile. Correct usage is singular as shown below.

```
Router# show sbc test sbe qos-profiles profile6
^
% long command detected at '^' marker.

Router# show sbc test sbe qos-profile profile6
SBC Service ''test''
QoS profile profile6
```

```
Class of Service Voice
Marking type Passthrough

Router#
```

# show sbc sbe radius-client-accounting accounting

To list the parameters configured for the account, use the **show sbc sbe radius-client-accounting accounting** command in Privileged EXEC mode.

```
show sbc sbc-name sbe radius-client-accounting accounting client-name
```

Syntax Description	
<i>sbc name</i>	This is the name of the SBC service.
<i>client-name</i>	Clears all statistics for the specified local RADIUS client.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example lists the parameters configured for accounting:

```
Router# show sbc uut105-1 sbe radius-client-accounting accounting SBC1-account-1
```

```
SBC Service ''uut105-1''
radius client address = 88.105.2.100
radius client retry interval = 1200
radius client retry limit = 5
radius client concurrent requests limit = 250
Router#
```

# show sbc sbe radius-client-accounting authentication

To list the parameters configured for the authentication, use the **show sbc sbe radius-client-accounting authentication** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe radius-client-accounting authentication**

<b>Syntax Description</b>	<i>sbc name</i> This is the name of the SBC service.				
<b>Command Default</b>	No default behavior or values are available.				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

## Examples

The following example lists the parameters configured for the authentication:

Router# **show sbc mysbc sbe radius-client-accounting authentication**

```
SBC Service ''node105''
radius client address = 88.105.128.100
radius client retry interval = 1800
radius client retry limit = 5
radius client concurrent requests limit = 250
```

# show sbc sbe radius-client-stats

To list the RADIUS accounting client statistics for all accounting clients configured on an SBE, use the **show sbc sbe radius-client-stats** command in Privileged EXEC mode.

```
show sbc sbc-name sbe radius-client-stats radius-client [accounting client-name |
authentication]
```

## Syntax Description

<i>sbc name</i>	This is the name of the SBC service.
<i>radius-client</i>	Specifies the RADIUS client to show.
<b>accounting</b> <i>client-name</i>	Specifies the name to assign to the accounting RADIUS client.
<b>authentication</b>	Enables client authentication.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to list the RADIUS accounting server statistics for all accounting servers configured on an SBE:

```
Router# show sbc j sbe radius-client-stats accounting CISCO_UM
SBC Service "j"
  Bad address packets:      0
  Primary server:           RADIUS1
  Radius SET state:        Active
```

The following example shows how to list the RADIUS accounting server statistics for all authentication servers configured on an SBE:

```
Router# show sbc j sbe radius-client-stats authentication
SBC Service "j"
  Bad address packets:      0
  Primary server:
```



## show sbc sbe radius-server-stats

To list the RADIUS server statistics for all accounting servers configured on a RADIUS client on an SBE, use the **show sbc sbe radius-server-stats** command in Privileged EXEC mode.

```
show sbc sbc-name sbe radius-server-stats radius-client [accounting client-name | authentication]
```

Syntax Description		
	<i>sbc name</i>	This is the name of the SBC service.
	<i>radius-client</i>	Specifies the RADIUS client to show.
	<b>accounting</b> <i>client-name</i>	Specifies the name to assign to the accounting RADIUS client.
	<b>authentication</b>	Enables client authentication.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Examples

The following example shows how to list the RADIUS server statistics for all accounting servers configured on a radius client on an SBE:

```
Router# show sbc sanity sbe radius-server-stats accounting SBC1-account-1

SBC Service ''sanity''
Cisco-AR1-PC:
Round trip time: 0 ms
Access-requests sent: 0
Access-request retransmitted: 0
Access-accepts received: 0
Access-reject received: 0
Access-challenge received: 0
Accounting-requests sent: 0
Accounting-requests retransmitted: 0
Accounting-responses received: 0
Malformed packets received: 0
Invalid authenticators received: 0
Outstanding responses: 0
Timeouts occurred: 0
Unknown packets: 0
Packets dropped: 0
```

The following example shows how to list the RADIUS server statistics for all authentication servers configured on a radius client on an SBE:

```
Router# show sbc sanity sbe radius-server-stats authentication
```

```
SBC Service ''sanity''  
Cisco-AR1-PC:  
Round trip time: 0 ms  
Access-requests sent: 0  
Access-request retransmitted: 0  
Access-accepts received: 0  
Access-reject received: 0  
Access-challenge received: 0  
Accounting-requests sent: 0  
Accounting-requests retransmitted: 0  
Accounting-responses received: 0  
Malformed packets received: 0  
Invalid authenticators received: 0  
Outstanding responses: 0  
Timeouts occurred: 0  
Unknown packets: 0  
Packets dropped: 0
```

# show sbc sbe redirect-limit

To display the current limit on the maximum number of redirections that a call can undergo, use the **show sbc sbe redirect-limit** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe redirect-limit**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Examples</b>	The following example displays the limit on the maximum number of redirections that a call can undergo:
-----------------	---

```
Router# show service sbc mysbc sbe redirect-limit
```

```
SBC Service "mySbc"
Call redirect limit is 4
```

# show sbc sbe resource-priority-sets

To display the resource priority sets, use the **show sbc sbe resource-priority-sets** command in Privileged EXEC mode.

```
show sbc sbc-name sbe resource-priority-sets
```

<b>Syntax Description</b>	<i>sbc-name</i> Specifies the name of the SBC service.
---------------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Lists the high-level status and capabilities of each instantiated SBE or DBE.

**Examples** The following example shows how the **show sbc sbe resource-priority-sets** command is used to display the resource priority sets:

```
Router# show sbc mysbc sbe resource-priority-sets
SBC Service 'mysbc'
Resource priority sets
-----
dsn
Router# show sbc test sbe resource-priority-set dsn
SBC Service 'mysbc'
Resource priority set: dsn

Name Value
-----
dsn.flash Flash
ACE-104-1.4/Admin#
```

# show sbc sbe script-set

To display a summary of the details pertaining to all the configured script sets or show the details of a specified script set, use the **show sbc sbe script-set** command in the privileged EXEC mode.

```
show sbc sbc-name sbe script-set script-set-number [program [line-numbers] | script script-name [line-numbers] | statistics]
```

## Syntax Description

<i>sbc-name</i>	Name of the SBC service.
<i>script-set-number</i>	Script set number.
<b>program</b>	Specifies that all scripts must be displayed as a single program.
<b>line-numbers</b>	Specifies that line numbers must be included while displaying the scripts.
<b>script</b>	Specifies that details of a single script from the script set must be displayed.
<i>script-name</i>	Name of the script that must be displayed.
<b>statistics</b>	Specifies that script set statistics must be displayed.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the privileged EXEC mode. The Examples section shows the output of the command for each output mode (program, script, and statistics) that the command supports.

## Examples

In the following example, the **program** output mode has been specified in the **show sbc sbe script-set** command:

```
Router# show sbc mySbc sbe script-set 10 program line-numbers

1  : function add_a_line1(msg)
2  : msg.sdp.insert_child_last(MeSdpLine.new("a=rtpmap:0 PCMU/8000"))
3  : end
4  : MeEditor.register(MeEditor.AFTER_SEND, "sdp_add_a_after", add_a_line1)
5  :
6  :
7  :
8  : --Script to delete all a=candidate and a=ice lines in sdp
```

```

9 :
10 : function remove_specified_a_line(msg)
11 :   for line in msg.sdp:select_by_prefix("a=candidate"):iter() do
12 :     line:delete()
13 :   end
14 :   for line in msg.sdp:select_by_prefix("a=ice"):iter() do
15 :     line:delete()
16 :   end
17 : end
18 :
19 :
MeEditor.register(MeEditor.BEFORE_RECEIVE,"remove_specified_a_line",remove_specified_a_line)

```

In the following example, the **script** output mode has been specified in the **show sbc sbe script-set** command:

```

Router# show sbc SBC1 sbe script-set 10 script remove-a-line line-numbers

1 :
2 : --Script to delete all a=candidate and a=ice lines in sdp
3 :
4 : function remove_specified_a_line(msg)
5 :   for line in msg.sdp:select_by_prefix("a=candidate"):iter() do
6 :     line:delete()
7 :   end
8 :   for line in msg.sdp:select_by_prefix("a=ice"):iter() do
9 :     line:delete()
10 :   end
11 : end
12 :
13 :
MeEditor.register(MeEditor.BEFORE_RECEIVE,"remove_specified_a_line",remove_specified_a_line)

```

In the following example, the **statistics** output mode has been specified in the **show sbc sbe script-set** command:

```

Router# show sbc mySbc sbe script-set 10 statistics

Current Memory Usage =      40461      (bytes)
Total Memory Limit =        0      (bytes)
Total Failures =            0
Last Script Failure =       ""
Last Failure Line-Number =  0
Last Failure Cause =       ""
Stack:

```

**Related Commands**

Command	Description
<b>active-script-set</b>	Activates a script set,
<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
<b>editor</b>	Specifies the order in which a particular editor must be applied.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.

<b>Command</b>	<b>Description</b>
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>test script-set</b>	Tests the working of a script set.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# show sbc sbe sdp-h245-mapping

To display the mapping for codec strings between SDP (SIP) and H245 (H323), use the **show sbc sbe sdp-h245-mapping** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sdp-h245-mapping
```

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Lists the high-level status and capabilities of each instantiated SBE or DBE.

**Examples** The following example shows how the **show sbc sbe sdp-h245-mapping** command is used.

```
Router# show sbc mysbc sbe sdp-h245-mappings
```

```
SBC Service 'mysbc'
```

```
SDP H.245
```

```
-----
```

```
PCMA g711A1aw64k
```

```
PCMU g711U1aw64k
```

```
G722 g722_64k
```

```
G723 g7231
```

```
G728 g728
```

```
G729 g729,
```

```
g729AnnexA,
```

```
g729wAnnexB,
```

```
g729AnnexAwAnnexB
```

```
GSM gsmFullRate
```

```
t38 t38Fax
```

```
In H.323 calls,
```

```
- T.38 fax is the only non-audio codec supported.
```

```
- Audio codecs not in the list above are reported as 'PCMU'.
```

```
In SIP/H.323 interworking calls, only audio codecs using static RTP payload types are supported.
```



# show sbc sbe sdp-match-table

This command was deprecated in Cisco IOS XE Release 2.5.

To show the SDP match table configured on the SBC, use the **show sbc sbe sdp-match-table** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sdp-match-table [detail]
```

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
detail	Shows the SDP attribute configured on a given SDP match table.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command was deprecated. It was replaced by the new command <b>show sbc sbe sip sdp-match-table</b> .

## Examples

The following example shows how the **show sbc sbe sdp-match-table** command is used to display SDP match table:

```
Router# show sbc pgw sbe sdp-match-table detail
  Name      : m          <--- table name
  Action    : blacklist  <--- action: blacklist or whitelist
  Match String : ddd      <--- several match string
                ddf

-----
  Name      : n
  Action    : whitelist
  Match String : 2
                3
                4
```

## Related Commands

Command	Description
<b>show sbc sbe sdp-h245-mapping</b>	Displays the mapping for codec strings between SDP (SIP) and H245 (H323).

# show sbc sbe sdp-policy-table

This command was deprecated in Cisco IOS XE Release 2.5.

To show the SDP policy table configured on the SBC, use the **show sbc sbe sdp-policy-table** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sdp-policy-table
```

<b>Syntax Description</b>	<i>sbc-name</i> Specifies the name of the SBC service.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	This command was deprecated. It was replaced by the new command <b>show sbc sbe sip sdp-policy-table</b> .

**Examples** The following example shows how the **show sbc sbe sdp-policy-table** command is used to display the SDP policy table:

```
Router# show sbc pgw sbe sdp-policy-table
      Name                               SDP Match Table
      -----                               -
      p                                   m           <--- "m" is sdp match table name
```

Related Commands	Command	Description
	<b>show sbc sbe sdp-match-table</b>	Shows the SDP match table configured on the SBC.

# show sbc sbe sip body-editor

To display all the body editors of the non-SDP message bodies or the details for a specific body editor, use the **show sbc sbe sip body-editor** command in the Privileged EXEC mode.

```
show sbc sbc-name sbe sip body-editor [editor-name]
```

Syntax Description	<i>sbc-name</i>	Name of the SBC service.
	<i>editor-name</i>	Name of the editor. Also, displays details about the specified editor.
		If omitted, information pertaining to all the SIP body editors is displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to display all the non-SDP message body editors that are in use:

```
Router# show sbc mySBC sbe sip body-editor
```

```
body-editors for SBC service "mySBC"
Name                               In use
=====
Hello                               No
default                             Yes
```

The following example shows how to display the details of a specific non-SDP message body editor named editor2:

```
Router# show sbc mySBC sbe sip body-editor Body1
```

```
body-editor "Body1"
Description: "The first Body Editor"
Bodies:
  media-type/media-sub-type
  action nopass
  hunt-on-reject false
In use by adjacency:SIPP (in)
Not in use with any method-editor
```

Related Commands	Command	Description
	<b>sip body-editor</b>	Configures a body editor.

# show sbc sbe sip body-profile

To display all body profiles of non-SDP message bodies or to show details for a specified body profile, use the **show sbc sbe sip body-profile** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sip body-profile [body_profile-name]
```

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
<b>body_profile-name</b>	Optional. Specifies the name of the body profile and displays details about the specified body profile.  If omitted, the command shows information about all body profiles.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example displays all the non-SDP message body profiles in use:

```
Router# show sbc mySBC sbe sip body-profile
```

```
Name                In Use
profile1            Yes
profile2            Yes
profile3            No
```

The following example displays the details of the specified non-SDP message body profile named “profile2”:

```
Router# show sbc mySBC sbe sip body-profile profile2
```

```
Name                : profile2
Description         : test-profile

Element            : application/ISUP
Action             : nopass

Hunt-on-reject:    : false

Element            : application/QSIG
Action             : pass
Hunt-on-reject:    : false
```

# show sbc sbe sip delegate-profiles

To display delegate profiles for subscribers for whom Provisioned Delegate Registration has been configured, use the **show sbc sbe sip delegate-profiles** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip delegate-profiles**

<b>Syntax Description</b>	<i>sbc-name</i> Specifies the name of the SBC service.				
<b>Command Default</b>	No default behavior or values are available.				
<b>Command Modes</b>	Privileged EXEC (#)				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

## Examples

The following example displays delegate profiles for subscribers for whom delegate registration has been configured:

```
Router# show sbc mySBC sbe sip delegate-profiles
      0      1      2      3      4      5      6      7
012345789012345789012345789012345789012345789012345789012345789

Delegate profiles:
-----
profile           = steve
Duration (secs)   = 1800
Retry Count       = 3
Retry Interval (secs) = 30
Refresh Buffer (secs) = 30
-----
```

# show sbc sbe sip error-profile

To display the configuration information of an error profile, use the **show sbc sbe sip error-profile** command in privileged EXEC mode.

**show sbc** *sbc-name* **sbe sip error-profile** *error-profile-name*

Syntax Description	Parameter	Description
	<i>sbc-name</i>	Name of the SBC service.
	<i>error-profile-name</i>	Name of the configured error profile.

**Command Default** If the *error-profile-name* is not given, information for all error profiles is displayed.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to display the configuration information of an error profile:

**Example 1: Default Error profile**

```
Router# show sbc SBC1 sbe sip error-profile

Name                               in-use
=====
default                             yes
```

**Example 2: Specific Error profile**

```
Router# show sbc SBC2 sbe sip error-profile Error_profile_1

Error profile "Error_profile_1"
  Description:
  cause rtg-no-route-found      sub-cause rtg-src-adjacency
    status-code: 604
    reason: "SBC: No route found based on src adjacency"
  cause rtg-route-unavailable  sub-cause
    status-code: 486
    reason: "SBC: no route available"
  in use by adjacency:sip-1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>error-profile</b>	Configures an existing error profile as the outbound SIP error profile.
<b>sip error-profile</b>	Creates an error profile and enters error profile configuration mode.
<b>cause</b>	Configures the cause of an internal error for an error profile.
<b>show sbc sbe sip error-profile</b>	Displays the configuration information of an error profile.

# show sbc sbe sip essential-headers

To display a list of the essential SIP headers, use the **show sbc sbe sip essential-headers** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip essential-headers**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip essential-headers** command is used to display a list of all essential headers:

```
Router# show sbc mySbc sbe sip essential-headers
```

```
Essential headers:
AUTHORIZATION CALL-ID CONTACT CONTENT-LENGTH
CONTENT-TYPE CSEQ EVENT EXPIRES FROM MAX-FORWARDS
MIN-EXPIRES PROXY-AUTHORIZATION
PROXY-AUTHENTICATE PROXY-REQUIRE RACK
RECORD-ROUTE REFERRED-BY REFER-TO REPLACES
REQUIRE ROUTE RSEQ SUBSCRIPTION-STATE SUPPORTED
TO VIA WWW-AUTHENTICATE
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc sbe sip header-profile</b>	Displays a list of all configured SIP header profiles.



# show sbc sbe sip essential-methods

To display a list of the essential SIP methods, use the **show sbc sbe sip essential-methods** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip essential-methods**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip essential-methods** command is used to display a list of all essential methods:

```
Router# show sbc mySbc sbe sip essential-methods
```

```
Essential methods:
```

```
ACK BYE CANCEL INVITE NOTIFY PRACK REFER REGISTER  
SUBSCRIBE
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc sbe sip method-profiles</b>	Displays a list of all configured SIP method profiles.

# show sbc sbe sip essential-options

To show the options that are vital for base SBC operation, use the **show sbc sbe sip essential-options** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip essential-options**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	These options can not be configured on an option profile.	
-------------------------	---	--

<b>Examples</b>	The following example shows how the <b>show sbc sbe sip essential-options</b> command is used to display a list of all essential methods:	
-----------------	---	--

```
Router# show sbc test sbe sip essential-options
Essential options:
100REL
```

# show sbc sbe sip fast-register-stats

To show how many subscribers have been afforded fast register status by the application, use the **show sbc sbe sip fast-register-stats** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sip fast-register-stats
```

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	A register message in the context of this command is counted as a unique combination of the pair of address-of-record (AOR) and Contact-URI (CURI). Thus, a single REGISTER message from the subscriber, identified by an AOR with two contact URI will translate to a count of 2.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>show sbc sbe sip essential-options</b> command is used to display a list of all essential methods:
-----------------	---

```
Router# show sbc mysbc sbe sip fast-register-stats
SBC Service "mysbc"
```

```
SIP fast register statistics:
  Total entries:
```

```
15
```

# show sbc sbe sip header-editor

To display a summary of all the configured header editors or the details pertaining to a specific header editor, use the **show sbc sbe sip header-editor** command in the Privileged EXEC mode.

```
show sbc sbc-name sbe sip header-editor [editor-name]
```

Syntax Description	
<i>sbc-name</i>	Name of the SBC service.
<i>editor-name</i>	Name of the editor. Also, displays details about the specified editor.
	If omitted, information pertaining to all the SIP header editors is displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip header-editor** command is used to display the details of a specific header editor:

```
Router# show sbc test sbe sip header-editor Head1

header-editor "Head1"
  Description:
  Type:       Whitelist
  src-address: (inbound only)
    header-prio 1 header-name head1
  store-rules:
    entry 1
      description:
        Not specified
  request-line:
    entry 1
      description:
        action replace-value value "hell#hkk"
  headers:
    head1
      entry 1
        description:
          action pass
    head3
      entry 1
        description:
          action as-profile
          parameter-profile Param1
  Not in use with any adjacencies
  Not in use with any method-editor
```

The following example shows how the **show sbc sbe sip header-editor** command is used to display a list of all the configured header editors:

```
Router# show sbc mySbc sbe sip header-editor
```

```
header-editors for SBC service "mySbc"
```

Name	In use
=====	
Head1	No
head1	No
NoHelo	No
headedit	No
HeadEdit1	No
preset-call-tag	No
preset-acc-in-hdr	No
preset-std-in-hdr	No
preset-acc-out-hdr	No
preset-core-in-hdr	No
preset-std-out-hdr	No
preset-core-out-hdr	No
preset-ipsec-in-hdr	No
preset-ipsec-out-hdr	No
default	Yes
preset-ibcf-ext-in-hdr	No
preset-ibcf-int-in-hdr	No
preset-ibcf-utr-in-hdr	No
preset-ibcf-ext-out-hdr	No
preset-ibcf-int-out-hdr	No
preset-ibcf-utr-out-hdr	No
preset-std-block-in-hdr	No
preset-std-block-out-hdr	No

#### Related Commands

Command	Description
<b>sip header-editor</b>	Configures a header editor.

# show sbc sbe sip header-profile

To display all SIP header profiles or to show details for a specified header profile, use the **show sbc sbe sip header-profile** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip header-profile [*profile-name*]**

Syntax Description	
<i>sbc-name</i>	Specifies the name of the SBC service.
<b>profile-name</b>	Optional. Specifies the name of the profile and displays details about the specified profile.
	If omitted, the command shows information about all SIP header profiles.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	The <i>profile-name</i> argument was changed from required to optional. The ability to list all SIP header profiles was added.

**Examples** The following example shows how the **show sbc sbe sip header-profile** command is used to display details of the specified header profile:

```
Router# show sbc test sbe sip header-profile default

Header profile ''default''
Type: Whitelist
Headers:
HEADERS-A
HEADERS-B
HEADERS-C
Adjacency: sip-60 (out)
Adjacency: sip-61 (in)
```

The following example shows how the **show sbc sbe sip header-profile** command is used to display a list of all configured header profiles:

```
Router# show sbc mySbc sbe sip header-profile

Header profile for SBC service "mysbc"
Name                               In use
=====
profile1                            Yes
Default                              No
```

# show sbc sbe sip header-profiles

To display a list of all configured SIP header profiles, use the **show sbc sbe sip header-profiles** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip header-profiles**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	This command was deprecated. Its functionality was added to the <b>show sbc sbe sip header-profile</b> command.

**Examples** The following example shows how the **show sbc sbe sip header-profiles** command is used to display a list of all configured header profiles:

```
Router# show sbc mySbc sbe sip header-profiles
```

```
Header profile for SBC service "mysbc"
Name                               In use
=====
profile1                            Yes
Default                             No
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc sbe sip header-profile</b>	Displays details of the specified SIP header profile.

# show sbc sbe sip ip-fqdn-mapping

To display the IP-FQDN mapping table, use the **show sbc sbe sip ip-fqdn-mapping** command in the privileged EXEC mode.

**show sbc *sbc-name* sbe sip ip-fqdn-mapping**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	The output of this command was modified with IPv6 details.

**Examples** The following example shows the IP-FQDN mappings (IPv4) that are configured on SBEs:

```
Router# show sbc test sbe sip ip-fqdn-mapping

IP FQDN mappings for SBC service "test"

      Index Up?                               IP Dir FQDN
      1 Yes                                     11.22.33.41 <-> example.sbc1.com

* -> = one-way, <-> = both-ways
Router#
```

The “Up?” column in the output shows whether an entry is active or inactive. Inactive entries are often caused by mappings that clash with each other.

The following example shows the IP-FQDN mappings (IPv6) that are configured on SBEs:

```
Router# show sbc test sbe sip ip-fqdn-mapping

Router# show sbc test sbe sip ip-fqdn-mapping
IP FQDN mappings for SBC service "test"

      Index Up?                               IP Dir FQDN
      1 Yes                                     2001::10:0:50:137 -> ccm137.cisco.com

-> = one-way, <-> = both-ways
```



# show sbc sbe sip method-editor

To display all the SIP method editors or the details pertaining to a specific method editor, use the **show sbc sbe sip method-editor** command in the Privileged EXEC mode.

```
show sbc sbc-name sbe sip method-editor [editor-name]
```

Syntax Description	<i>sbc-name</i>	Name of the SBC service.
	<i>editor-name</i>	Name of the editor. Also, displays details about the specified editor.
		If omitted, information pertaining to all the SIP method editors is displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip method-editor** command is used to display a specific method editor:

```
Router# show sbc test sbe sip method-editor method2
method-editor "method2"
  Description:
  Type:      Whitelist
  Methods:
    No method-editor elements found.
    Not in use with any adjacencies
```

The following example shows how the **show sbc sbe sip method-editor** command is used to display a list of all the configured method editors:

```
Router# show sbc mySbc sbe sip method-editor
method-editors for SBC service "mySbc"
```

```

Name                               In use
=====
Hello1                              No
methodeditor                        No
preset-acc-in-mth                   No
preset-std-in-mth                    No
preset-acc-out-mth                   No
preset-core-in-mth                  No
preset-std-out-mth                   No
preset-core-out-mth                 No
preset-ipsec-in-mth                 No
preset-ipsec-out-mth                 No
default                             Yes
```

```
preset-ibcf-ext-in-mth      No
preset-ibcf-int-in-mth     No
preset-ibcf-utr-in-mth     No
preset-ibcf-ext-out-mth    No
preset-ibcf-int-out-mth    No
preset-ibcf-utr-out-mth    No
preset-std-block-in-mth    No
preset-std-block-out-mth   No
```

---

**Related Commands**

---

<b>Command</b>	<b>Description</b>
<b>sip method-editor</b>	Configures a method editor.

---

# show sbc sbe sip method-profile

To display all SIP method profiles or to show details for a specified method profile, use the **show sbc sbe sip method-profile** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sip method-profile [prof-name]
```

## Syntax Description

<b><i>sbc-name</i></b>	<b>Specifies the name of the SBC service.</b>
<b><i>prof-name</i></b>	Optional. Name of profile. If omitted, the command shows information about all profiles.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	The <i>prof-name</i> argument was changed from required to optional. The ability to list all SIP method profiles was added.

## Examples

The following example shows how the **show sbc sbe sip method-profile** command is used to display a specific method profile:

```
Router# show sbc test sbe sip method-profile method2

Method profile 'method2'
Type: Whitelist
Methods:
meth1
meth2
Adjacency: sip-60 (in)
Adjacency: sip-61 (out)
```

The following example shows how the **show sbc sbe sip method-profile** command is used to display a list of all configured method profiles:

```
Router# show sbc mySbc sbe sip method-profile
Method profile for SBC service "mysbc"
Name                               In use
=====
profile1                            No
Default                              Yes
```

# show sbc sbe sip method-profiles

This command was deprecated in Cisco IOS XE Release 2.5.

To display a list of all SIP method profiles, use the **show sbc sbe sip method-profiles** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip method-profiles**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

<b>Command Default</b>	No default behavior or values are available.	
------------------------	--	--

<b>Command Modes</b>	Privileged EXEC (#)	
----------------------	---------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	This command was deprecated. Its functionality was added to the <b>show sbc sbe sip method-profile</b> command.

**Examples** The following example shows how the **show sbc sbe sip method-profiles** command is used to display a list of all configured method profiles:

```
Router# show sbc mySbc sbe sip method-profiles
Method profile for SBC service "mysbc"
Name                               In use
=====
profile1                            No
Default                             Yes
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc sbe sip method-profile</b>	Displays details of the specified SIP method profile.

# show sbc sbe sip method-stats

To show the summary or detailed statistics for a SIP method, use the **show sbc sbe sip method-stats** command in Privileged EXEC mode.



## Note

This command name was changed slightly in Cisco IOS XE Release 2.5.

*show sbc sbc-name sbe sip method-stats adj-name sip-req-name sip-response-code summery-period*

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
<i>adj-name</i>	Specifies the name of the adjacency.
<i>sip-req-name</i>	Specifies the request name: ACK BYE CANCEL INFO INVITE MESSAGE NOTIFY OPTIONS PRACK REFER REGISTER SUBSCRIBE UNKNOWN UPDATE
<i>sip-response-code</i>	100-999
<i>summery-period</i>	Values you can enter are <i>current5mins</i> , <i>current15mins</i> , <i>currenthour</i> , <i>currentday</i> , <i>previous5mins</i> , <i>previous15mins</i> , <i>previoushour</i> , or <i>previousday</i> .

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command name was changed from <b>show sbc sbe sip-method-stats</b> to <b>show sbc sbe sip method-stats</b> (the hyphen between sip and method was removed). This command is obsolete in Cisco IOS XE Release 2.5

## Usage Guidelines

The **statistics-setting** command must be configured before using the **show sbc sbe sip method-stats** command to display SIP method statistics.

- Use the **statistics-setting summary** command to allow the **show sbc sbe sip method-stats** command to display statistics about SIP request names only.
- Use the **statistics-setting detail** command to allow the **show sbc sbe sip method-stats** command to display statistics about SIP response codes and SIP request names.

Summary statistics display all the response codes sent and received for a specific SIP method.

Detailed statistics display the statistics for specific SIP method and response code. You must use the *sip-response-code* string to view detailed statistics.

**Examples**

The following example shows how the **show sbc sbe sip method-stats** command is used to display summary statistics for a specific SIP method. The **statistics-setting summary** command was configured on the adjacency before executing the **show sbc sbe sip method-stats** command.

```
Router# show sbc sbc sbe sip method-stats sip-41 invite currenthour
SBC Service "sbc"
Adjacency sip-41 (SIP)
Statistics for SIP method INVITE
Total request received      :3
Total request sent         :0
Total 1xx response received :0
Total 1xx response sent    :3
Total 2xx response received :0
Total 2xx response sent    :0
Total 3xx response received :0
Total 3xx response sent    :0
Total 4xx response received :0
Total 4xx response sent    :0
Total 5xx response received :0
Total 5xx response sent    :0
Total 6xx response received :0
Total 6xx response sent    :3
Other response received    :0
Other response sent        :0
```

The following example shows how the **show sbc sbe sip method-stats** command is used to display detailed statistics for a specific SIP method. The **statistics-setting detail** command was configured on the adjacency before executing the **show sbc sbe sip method-stats** command.

```
Router# show sbc sbc sbe sip method-stats sip-41 invite 604 currenthour
SBC Service "sbc"
Adjacency sip-41 (SIP)
Statistics for SIP method INVITE ,response 604
Response received: 0
Response sent      : 3
```

The following example shows that the **statistics-setting detail** command was not configured on the adjacency before executing the **show sbc sbe sip method-stats** command:

```
Router# show sbc sbc sbe sip method-stats sip-41 invite 604 currenthour
Statistics not available.
Set adjacency statistics-setting to detail to enable detailed statistics
```

**Related Commands**

Command	Description
<b>clear sbc sbe adjacency statistics</b>	Clears the SIP method statistics counters and resets them to zero.
<b>show sbc sbe adjacencies</b>	Lists the adjacencies configured on signaling border elements (SBEs).
<b>show sbc sbe sip option-profiles</b>	Displays a list of all configured SIP option profiles.
<b>statistics-setting</b>	Configures an adjacency to support SIP method statistics.

# show sbc sbe sip option-editor

To display all the SIP option editors or the details pertaining to a specific option editor, use the **show sbc sbe sip option-editor** command in the Privileged EXEC mode.

```
show sbc sbc-name sbe sip option-editor [editor-name]
```

Syntax Description	<i>sbc-name</i>	Name of the SBC service.
	<i>editor-name</i>	Name of the editor. Also, displays details about the specified editor.
		If omitted, information pertaining to all the SIP option editors is displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip option-editor** command is used to display the details of a specific option editor:

```
Router# show sbc test sbe sip option-editor editor1

option-editor "editor1"
  Description:
  Type:      Whitelist
  Options:
    No option editor elements found.
    Not in use with any adjacencies
```

The following example shows how the **show sbc sbe sip option-editor** command is used to display a list of all the configured option editors:

```
Router# show sbc test sbe sip option-editor

option editors for SBC service "test"
  Name                               In use
  =====
  TheHello                           No
  preset-acc-in-opt                   No
  preset-std-in-opt                   No
  preset-acc-out-opt                  No
  preset-core-in-opt                  No
  preset-std-out-opt                   No
  preset-core-out-opt                 No
  preset-ipsec-in-opt                 No
  preset-ipsec-out-opt                No
  default                             Yes
```

```
preset-ibcf-ext-in-opt      No
preset-ibcf-int-in-opt     No
preset-ibcf-utr-in-opt     No
preset-ibcf-ext-out-opt    No
preset-ibcf-int-out-opt    No
preset-ibcf-utr-out-opt    No
preset-std-block-in-opt    No
preset-std-block-out-opt   No
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip option-editor</b>	Configures an option editor.



# show sbc sbe sip option-profile

To display all SIP option profiles or to show details for a specified option profile, use the **show sbc sbe sip option-profile** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sip option-profile [profile-name]
```

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
<i>profile-name</i>	Optional. Specifies the name of the profile. If omitted, the command shows information about all SIP option profiles.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	The <i>profile-name</i> argument was changed from required to optional. The ability to list all SIP option profiles was added.

## Examples

The following example shows how the **show sbc sbe sip option-profile** command is used to display details of the specified option profile:

```
Router# show sbc test sbe sip option-profile profile1
```

```
Option profile 'profile1'
Type: Whitelist
Options:
opt1
Adjacency: sip-60 (in-px)
```

```
Router# show sbc test sbe sip option-profile profile2
```

```
Option profile 'profile2'
Type: Whitelist
Options:
opt1
opt2
Not in use with any adjacencies
```

The following example shows how the **show sbc sbe sip option-profile** command is used to display details of the specified header profile:

```
Router# show sbc test sbe sip option-profile
```

```
Option profiles for SBC service "test":
```

```
      Name                Description                In use
```

```
=====
default          Default profile      Yes
OP1              Option profile 1    Yes
OP2              Option profile 2    Yes
OPTest           Unused profile       No
```

# show sbc sbe sip option-profiles

This command was deprecated in Cisco IOS XE Release 2.5.

To display a summary of the configured option profiles, use the **show sbc sbe sip option-profiles** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sip option-profiles
```

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
<i>profile-name</i>	Specifies the name of the profile.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command was deprecated. Its functionality was added to the <b>show sbc sbe sip option-profile</b> command.

## Examples

The following example shows how the **show sbc sbe sip option-profiles** command is used to display details of the specified header profile:

```
Router# show sbc test sbe sip option-profiles
```

```
Option profiles for SBC service "test":
```

Name	Description	In use
default	Default profile	Yes
OP1	Option profile 1	Yes
OP2	Option profile 2	Yes
OPTest	Unused profile	No

## Related Commands

Command	Description
<b>show sbc sbe sip option-profile</b>	Displays a specified option profile.

# show sbc sbe sip parameter-editor

To display all the SIP parameter editors or the details pertaining to a specific parameter editor, use the **show sbc sbe sip parameter-editor** command in the Privileged EXEC mode.

**show sbc *sbc-name* sbe sip parameter-editor** [*editor-name*]

Syntax Description	
<i>sbc-name</i>	Name of the SBC service.
<i>editor-name</i>	Name of the editor. Also, displays details about the specified editor. If omitted, information pertaining to all the SIP parameter editors is displayed.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip parameter-editor** command is used to display the details of a specific parameter editor:

```
Router# show sbc test sbe sip parameter-editor Parameter1
parameter-editor "Parameter1"
  Description:
  Parameters:
    No parameters found.
  In use by header-editor:Head1, header:head3, entry:1
```

The following example shows how the **show sbc sbe sip parameter-editor** command is used to display a list of all the configured parameter editors:

```
Router# show sbc test sbe sip parameter-editor
parameter-editors for SBC service "sbc"

Name                               In use
=====
Param1                             Yes
param2                             No
DoneHello                          No
```

Related Commands	Command	Description
	<b>sip parameter-editor</b>	Configures a parameter editor.

# show sbc sbe sip sdp-match-table

To show the SDP match table configured on the SBC, use the **show sbc sbe sip sdp-match-table** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip sdp-match-table [detail]**

## Syntax Description

<i>sbc-name</i>	Specifies the name of the SBC service.
detail	Shows the SDP attribute configured on a given SDP match table.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how the **show sbc sbe sip sdp-match-table** command is used to display SDP match table:

```
Router# show sbc pgw sbe sip sdp-match-table detail
  Name      : m                <--- table name
  Action    : blacklist       <--- action: blacklist or whitelist
  Match String : ddd          <--- several match string
                ddf

-----
  Name      : n
  Action    : whitelist
  Match String : 2
                3
                4
```

## Related Commands

Command	Description
<b>show sbc sbe sdp-h245-mapping</b>	Displays the mapping for codec strings between SDP (SIP) and H245 (H323).

# show sbc sbe sip sdp-media-profile

To show all SDP media profiles in an SBC service or details for a specified profile, use the **show sbc sbe sip sdp-media-profile** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sip sdp-media-profile [profile-name]
```

Syntax Description	Parameter	Description
	<i>sbc-name</i>	Specifies the name of the SBC service.
	<i>profile-name</i>	Specifies the name of the profile. If omitted, the command lists all profiles in the SBC service.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows a list of SDP media profiles configured under an SBC:

```
Router# show sbc test sbe sip sdp-media-profile
SDP Media profiles for SBC service "test"

Name                               In use
=====
Mediaprofile                       No
```

The following example shows the contents of a named SDP media profile:

```
Router# show sbc test sbe sip sdp-media-profile Mediaprofile
SDP media profile "Mediaprofile"
Elements:
  Sequence Number : 1
    Line 1         : m=audio 0 RTP/AVP 31
    Line 2         : a=aaa:testing

Not in use by any CAC table entries
```

Related Commands	Command	Description
	<b>sdp-media-profile</b>	Creates or modifies a customized SDP media profile.

# show sbc sbe sip sdp-policy-table

To show the SDP policy table configured on the SBC, use the **show sbc sbe sip sdp-policy-table** command in Privileged EXEC mode.

**show sbc *sbc-name* sbe sip sdp-policy-table**

<b>Syntax Description</b>	<i>sbc-name</i>	Specifies the name of the SBC service.
---------------------------	-----------------	--

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip sdp-policy-table** command is used to display the SDP policy table:

```
Router# show sbc pgw sbe sip sdp-policy-table
      Name                               SDP Match Table
-----
      p                                   m          <--- "m" is sdp match table name
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc sbe sip sdp-match-table</b>	Shows the SDP match table configured on the SBC.

# show sbc sbe sip statistics

To display the aggregated SIP statistics handled by the Cisco Unified Border Element (SP Edition) process on the Cisco ASR 1000 Series Routers, use the **show sbc sbe sip statistics** command in Privileged EXEC mode.

```
show sbc service-name sbe sip statistics [ global | adjacency adj-name method sip-req-name ]
sip-response-code period
```

## Syntax Description

<i>service-name</i>	Specifies the name of the Session Border Controller (SBC) service.
<i>adj-name</i>	Specifies the name of the adjacency.
<i>sip-req-name</i>	Specifies the request name: ACK BYE CANCEL INFO INVITE MESSAGE NOTIFY OPTIONS PRACK REFER REGISTER SUBSCRIBE UNKNOWN UPDATE
<i>sip-response-code</i>	0-999
<i>period</i>	Specifies the interval when the statistics display. The possible values are: current5mins, current15mins, currenthour, currentday, previous5mins, previous15mins, previoushour, or previousday.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	Added new parameters to show the summary or detailed statistics for a SIP method.

## Usage Guidelines

The **statistics-setting** command must be configured before using the **show sbc sbe sip statistics** command to display SIP method statistics.

- Use the **statistics-setting summary** command to allow the **show sbc sbe sip statistics** command to display statistics about SIP request names only.
- Use the **statistics-setting detail** command to allow the **show sbc sbe sip statistics** command to display statistics about SIP response codes and SIP request names.

Summary statistics display all the response codes sent and received for a specific SIP method.

Detailed statistics display the statistics for specific SIP method and response code. You must use the *sip-response-code* string to view detailed statistics.



**Examples**

The following example shows the aggregated SIP statistics handled by the Cisco Unified Border Element (SP Edition) process on the Cisco ASR 1000 Series Routers:

```
Router# show sbc global sbe sip statistics

SIP Statistics
-----
Total SIP Transactions: 6

                In          Out
-----
Total SIP Requests      4          4
Total SIP Responses     3          5

SIP Request Messages:
SIP INVITES             2          2
SIP ACKs                1          1
SIP BYEs                1          1
SIP CANCELs            0          0
SIP OPTIONS             0          0
SIP REGISTERs          0          0
SIP SUBSCRIBEs         0          0
SIP REFERs             0          0
SIP NOTIFY             0          0

SIP Response Classes:
SIP Info                (1xx)      1          3
SIP Success              (2xx)      2          2
SIP Redirects           (3xx)      0          0
SIP Client Errors       (4xx)      0          0
SIP Server Errors       (5xx)      0          0
SIP Global Errors       (6xx)      0          0

Internally Generated SIP Response Classes:
SIP Info                (1xx)      0
SIP Success              (2xx)      0
SIP Redirects           (3xx)      0
SIP Client Errors       (4xx)      0
SIP Server Errors       (5xx)      0
SIP Global Errors       (6xx)      0

Transaction Manager (TM) Internal Statistics:
Request/Response Congestion Failures = 0
Current Transactions awaiting response = 0
Free Buffers in TM inbound pool = 1200
Free Buffers in TM outbound pool = 20000
TM Congestion Level (uncongested = 0) = 0
Congestion Queue - Packets Accepted = 0
Congestion Queue - Packets Rejected = 0
Congestion Queue - Length = 0
Congestion Queue - Time Since Reset(ms)= 904270
Congestion Queue - Oldest Pkt Age (ms) = 0
Congestion Queue - Max Pkt Delay (ms) = 0

Control Block (CB) utilization:
Server Location NAPTR CBs = 0
Server Location SRV CBs = 0
Server Location address CBs = 2
Server Location Cache CBs = 0
Server Location Alias CBs = 0
Call CBs = 0
UA Dialog CBs = 0
UA INVITE Dialog CBs = 0
UA Subscription CBs = 0
```

```

Proxy Forking CBs                = 0
Proxy Dialog CBs                 = 0
Proxy Proto Dialog CBs           = 0
Proxy Server Transaction CBs     = 0
Proxy Client Transaction CBs     = 0
Transaction CBs                  = 0
Response CBs                     = 0
Extension Method CBs             = 0
Status Code CBs                  = 0
    
```

Table 6 describes the important fields shown in the output of the command.

**Table 6** *show sbc sbe sip statistics Field Descriptions*

Field	Description
In	Counts of messages that have been received by the endpoints. These are messages received in the SBC by the Cisco IOS task running on the route processor.
Out	Counts of messages sent out of the SBC. The message count is an aggregation of the messages internally generated and generated in response to an external event.
SIP Request Messages	In and Out message counts of the Request classes for the SIP messages. Request classes are: SIP INVITES, SIP ACKs, SIP BYEs, SIP CANCELs, SIP OPTIONS, SIP REGISTERs, SIP SUBSCRIBEs, SIP REFERs, and SIP NOTIFY.
SIP Response Classes	In and Out message counts of the Response classes for the SIP messages. Response classes are: SIP Info, SIP Success, SIP Redirects, SIP Client Errors, SIP Server Errors, and SIP Global Errors.
Internally Generated SIP Response Classes	In and Out message counts generated by the SBC due to a decision that is outside the normal call flow.
Transaction Manager (TM) Internal Statistics	Describes statistics of the state of the dynamic message handling.
Control Block (CB) utilization	Count of the memory usage of the control blocks.

**Related Commands**

Command	Description
<b>clear sbc sbe sip statistics</b>	Clears aggregated SIP statistics handled by the Cisco Unified Border Element (SP Edition).

# show sbc sbe sip subscribers

To display details of all SIP endpoints that have registered with the SBC, use the **show sbc sbe sip subscribers** command in Privileged EXEC mode.

```
show sbc sbc-name sbe sip subscribers [filter prefix] [adjacency adj-name] [delegate]
```

Syntax Description		
<i>sbc-name</i>		Specifies the name of the SBC service.
<i>filter prefix</i>		Match only subscribers whose address-of-record starts with the specified prefix.
<b>adjacency adj-name</b>		Match only subscribers registered on this adjacency.
<i>delegate</i>		Display subscribers that have provisioned delegate registration configured, and the associated Uniform Resource Identifier (URI) contact information for the subscribers.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how the **show sbc sbe sip subscribers** command is used to display details of the SIP endpoints that have registered with the SBC:

```
Router# show sbc node2 sbe sip subscribers

SBC Service ''node2''
SIP subscribers:

AOR: sip:4082230000@amd-ua3.amd.com
Subscriber location: sip:4082230000@103.2.192.1:5060;transport=UDP
SIP URI : sip:4082230000@102.102.102.45:5060
Subscriber adj: amd-ua3
Registrar adj: slt-csps4
Time left: 59 mins

AOR: sip:4082220000@amd-ua2.amd.com
Subscriber location: sip:4082220000@103.2.128.1:5060;transport=UDP
SIP URI : sip:4082220000@102.102.102.45:5060
Subscriber adj: amd-ua2
Registrar adj: slt-csps3
Time left: 59 mins
```

The following show example displays subscribers for which delegate registration have been configured. The **delegate** keyword displays the associated URI contact information for subscribers.

Router# **show sbc mySBC sbe sip subscribers delegate**

          0          1          2          3          4          5          6          7  
012345789012345789012345789012345789012345789012345789012345789

AOR:                          sip:steve1.cisco.com  
Subscriber Location[s]:  sip:contact@cisco.com -> CallMgrC  
                          sip:contact2@cisco.com -> CallMgrD  
Registrar adj:              CallMgrA  
Registrar:                  sip:myreg@172.18.52.148  
Register Duration:          1800  
Register Retries:           3  
Retry Interval:             30  
Refresh Buffer:              30  
Time left:                  0 days

# show sbc sbe sip timers

To show the current configuration of SIP-related timers, use the **show sbc sbe sip timers** command in Privileged EXEC mode.

**show sbc** *service-name* **sbe sip timers**

<b>Syntax Description</b>	<i>service-name</i>	Specifies the name of the SBC.
<b>Command Default</b>	No default behavior or values are available.	
<b>Command Modes</b>	Privileged EXEC (#)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to list the configurations of SIP-related timers:

```
Router# show sbc test sbe sip timers

SBC Service 'test'

IP timer configuration:
TCP connect timeout: 0 ms
TCP idle timeout: 120000 ms
TLS idle timeout: 3600000 ms
INVITE timeout: 180 s
UDP first retransmit interval: 500 ms
UDP max retransmit interval: 4000 ms
UDP response linger period: 5000 ms
```

# show sbc sbe stream-list

To list the stream lists on the signaling border element (SBE), use the **show sbc sbe stream-list** command in Privileged EXEC configuration mode.

**show sbc** *service-name* **sbe stream-list** [*stream-list-name* **detail**]

Syntax Description	
<i>service-name</i>	The name of the SBC.
<i>stream-list-name</i>	The name of the stream list.
<b>detail</b>	Displays detailed configuration information about a stream list.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode.

**Examples** The following example shows how to display the stream lists on the SBE:

```
Router# show sbc mysbc sbe stream-list my-stream
SBC Service "sbc"

Stream list: my-stream
  Description This is my first stream list
  Media-type application Transport udp protocol BFCP
  Media-type message Transport udp protocol Streambased
```

Related Commands	Command	Description
	<b>generic-stream</b>	Configures the media type for a generic stream.
	<b>media-type</b>	
	<b>stream-list</b>	Configures a stream list.

# show sbc sbe subscriber-stats

To display the statistics pertaining to the subscribers registered on an SBC, use the **show sbc sbe subscriber-stats** command in the privileged EXEC mode.

```
show sbc sbc-name sbe subscriber-stats {all | dst-account name | dst-adjacency name | global |
src-account name | src-adjacency name | } [current15mins | current5mins | currentday |
currenthour | currentindefinite | previous15mins | previous5mins | previousday |
previoushour]
```

Syntax Description	
<i>sbc-name</i>	Name of the SBC service.
name	Name of the adjacency or account for which you want the statistics to be displayed.
all	Displays the global statistics and the subscriber statistics on each source adjacency, destination adjacency, source account, and destination account on the SBC.
dst-account	Displays statistics for the specified destination account.
dst-adjacency	Displays statistics for the specified destination adjacency.
global	Displays globally scoped statistics for the entire SBC.
src-adjacency	Displays statistics for the specified source adjacency.
src-account	Displays statistics for the specified source account.
current15mins	Displays the statistics pertaining to the current 5-minute interval and the two 5-minute intervals prior to this.
current5mins	Displays the statistics pertaining to the current 5-minute interval.
currentday	Displays the statistics pertaining to the current 5-minute interval and the two hundred eighty seven 5-minute intervals prior to this.
currenthour	Displays the statistics pertaining to the current 5-minute interval and the eleven 5-minute intervals prior to this.
currentindefinite	Displays the statistics pertaining to the period since the last explicit reset.
previous15mins	Displays the statistics pertaining to the previous 5-minute interval and the two 5-minute intervals prior to this.
previous5mins	Displays the statistics pertaining to the 5-minute interval prior to this.
previousday	Displays the statistics pertaining to the previous 5-minute interval and the two hundred eighty seven 5-minute intervals prior to this.
previoushour	Displays the statistics pertaining to the previous 5-minute interval and the eleven 5-minute intervals prior to this.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

**Command History**

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Router.

**Usage Guidelines**

The statistics are collected at 5-minute intervals past the hour, that is, 0, 5, 10, 15, and so on. The system maintains a bucket for each of the over 5-minutes counts. Each bucket is started at 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, and 55-minutes past the hour according to the system clock. The **show sbc sbe call-stats** command then combines a number of these buckets and displays the sum of these buckets.

For example, if the current time is 12:34, *currenthour* will apply to the statistics collected since 11:35, and *current15mins* will apply to the statistics collected since 12:20. In this example, *previoushour* would be 10:35 to 11:35, and *previous15mins* would be 12:05 to 12:20.



**Note**

Call statistics for rejection of calls based on the memory threshold is not tracked based on time intervals.

**Examples**

The following example shows how to display all the subscriber statistics for the current day:

```
Router# show sbc mySbc sbe subscriber-stats all currentday
```

```
Subscribe count totals:
```

```
Active subscribers           = 10
```

```
Subscriber high water mark  = 15
```

```
Subscriber low water mark   = 3
```

```
Stats Reset Timestamp:
```

```
Timestamp when stats for this summary period were reset = 2011/01/25 23:26:03
```

[Table 7](#) describes the important fields shown in the output of the command.

**Table 7** show sbc sbe subscriber-stats Field Descriptions

Field	Description
Active subscribers	Number of subscribers who are currently active.
Subscriber high water mark	Highest number of subscribers who are active at any given point in time during the period specified in the command.
Subscriber low water mark	Lowest number of subscribers who are active at any given point in time during the period specified in the command.

**Related Commands**

Command	Description
<b>clear sbc sbe call-stats</b>	Clears the call statistics on the SBE.
<b>reject-threshold</b>	Configures the memory threshold and reject rate for new calls.
<b>sbc mysbc sbe call-stats</b>	Lists all the calls on the SBE.



<b>Command</b>	<b>Description</b>
<b>show sbc mysbc sbe call-rate-stats</b>	Lists the call rate on the SBE.
<b>show sbc mysbc sbe sip subscribers</b>	Lists details of the subscribers on the SBE.

# show sbc sbe transcoding-stats

To display the voice transcoding-related statistics pertaining to the Session Border Controller (SBC), use the **show sbc sbe transcoding-stats** command in the Privileged EXEC mode.

```
show sbc sbc-name sbe transcoding-stats {adjacency adjacency-name | global} {current15mins
| current5mins | currentday | currenthour | currentindefinite | previous15mins |
previous5mins | previousday | previoushour}
```

## Syntax Description

<i>sbc-name</i>	Name of the SBC service.
<b>adjacency</b>	Displays the transcoding-related statistics pertaining to the specified adjacency.
<i>adjacency-name</i>	Name of the specified adjacency.
<b>global</b>	Displays globally scoped statistics for the SBC.
<b>current15mins</b>	Displays statistics pertaining to the current 15-minute interval.
<b>current5mins</b>	Displays statistics pertaining to the current 5-minute interval.
<b>currentday</b>	Displays statistics pertaining to the current day, from midnight.
<b>currenthour</b>	Displays statistics pertaining to the current hour.
<b>currentindefinite</b>	Displays statistics pertaining to the period since the last explicit reset.
<b>previous15mins</b>	Displays statistics pertaining to the previous 15-minute interval.
<b>previous5mins</b>	Displays statistics pertaining to the previous 5-minute interval.
<b>previousday</b>	Displays statistics pertaining to the previous day.
<b>previoushour</b>	Displays statistics pertaining to the previous hour.

## Command Default

No default behavior or values are available.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode.

## Examples

The following example shows how to display the voice transcoding-related statistics pertaining to the SIPPI adjacency for the current 15-minute interval:

```
Router# show sbc mySBC sbe transcoding-stats adjacency SIPPI current15mins

Codec1  Codec2  Transcoded Stream  HWM of TranscodedStream  Last Reset
G711A   G711U      4                   10                         2010/09/10 19:27:15
```

Table 8 describes the significant fields shown in the display.

**Table 8** *show sbc sbe transcoding-stats Field Descriptions*

Field	Description
Codec1 and Codec 2	The combination of codecs between which the active calls are transcoded.
Transcoded Stream	The number of active calls being transcoded.
HWM of TranscodedStream	The high water mark (HWM) of the transcoded stream.
Last Reset	Information about when the HWM was last reset.

#### Related Commands

Command	Description
<b>clear sbc sbe transcoding-stats</b>	Clears the voice transcoding-related statistics.

# show sbc services

To display lists all of the SBC services on the chassis, use the **show sbc services** command in Privileged EXEC mode.

**show sbc services**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Lists the high-level status and capabilities of each instantiated SBE or DBE.

**Examples** The following example shows how the **show sbc services** command is used to display lists of all the SBC services on the chassis.

```
Router# show sbc mysbc services

SBC Service "mySbc"
SBE capabilities
SIP Signaling
H.323 Signaling
H.248 media gateway control (MGC)

DBE capabilities
```

# signaling-address

To define the local signaling address of an H.323 or SIP adjacency, use the **signaling-address** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
signaling-address {ipv4 ipv4_IP_address | ipv6 ipv6_IP_address}
```

```
no signaling-address
```

## Syntax Description

<i>ipv4_IP_address</i>	Specifies the IPv4 address for the signaling address of the SIP or H.323 adjacency.
<i>ipv6_IP_address</i>	Specifies the IPv6 address for the signaling address of the SIP adjacency.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)—for IPv4 IP addresses only.  
Adjacency SIP configuration (config-sbc-sbe-adj-sip)—for IPv4 and IPv6 IP addresses.

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.6	Introduced IPv6 keyword.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

When defined, the SBE listens on this address for inbound call signaling from the adjacency. If two adjacencies share the same signaling address, a different remote domain name must be specified for each one.

## Examples

The following example shows how to configure the H.323 adjacency h323ToIsp42 to listen on IPv4 signaling address 10.1.0.2:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# signaling-address ipv4 10.1.0.2
```

The following example shows how to configure the SIP adjacency adjSip1 to listen on IPv4 signaling address 10.10.10.10:

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# adjacency sip adjSip1  
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.10.10.10
```

The following example shows how to configure the SIP adjacency adjSip1 to listen on IPv6 signaling address 2001:A401::33:33:36:1:

```
Router# configure terminal  
Router(config)# sbc mySbc  
Router(config-sbc)# sbe  
Router(config-sbc-sbe)# adjacency sip adjSip1  
Router(config-sbc-sbe-adj-sip)# signaling-address ipv6 2001:A401::33:33:36:1
```

# signaling-peer-port

To configure an H.323 or SIP adjacency to use the given remote signaling-peer's port, use the **signaling-peer-port** command in the appropriate configuration mode. To remove this configuration, use the **no** form of this command.

**signaling-peer-port** *port-num*

**no signaling-peer-port**

<b>Syntax Description</b>	<i>port-num</i>	Specifies the number of the signaling port. Range is 1 to 65535.
---------------------------	-----------------	--

<b>Command Default</b>	By default, this command assumes that <i>port-num</i> is 5060.
------------------------	--

<b>Command Modes</b>	Adjacency H.323 configuration (config-sbc-sbe-adj-h323) Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure the H.323 adjacency h323ToIsp42 to use port 123 on the signaling peer:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# signaling-peer-port 123
```

The following example shows how to configure the SIP adjacency SipToIsp42 to port 123 as the signaling peer's port:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# signaling-peer-port 123
```

# signaling-peer-priority

To configure the priority of a signaling peer in a Session Initiation Protocol (SIP) adjacency, use the **signaling-peer-priority** command in adjacency SIP configuration mode. To deconfigure the priority, use the **no** form of this command.

**signaling-peer-priority** *priority*

**no signaling-peer-priority** *priority*

<b>Syntax Description</b>	<i>priority</i>	The priority of a signaling peer. The range is from 1 to 6.
---------------------------	-----------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.



**Note**

The main peer address in an adjacency share the same priority values, ranging from 1 to 6, with the redundant peer addresses.

**Examples** The following example shows how the **signaling-peer-priority** command is used to configure the priority of a signaling peer on a SIP adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# signaling-peer-priority 6
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>redundant peer</b>	Configures an alternative signaling peer for an adjacency.



<b>Command</b>	<b>Description</b>
<b>force-signaling-peer</b>	Forces SIP messages to go to a configured signaling peer.
<b>signaling-peer-switch</b>	Configures a SIP adjacency to switch a signaling peer to an available destination.

# signaling-peer-switch

To configure a method for Session Initiation Protocol (SIP) adjacency, enabling it to switch a signaling peer to an available destination, use the **signaling-peer-switch** command in adjacency SIP configuration mode. To deconfigure a signaling peer from switching to an available destination, use the **no** form of this command.

**signaling-peer-switch** { **always** | **on-fail** }

**no signaling-peer-switch** { **always** | **on-fail** }

## Syntax Description

always	Switches to a new destination with highest priority.
on-fail	Switches to a new destination when a current peer failure occurs.

## Command Default

By default, the **always** keyword is enabled.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

## Examples

The following example shows how the **signaling-peer-switch** command is used to configure a method for SIP adjacency, enabling it to switch the signaling peer to a destination having the highest priority:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-adj-sip)# signaling-peer-switch always
```

## Related Commands

Command	Description
<b>force-signaling-peer</b>	Forces SIP messages to go to a configured signaling peer.
<b>redundant peer</b>	Configures an alternative signaling peer for an adjacency.
<b>signaling-peer-priority</b>	Configures the priority of a signaling peer in a SIP adjacency.

# signaling-peer

To configure an H.323 or SIP adjacency to use the given remote signaling-peer, use the **signaling-peer** command in the **appropriate configuration** mode. To remove this configuration, use the **no** form of this command.

**signaling-peer gk** *peer-name*

**no signaling-peer**

## Syntax Description

<i>peer-name</i>	Specifies the IPv4 address in dotted decimal format.
<b>gk</b>	Specifies the H.323 gatekeeper.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the H.323 adjacency h323ToIsp42 to use gatekeeper andrew:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# signaling-peer gk andrew
```



### Note

You can use the **signaling-peer** command to configure the SIP adjacency using the IP address or the host name of the given remote signaling-peer.

The following example shows how to configure SIP adjacency using the IP address of the given remote signaling-peer:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
```

```
Router(config-sbc-sbe)# adjacency sip adjSip1
Router(config-sbc-sbe-adj-sip)# signaling-peer 10.1.2.3
```

The following example shows how to configure SIP adjacency using the hostname of the given remote signaling-peer:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# signaling-peer athene
```

---

**Related Commands**

Command	Description
<b>signaling-peer-port</b>	Configures an H.323 or SIP adjacency to use the given remote signaling-peer's port.

# signaling-port

To define the local port of signaling address of an H.323 or SIP adjacency, use the **signaling-port** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

**signaling-port** *port-num* [*max-port-num*]

**no signaling-port**

## Syntax Description

<i>port-num</i>	Required for both H.323 and SIP adjacencies. Specifies the number of the signaling peer. Range is 1 to 65535.
<i>max-port-num</i>	Optional for SIP adjacencies. Specifies the maximum port number of the range (the upper boundary of the range) of local listen ports for the adjacency. Range is from 1 through 65535.  Configure both <i>port-num</i> and <i>max-port-num</i> if you want a range of local listen ports for a SIP adjacency.  <i>max-port-num</i> should not be specified if this is an IPsec-enabled adjacency.

## Command Default

*port-num* is 5060.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	The <i>max-port-num</i> argument was added for SIP adjacencies.

## Usage Guidelines

The SBE will listen on this port for inbound call signaling from the adjacency. The port will also be appended to the SBE's contact header on outbound SIP requests and responses.

If both *port-num* and *max-port-num* are specified, then the *port-num* indicates the lower boundary of the range and *max-port-num* indicates the upper boundary of the range. If no *max-port-num* is specified, then the adjacency listens only on the single *port-num*. *Max-port-num* only needs to be set if a range of local listen ports is required for this adjacency.

For the Contact Username Passthrough feature for non-IMS networks—the **signaling-port** command configures a range of valid signaling ports (on the same registrar-facing SIP adjacency where the **registration contact username passthrough** command was configured) to allow the SBC to disambiguate subscribers that register from different devices with the same username.

The *port-num* and *max-port-num* cannot be changed while the adjacency is active.

The number of ports in the range (*max-port-num* – *port-num* + 1) must be less than or equal to 10. Also *max-num-port* should not be specified if this is an IPsec-enabled adjacency.

**Examples**

The following example shows how to configure the SIP adjacency SipToIsp42 to listen on signaling port 5000:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbc-sbe-adj-sip)# signaling-port 5000
```

The following is an example showing that a signaling port range of 5060 to 5062 (3 local ports) is configured for a SIP adjacency where registration contact username passthrough is configured:

```
adjacency sip SIPPlReg
  group SIPPlReg
  inherit profile preset-core
  signaling-address ipv4 192.168.101.1
  statistics-setting summary
  signaling-port 5060 5062
  remote-address ipv4 192.168.101.12 255.255.255.255
  signaling-peer 192.168.101.12
  signaling-peer-port 7068
  registration target address 192.168.101.12
  registration target port 7069
  registration contact username passthrough
attach
```

**Related Commands**

Command	Description
signaling-address ipv4	Configures a SIP adjacency to use the given remote signaling-peer.
registration contact username	Specifies if the contact username in a SIP REGISTER request is passed through unchanged

# sip-contact

To configure the SIP contact information for a specified Uniform Resource Identifier (URI) for a delegate subscriber, use the **sip-contact** command in subscriber-entry configuration mode. To remove the SIP contact information for an URI for a delegate subscriber, use the **no sip-contact** command.

```
sip-contact {uri}
```

```
no sip-contact {uri}
```

## Syntax Description

<i>uri</i>	This is the Uniform Resource Identifier (URI) of the delegate subscriber for whom you want to configure Provisioned Delegate Registration.  It is an IP address. It is a string field of 62 characters maximum length.
------------	--

## Command Default

No default behavior or values are available.

## Command Modes

subscriber-entry configuration (config-sbc-sbe-subscriber-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

This command configures the SIP contact information for a specified URI IP address location or address of record. The contact information is used to provision the SBC with client device information, so the SBC can register the device.

A delegate subscriber must have one or more SIP contacts or Uniform Resource Identifiers (URIs) associated with it. For every delegate registration configured with the **delegate-registration** *hostname* command, one or more SIP contacts/URIs must be configured in the SIP Contacts table (*amb\_mw\_sudb\_local\_id*). After a SIP contact is configured, the client adjacency is also defined in a subsequent step.

The following rules apply to configuring SIP contact information:

- The subscriber detail table must exist before contacts can be created.
- Contacts in a currently active subscriber cannot be created, modified, or deleted.
- A contact cannot be deactivated while the parent subscriber is active.

## Examples

The following example configures a SIP contact information for a subscriber, for whom a subscriber detail table exists, and for whom, after the SIP contact is configured, delegate registration can be configured:

```
sbc mySbc
sbe
subscriber sip:bob@isp.example
```

```

sip-contact sip:steve@10.1.1.2
adjacency CallMgrB
exit

```

The following example configures a SIP contact information for a delegate subscriber at the address of record, where aor= sip:bob@isp.example, and configures delegate registration for the subscriber:

```

(config)# sbc mySbc
(config)# sbe
(config-sbc-sbe)# subscriber sip:bob@isp.example
(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
(config-sbc-sbe-subscriber-contact)# exit
(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
(config-sbc-sbe-subscriber-delegate)# profile my-profile
(config-sbc-sbe-subscriber-delegate)# activate

```

#### Related Commands

Command	Description
subscriber	Defines a unique subscriber for whom you want to configure Provisioned Delegate Registration.
delegate-profile	Configures a delegate registration profile that is applied to a delegate registration subscriber.
delegate-registration	Configures a delegate registration for a delegate client.
adjacency	Configures the adjacency facing the registrar.
profile	Applies a delegate registration profile to a delegate registration subscriber.
show sbc sbe sip delegate-profile	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.
show sbc sbe sip subscribers	Displays subscribers for whom Provisioned Delegate Registration has been provisioned.



# sipi

To configure the SIP-I commands on a SIP adjacency, use the **sipi** command in adjacency SIP configuration mode. To deconfigure the SIP-I commands, use the **no** form of this command.

**sipi passthrough**

**no sipi passthrough**

<b>Syntax Description</b>	<b>passthrough</b> Configures a SIP adjacency for SIP-I passthrough.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>sipi</b> command is used to configure a SIP adjacency for SIP-I passthrough:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# sipi passthrough
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbcs sbe adjacencies</b>	Lists the adjacencies configured on the SBE.

# sip adjacency

To configure a SIP adjacency for a Session Border Controller (SBC) service, use the **sip adjacency** command in the SBE configuration mode. To deconfigure the SIP adjacency, use the **no** form of this command.

**sip adjacency** *adjacency-name*

**no sip adjacency** *adjacency-name*

## Syntax Description

*adjacency-name* Specifies the name of the SIP adjacency.

The *adjacency-name* can have a maximum of 30 characters which can include the underscore character (\_) and alphanumeric characters.

**Note** Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following example shows how to configure a SIP adjacency named sipGW:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip adjacency sipGW
```

## Related Commands

Command	Description
<b>adjacency</b>	Configures a H.323 adjacency.

# sip body-editor

To create a body editor to filter the non-SDP message bodies from the incoming and outgoing SIP messages, use the **sip body-editor** command in the Signaling Border Element (SBE) configuration mode. To remove a body editor, use the **no** form of this command.

**sip body-editor** *editor-name*

**no sip body-editor** *editor-name*

<b>Syntax Description</b>	<i>editor-name</i>	Specifies the name of the body editor.  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------------	--------------------	---

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	When you use this command to create a body editor, you must also use the <b>body</b> and the <b>description</b> commands under the SIP Body Editor configuration mode to complete the configuration.
-------------------------	--

<b>Examples</b>	The following example shows how to create a body editor named bodyeditor1 in the SBE configuration mode:  <pre>Router(config)# sbc mySBC Router(config-sbc)# sbe Router(config-sbc-sbe)# sip body-editor bodyeditor1 Router(config-sbc-sbe-mep-bdy)#</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sip header-editor</b>	Configures a header editor.
	<b>sip method-editor</b>	Configures a method editor.
	<b>sip option-editor</b>	Configures an option editor.
	<b>sip parameter-editor</b>	Configures a parameter editor.



# sip body-profile

To create a body profile to filter non-SDP message bodies from incoming and outgoing SIP messages, use the **sip body-profile** command in SBE configuration mode. To remove the body profile, use the **no sip body-profile** command.

```
sip body-profile {profile_name}
```

```
no sip body-profile {profile_name}
```

<b>Syntax Description</b>	<p><i>profile_name</i> Describes the body profile name.</p> <p>The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	---

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.6</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	<p>When you use this command to create a body profile under the SBE mode, you must also use the <b>body</b> <i>{body_name}</i> and the <b>action</b> commands to complete the configuration.</p>
-------------------------	--

After creating a body profile with the **sip body-profile** *{profile\_name}* command, you can associate the body profile at the following levels and configuration modes:

- At the SIP signaling entity level (ingress or egress), under SBE mode, using the **sip default body-profile** **[[inbound|outbound]** *{profile\_name}* command. The body profile is associated for the entire signaling instance (that is all messages, either ingress or egress, passing through the SBC).
- SIP adjacency level, under SIP adjacency mode, using the **body-profile** **[[inbound|outbound]** *{profile\_name}* command. The body profile is associated to an adjacency.
- At SIP method profile level, under method profile mode, using the **body-profile** *{profile\_name}* command. The body profile is associated to a method profile.

The SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

**Examples**

The following example does the following: creates a body profile named bodyprofile1; associates the body profile at the SIP signaling level for all inbound calls passing through the SBC; describes the body type, that is to act on messages with Content-Type header “application/ISUP”; and instructs SBC to strip that particular message body and pass the rest of the message:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-profile bodyprofile1
Router(config-sbc-sbe)# sip default body-profile inbound bodyprofile1
Router(config-sbc-sbe-sip-body)# body application/ISUP
Router(config-sbc-sbe-sip-body-ele)# action strip
Router(config-sbc-sbe-sip-body-ele)#
```

**Related Commands**

Command	Description
<b>sip default body-profile</b>	To associate a body profile at the SIP signaling level under the SBE mode.
<b>body-profile</b>	To associate a body profile to a method profile under the method profile mode.
<b>body-profile (sip adj)</b>	To associate a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
<b>body</b>	To name a body type or content header type for a non-SDP message body that is part of the body profile.
<b>action</b>	To set the action to take on a body type in a SIP body profile for a non-SDP message body.

# sip default body-profile

To associate a body profile at the SIP signaling level and for the entire signaling instance, use the **sip default body-profile** command in SBE configuration mode. To remove the body profile, use the **no sip default body-profile** command.

```
sip default body-profile [inbound | outbound] {profile_name}
```

```
no sip default body-profile [inbound | outbound] {profile_name}
```

## Syntax Description

inbound	Sets the inbound path for the body profile. Select inbound or outbound for the path.
outbound	Sets the outbound path for the body profile. Select inbound or outbound for the path.
<i>profile_name</i>	Describes the body profile name.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

“For the entire signaling instance” means all messages, either ingress or egress, passing through the SBC.

After creating a body profile with the **sip body-profile** *{profile\_name}* command, you can associate the body profile at the following additional levels and configuration modes:

- SIP adjacency level, under SIP adjacency mode, using the **body-profile** **[[inbound|outbound]** *{profile\_name}* command. The body profile is associated to an adjacency.
- At SIP method profile level, under method profile mode, using the **body-profile** *{profile\_name}* command. The body profile is associated to a method profile.

SBC uses a body profile that you create and associate to filter non-SDP bodies from incoming and outgoing SIP messages, based on the Content-Type header field. A body profile allows a message containing a specific non-SDP body to be either passed (without altering the message), stripped of the body (and pass the rest of the message), or be rejected.

**Examples**

The following example does the following: creates a body profile named `bodyprofile1`; describes the body type, that is to act on messages with Content-Type header “application/ISUP”; instructs SBC to strip that particular message body and pass the rest of the message; and associates the body profile at the SIP signaling level for all inbound calls passing through the SBC:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip body-profile bodyprofile1
Router(config-sbc-sbe-sip-body)# body application/ISUP
Router(config-sbc-sbe-sip-body-ele)# action strip
Router(config-sbc-sbe-sip-body-ele)# exit
Router(config-sbc-sbe-sip-body)# exit
Router(config-sbc-sbe)# sip default body-profile inbound bodyprofile1
```

**Related Commands**

Command	Description
<b>body-profile</b>	To associate a body profile to a method profile under the method profile mode.
<b>body-profile (sip adj)</b>	To associate a body profile at the SIP adjacency level, to an adjacency, under SIP adjacency mode.
<b>sip body-profile</b>	To create a body profile used to filter non-SDP bodies from incoming and outgoing SIP messages.
<b>body</b>	To name the body type or content header type for a non-SDP message body that is part of the body profile.
<b>action</b>	To set the action to take on a body type in a SIP body profile for a non-SDP message body



# sip dns

To enter the SIP DNS configuration mode, use the **sip dns** command in the SBE configuration mode. To exit this mode, use the **exit** command.

## sip dns

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure limits on DNS entries:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip dns
Router(config-sbe-dns)#
```

Related Commands	Command	Description
	<b>cache-lifetime</b>	Configures the lifetime of any DNS entry.
	<b>cache-limit</b>	Configures the maximum number of entries that are permitted in the DNS cache.

# sip editor-type

To set a default editor type to be applied to an adjacency that has not been explicitly set, use the **sip editor-type** command in the SBE configuration mode. To remove the default editor type, use the **no** form of this command.

**sip editor-type { editor | profile }**

**no sip editor-type**

## Syntax Description

<b>editor</b>	Sets the default to use the method, header, option, parameter, or body editor.
<b>profile</b>	Sets the default to use the method, header, option, parameter, or body profile.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to set a default editor type:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip editor-type editor
```

## Related Commands

Command	Description
<b>sip method-editor</b>	Configures a method editor.
<b>sip header-editor</b>	Configures a header editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>sip body-editor</b>	Configures a body editor.
<b>sip option-editor</b>	Configures an option editor.

# sip encryption key

To configure a global encryption key on a SIP Interconnection Border Control Function (IBCF) adjacency, use the **sip encryption key** command in the SIP adjacency mode. To deconfigure the global encryption key, use the **no** form of this command.

**sip encryption key** *key*

**no sip encryption key** *key*

<b>Syntax Description</b>	<i>key</i> Specifies the encryption key.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>sip encryption key</b> command is used to configure a global encryption key on a SIP IBCF adjacency:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# encryption key mykey
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sip inherit profile</b>	Configures a global inherit profile in the SIP adjacency mode.

# sip error-profile

To create an error profile and enter error profile configuration mode, use the **sip error-profile** command in SBE configuration mode. To remove an error profile, use the no form of this command.

**sip error-profile** *profile-name*

**no sip error-profile** *profile-name*

## Syntax Description

<i>profile-name</i>	Specifies the name of the error profile. The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip error-profile Error_profile_1
Router(config-sbc-sbe-err)
```

## Related Commands

Command	Description
<b>error-profile</b>	Configures an existing error profile as the outbound SIP error profile.
<b>sip error-profile</b>	Creates an error profile and enters error profile configuration mode.
<b>cause</b>	Configures the cause of an internal error for an error profile.
<b>show sbc sbe sip error-profile</b>	Displays the configuration information of an error profile.



# sip header-editor

To configure a header editor in the mode of an signaling border element (SBE) entity, use the **sip header-editor** command in the SBE configuration mode. To remove a header editor, use the **no** form of this command.

**sip header-editor** { *editor-name* | **default** }

**no sip method-editor** { *editor-name* | **default** }

## Syntax Description

<i>editor-name</i>	Specifies the name of the header editor. If you enter the name <b>default</b> , the default editor is configured.  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
<b>default</b>	Configures the default header editor.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Use the **sip header-editor** command to enter the SBE SIP header configuration mode.

If you use the **default** keyword, the default editor is configured. This editor is used for all the adjacencies that do not have a specific editor configured.

## Examples

The following example shows how the **sip header-editor** command configures a header editor named test1:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor test1
Router(config-sbc-sbe-mep-hdr)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip body-editor</b>	Creates a body editor to filter the non-SDP message bodies from the incoming and outgoing SIP messages.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.

# sip header-profile

To configure a header profile in the mode of an SBE entity, use the **sip header-profile** command in SBE configuration mode. To remove the method profile, use the **no** form of this command.

**sip header-profile** *profile-name*

**no sip method-profile**

## Syntax Description

<i>profile-name</i>	Specifies the name of the method profile.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.
<b>Note</b>	If you enter the <i>name</i> <b>default</b> , the default profile is configured.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **sip header-profile** command configures a method profile with the name of test1:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile test1
```



# sip home network identifier

To configure a home network identifier on all IBCF adjacencies, use the **sip home network identifier** command in the SBE configuration mode. To deconfigure the home network identifier, use the **no** form of this command.

**sip home network identifier** *network-name*

**no sip home network identifier**

## Syntax Description

<i>network-name</i>	Specifies the name of the home network identifier. The <i>network-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **home network identifier** command is used to configure a home network identifier on all IBCF adjacencies:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip home network identifier myhome.com
```

## Related Commands

Command	Description
<b>sip visited network identifier</b>	Configures a visited network identifier on a SIP Proxy-Call Session Control Function (P-CSCF) adjacency.

# sip hunting-trigger

To configure failure return codes to trigger hunting in SBE configuration mode, use the **sip hunting-trigger** command in SBE configuration mode.

The **no** form of the command clears all error codes.

If you specify **no sip hunting-trigger x y**, then just codes x and y are removed from the configured list.

*sip hunting-trigger {error-codes | disable} error-codes*

*no sip hunting-trigger {error-codes | disable} error-codes*

<b>Syntax Description</b>	<i>error-codes</i>	Signifies a space-separated list of SIP numeric error codes.
---------------------------	--------------------	--

<b>Command Default</b>	<i>No default behavior or values are available.</i>	
------------------------	---	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)	
----------------------	------------------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	<p>If you enter <b>sip hunting-trigger x</b> followed by <b>sip hunting-trigger y</b>, the value of x is replaced with y.</p> <p>To set both x and y to be hunting triggers, you must enter <b>sip hunting-trigger x y</b>.</p> <p>The related command <b>hunting-trigger</b> is used to configure failure return codes to trigger hunting in H.323 (global H.323 scope), adjacency SIP (destination SIP adjacency), and adjacency h323 (destination H.323 adjacency) modes. The <b>hunting-trigger</b> command does not apply in global SIP mode; instead the <b>sip hunting-trigger</b> command is used in global SIP mode.</p>
-------------------------	---

<b>Examples</b>	<p>The following example shows how to configure SIP to retry routing if it receives a 415 (media unsupported) or 480 (temporarily unavailable) error:</p>
-----------------	---

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# sip hunting-trigger 416 480
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show sbc sbe hunting-trigger</b>	Shows the H.323 or SIP hunting triggers at the global level.

# sip inherit profile

To configure a global inherit profile, use the **sip inherit profile** command in the SBE configuration mode. To deconfigure the global inherit profile, use the **no** form of this command.

```
sip inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external
| preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering |
preset-standard-non-ims}
```

```
no sip inherit profile
```

Syntax Description		
	preset-access	Specifies a preset access profile.
	preset-core	Specifies a preset core profile.
	<b>preset-ibcf-ext-untrusted</b>	Specifies a preset IBCF external untrusted profile.
	<b>preset-ibcf-external</b>	Specifies a preset IBCF external profile.
	<b>preset-ibcf-internal</b>	Specifies a preset IBCF internal profile.
	<b>preset-p-cscf-access</b>	Specifies a preset P-CSCF-access profile.
	<b>preset-p-cscf-core</b>	Specifies a preset P-CSCF-core profile.
	preset-peering	Specifies a preset peering profile.
	<b>preset-standard-non-ims</b>	Specified a preset standard-non-IMS profile.

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	The command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **sip inherit profile** command is used to configure a P-CSCF-access inherit profile on a SBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip inherit profile preset-p-cscf-access
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip timer</b>	Enters the mode of a SIP timer function.

# sip ip-fqdn-mapping

To configure SIP IP-to-FQDN mapping on signaling border elements (SBEs), use the **sip ip-fqdn-mapping** command in the SBE configuration mode.

```
sip ip-fqdn-mapping index { ipv4 | ipv6 } ip-address fqdn { both-ways | ip-to-fqdn }
```

Syntax Description		
<i>index</i>		Index number that uniquely identifies this mapping
<i>ip-address</i>		Specifies the IPv4 or IPv6 address for the signaling address of the SIP
<i>fqdn</i>		Fully qualified domain name
<b>both-ways</b>		Both ways mapping between IP address and FQDN
<b>ip-to-fqdn</b>		Only maps IP address to FQDN

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.6	The <i>ipv6</i> keyword was added.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the both ways mapping between IP and FQDN for IPv4 address:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip ip-fqdn-mapping 1 ipv4 11.22.33.41 example.sbc1.com both-ways
Router(config-sbc-sbe)#
```

The following example shows how to configure the one way IP-to-FQDN mapping for IPv4 address:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip ip-fqdn-mapping 2 ipv4 11.22.33.44 example2.sbc1.com
ip-to-fqdn
Router(config-sbc-sbe)#
```

# sip max-connections

To configure the maximum number of SIP connections that will be made to each remote address, use the **sip max-channels** command in SBE configuration mode. To set this to an unlimited number of connections, use the **no** form of this command.

**sip max-connections** *number-of-connections*

**no sip max-connections** *number-of-connections*

## Syntax Description

*number-of-connections* The maximum number of connections.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command configures the maximum number of connections to each remote address to 1:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip max-connections 1
```

## Related Commands

Command	Description
<b>max-bandwidth</b>	Configures the maximum bandwidth for an entry in an admission control table.
<b>max-regs-rate</b>	Configures the maximum call number of subscriber registrations for an entry in an admission control table.
<b>max-updates</b>	Configures the maximum call updates for an entry in an admission control table.

# sip method-editor

To configure a method editor in the mode of an SBE entity, use the **sip method-editor** command in the Signaling Border Element (SBE) configuration mode. To remove a method editor, use the **no** form of this command.

```
sip method-editor {editor-name | default}
```

```
no sip method-editor {editor-name | default}
```

Syntax Description		
	<i>editor-name</i>	Specifies the name of the method editor.  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
	<b>default</b>	Configures the default method editor. This editor is used for all the adjacencies that do not have a specific method editor configured.

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Use the **sip method-editor** command to enter the SIP method configuration mode.

**Examples** The following example shows how the **sip method-editor** command configures a method editor named test1:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-editor test1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>blacklist</b>	Configures the SIP header or a method blacklist editor on a SIP message.
<b>description</b>	Configures the description for the SIP header editor or SIP method editor.
<b>sip body-editor</b>	Creates a body editor to filter the non-SDP message bodies from the incoming and outgoing SIP messages.
<b>sip header-editor</b>	Configures a header editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.



# sip method-profile

To configure a method profile in the mode of an SBE entity, use the **sip method-profile** command in SBE configuration mode. To remove the method profile, use the **no** form of this command.

**sip method-profile** *profile-name*

**no sip method-profile**

<b>Syntax Description</b>	<p><i>profile-name</i></p> <p>Specifies the name of the method profile. If you enter the <i>name</i> <b>default</b>, the default profile is configured. This profile is used for all agencies that do not have a specific profile configured.</p> <p>The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how the <b>sip method-profile</b> command configures a method profile with the name of test1:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile test1
```

# sip option-editor

To configure an option editor in the mode of an Signaling Border Element (SBE) entity for a Session Initiation Protocol (SIP) option whitelist editor or blacklist editor, use the **sip option-editor** command in the SBE configuration mode. To remove an option editor, use the **no** form of this command.

**sip option-editor** { *editor-name* | **default** }

**no sip option-editor** { *editor-name* | **default** }

## Syntax Description

<i>editor-name</i>	Specifies the name of the option editor.  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
<b>default</b>	Configures the default option editor.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Use the **sip option-editor** command to enter the SBE SIP option configuration mode.

If you use the **default** keyword, the default editor is configured. This editor is used for all the adjacencies that do not have a specific editor configured.

## Examples

The following example shows how to configure an option editor named test1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-editor test1
Router(config-sbc-sbe-mep-opt)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>blacklist</b>	Configures the SIP header or a method blacklist editor on a SIP message.
<b>description</b>	Configures the description for the SIP header editor or SIP method editor.
<b>sip body-editor</b>	Creates a body editor to filter the non-SDP message bodies from the incoming and outgoing SIP messages.
<b>sip header-editor</b>	Configures a header editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.

# sip option-profile

To configure a option profile in the mode of an SBE entity for a SIP option whitelist or blacklist profile, use the **sip option-profile** command in SBE configuration mode. To remove the option profile, use the **no** form of this command.

**sip option-profile** {*profile-name* | **default**}

**no sip option-profile** {*profile-name* | **default**}

## Syntax Description

<i>profile name</i>	Specifies the name of the method profile.  The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
<b>default</b>	Configures the default option profile.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If a configuration is loaded on top of an active configuration, warnings are generated to notify that the configuration cannot be modified. If you must modify the entire configuration by loading a new one, please remove the existing configuration first.

Use the **sip option-profile** command to enter SBE SIP option configuration mode.

If you use the **default** keyword, the default profile is configured. This profile is used for all adjacencies which do not have a specific profile configured.

## Examples

The following example shows how to configure a option profile with the name of test1.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-profile test1
Router(config-sbc-sbe-sip-opt)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>blacklist</b>	Configures SIP header or method blacklist profiles on a Session Initiation Protocol (SIP) message.
<b>description</b>	Configures the description for the SIP header-profile or SIP method-profile.
<b>method</b>	Adds a method with a specified name to a SIP message profile.
<b>pass-body</b>	Permits SIP message bodies to pass through [for non-vital SIP methods accepted by a method profile] in the SIP method profile mode of an SBE entity.

# sip parameter-editor

To configure a parameter editor in the signaling border element (SBE) entity mode, use the **sip parameter-editor** command in the SBE configuration mode. To remove a parameter editor, use the **no** form of this command.

**sip parameter-editor** *editor-name*

**no sip parameter-editor** *editor-name*

## Syntax Description

<i>editor-name</i>	Specifies the name of the parameter editor.  The <i>editor-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
--------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Use the **sip parameter-editor** command to enter the SBE SIP parameter configuration mode.

## Examples

The following example shows how to configure a parameter editor named paramedit1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-editor paramedit1
Router(config-sbc-sbe-mep-prm)#
```

## Related Commands

Command	Description
<b>sip body-editor</b>	Creates a body editor to filter the non-SDP message bodies from the incoming and outgoing SIP messages.
<b>sip header-editor</b>	Configures a header editor.

<b>Command</b>	<b>Description</b>
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.

# sip parameter-profile

To configure a parameter profile for a method profile in the mode of an SBE entity, use the **sip parameter-profile** command in SBE configuration mode. To remove the parameter profile, use the **no** form of this command.

**sip parameter-profile** *profile-name*

**no sip parameter-profile** *profile-name*

## Syntax Description

<i>profile name</i>	Specifies the name of the parameter profile. The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The following example shows how to configure a parameter profile with the name of paramprof1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip parameter-profile paramprof1
Router(config-sbc-sbe-sip-prm)# parameter user
Router(config-sbc-sbe-sip-prm-ele)# action add-not-present value phone
```

## Related Commands

Command	Description
<b>sip-method profile</b>	Configures a method-profile.



# sip sdp-match-table

To create an SDP match table, use the **sip sdp-match-table** command in SBE configuration mode. To remove an SDP match table, use the **no** form of this command.

**sip sdp-match-table** *table-name*

**no sip sdp-match-table** *table-name*

<b>Syntax Description</b>	<p><i>table-name</i> Specifies the user name to fill in on generated SDPs.</p> <p>The <i>table-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	The <b>sdp-match-table</b> command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	This command was modified to be <b>sip sdp-match-table</b> .

**Usage Guidelines** One policy can only hold one sdp-match-table.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following command configures the SDP match table foo:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip sdp-match-table foo
Router(config-sbc-sbe-sip)#
```

Related Commands	Command	Description
	<b>action (sdp)</b>	Configures an SDP policy table action.
	<b>match-string</b>	Configure an SDP attribute matching string.
	<b>sip sdp-policy-table</b>	<b>Configure</b> an SDP policy table.



# sip sdp-media-profile

To create or modify an SDP media profile, or to associate an SDP media profile to a CAC policy, use the **sip sdp-media-profile** command in SBE configuration mode or in SBE CAC policy CAC table entry mode. Use the **no** form of the command to remove an SDP media profile.

**sip sdp-media-profile** *profile-name*

**no sip sdp-media-profile** *profile-name*

## Syntax Description

<i>profile-name</i>	Specifies the name of profile to create or modify. The <i>profile-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters. <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
---------------------	--

## Command Default

The global default is used.

## Command Modes

SBE configuration (config-sbc-sbe)

SBE CAC policy CAC table entry (sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Use the **sip sdp-media-profile** command to configure media descriptions for customized offers for late-to-early media interworking. After creating an SDP media profile, associate the profile to a signal by adding the profile name to a CAC policy. You can add a maximum of ten entries for each sdp-media-profile.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to create a new SDP profile for customizing media descriptions in late-to-early interworking offers:

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip sdp-media-profile Mediaprofile
Router(config-sbc-sbe-sip-sdp-media)# entry 1
Router(config-sbc-sbe-sip-sdp-media-ele)# line 1 "m=audio 0 RTP/AVP 31"
Router(config-sbc-sbe-sip-sdp-media-ele)# line 2 "a=aaa:testing"
Router(config-sbc-sbe-sip-sdp-media-ele)# Ctrl Z
```

The following example associates the profile to an existing CAC policy:

```
Router# configure terminal
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table testpolicytable
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# sip sdp-media-profile Mediaprofile
Router(config-sbc-sbe-cacpolicy-cactable-entry)
```

#### Related Commands

Command	Description
<b>entry</b>	Creates or modifies an entry in a table or an SDP media profile.
<b>media-line</b>	Adds a media description line to an entry in an SDP media profile.
<b>show sbc sbe sip sdp-media-profile</b>	Shows all SDP media profiles in an SBC service or details for a specified profile.

# sip sdp-policy-table

To **configure** an SDP policy table, use the **sip sdp-policy-table** command in the SBE configuration mode. To **deconfigure** an SDP policy table, use the **no** form of this command.

**sip sdp-policy-table** *table\_name*

**no sip sdp-policy-table** *table\_name*

<b>Syntax Description</b>	<p><i>table_name</i> Specifies the name of the SDP policy.</p> <p>The <i>table_name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	The <b>sdp-policy-table</b> command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	This command modified to be <b>sip sdp-policy-table</b> .

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following command configures the SDP policy table foo:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip sdp-policy-table foo
Router(config-sbc-sbe-sip)#
```

Related Commands	Command	Description
	<b>sip sdp-match-table</b>	Creates an SDP match table.
	<b>action (sdp)</b>	Configures an SDP policy table action.
	<b>match-string</b>	Configure an SDP attribute matching string.



# sip sdp origin-user-name

To **configure** the originating user name that is filled in generated SDPs, use the **sdp origin-user-name** command in the SBE configuration mode. To reset this user name such that received user name from an SDP is the user name used on the generated SDP, use the **no** form of this command.

**sip sdp origin-user-name** *user-name*

**no sip sdp origin-user-name** *user-name*

## Syntax Description

<i>user-name</i>	Specifies the user name to be filled in on generated SDPs. The <i>user-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	The <b>sdp origin-user-name</b> command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command was modified to be <b>sip sdp origin-user-name</b> .

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command configures the SDP username to use on generated SDPs to foo:

```
Router# configure
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip sdp origin-user-name foo
Router(config-sbc-sbe-sip)#
```

# sip timer

To enter the mode of the SIP timer function, use the **sip timer command in SBE configuration mode**. To return to the default value, use the **no** form of this command.

**sip timer**

**no sip timer**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to enter the SIP timer mode:

```
Router# config
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)
```



# sip visited network identifier

To configure a visited network identifier on a SIP P-CSCF adjacency, use the **sip visited network identifier** command in SBE configuration mode. To deconfigure the visited network identifier, use the **no** form of this command.

**sip visited network identifier** *network-name*

**no sip visited network identifier**

## Syntax Description

*network-name* Specifies the name of the visited network identifier.

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to use the **sip visited network identifier** command to configure a visited network identifier on a P-CSCF-access adjacency:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
Router(config-sbe-adj-sip)# sip visited network identifier cisco.com2
```

## Related Commands

Command	Description
<b>sip home network identifier</b>	Configures a home network identifier on all IBCF adjacencies.

# snmp-server enable traps sbc

To enable SBC notification types, use the **snmp-server enable traps sbc** command in global configuration mode without keywords. To disable all SBC notification types, use the **no** form of this command without keywords.

**snmp-server enable traps sbc** [adj-status | blacklist | congestion-alarm | h248-ctrlr-status | media-source | qos-statistics | radius-conn-status | sla-violation | svc-state]

**no snmp-server enable traps sbc** [adj-status | blacklist | congestion-alarm | h248-ctrlr-status | media-source | qos-statistics | radius-conn-status | sla-violation | svc-state]

## Syntax Description

adj-status	Enables the SNMP SBC Adjacency Status traps.
blacklist	Enables the SNMP SBC Blacklist traps.
congestion-alarm	Enables the SNMP SBC Congestion Alarm traps.
h248-ctrlr-status	Enables the SNMP SBC H.248 Controller Status traps.
media-source	Enables the SNMP SBC Media Source Alert traps.
qos-statistics	Enable the SNMP SBC QoS Statistics traps.
radius-conn-status	Enable the SNMP SBC Radius Connect Status traps.
sla-violation	Enable the SNMP SBC Sla Violation traps.
svc-state	Enable the SNMP SBC Service state traps.

## Command Default

All the SBC-related traps are disabled.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.4	The <b>qos-statistics</b> keyword was added to this command.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

Use the **snmp-server enable traps sbc** command to enable or disable all of the SNMP traps. Use specific keywords to enable or disable specific SNMP traps.

After you enable a trap, specify the recipient of a SNMP notification operation by using the **snmp-server host** command.

## Examples

The following example shows how to enable only SNMP blacklist notification:

```
Router# configure terminal  
Router(config)# snmp-server enable traps sbc blacklist
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>calc-moscqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.

# softswitch-shield

To enable the softswitch shielding on the SIP, use the **softswitch-shield** command in adjacency SIP configuration mode. To disable the softswitch shielding, use the no form of this command.

**softswitch-shield**

**no softswitch-shield**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	Adjacency SIP configuration (config-sbc-sbe-adj-sip)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to enable the softswitch shielding on the SIP adjacency:
-----------------	--

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip test
Router(config-sbc-sbe-adj-sip) softswitch-shield
Router(config-sbc-sbe-adj-sip)
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>expires-header</b>	Configures the expires parameter in the SIP contact header.
	<b>show sbc sbe adjacencies</b>	Displays all the detailed field output pertaining to a specified Session Initiation Protocol (SIP) adjacency.

# src-address

To enter the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only), use the **src-address** command in SIP header configuration mode. To exit the source address mode, use the **no** form of this command or the **exit** command.

**src-address**

**no src-address**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SIP header configuration (config-sbc-sbe-sip-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of modes required to run the command.

This command puts you in the source address mode where you use the **header-prio header-name** command to set the priority of the header or headers from which a calling party address is derived.



**Note**

The header list is for inbound calls only.

**Examples** The following example shows how to enter the source address mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-profile HP1
Router(config-sbc-sbe-sip-hdr) src-address
Router(config-sbc-sbe-sip-hdr-scr)#
```

Related Commands	Command	Description
	<b>activate (enum)</b>	Activates ENUM client.
	<b>dial-plan-suffix</b>	Configures the dial plan suffix used for the ENUM query.
	<b>div-address</b>	Enters the diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).

<b>Command</b>	<b>Description</b>
<b>dst-address</b>	Enters the destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>entry (enum)</b>	Configures the ENUM client entry name and enter the ENUM entry configuration mode.
<b>enum</b>	Configures the ENUM client ID number and enter the ENUM configuration mode.
<b>header-prio</b> <b>header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>max-recursive-depth</b>	Configures the maximum number of recursive ENUM look-ups for non-terminal Resource Records (RR).
<b>max-responses</b>	Configures the maximum number of ENUM records returned to the routing module.
<b>req-timeout</b>	Configures the ENUM request timeout period.
<b>src-address</b>	Enters the source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).
<b>server ipv4</b>	Configures the IPv4 address of a DNS server for ENUM client and optionally associate the DNS server to a VRF.
<b>show sbc sbe call-policy-set</b>	Displays configuration and status information about call policy sets.
<b>show sbc sbe enum</b>	Displays the configuration information about an ENUM client.
<b>show sbc sbe enum entry</b>	Displays the contents of an ENUM client entry.

## src-address (editor)

To enter the Source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only), use the **src-address** command in the SIP Header Editor configuration mode. To exit the Source address mode, use the **no** form of this command or the **exit** command.

**src-address**

**no src-address**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

This command puts you in the Source address mode from where you can use the **header-prio header-name** command to set the priority of the header or headers from which a calling party address is derived.



**Note**

The header list is for inbound calls only.

**Examples** The following example shows how to enter the Source address mode:

```
Router# configure terminal
Router(config)# sbc MySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor HP1
Router(config-sbc-sbe-mep-hdr) src-address
Router(config-sbc-sbe-mep-hdr-src)#
```

Related Commands	Command	Description
------------------	---------	-------------

<b>div-address</b>	Enables entry into the Diverted-by address mode to set the priority of the header or headers from which to derive a diverted-by address (inbound only).
<b>dst-address</b>	Enables entry into the Destination address mode to set the priority of the header or headers from which to derive a called party address (inbound only).
<b>header-prio header-name</b>	Configures the priority of a header that is used to derive a source, destination, or diverted-by address.
<b>sip header-editor</b>	Configures a header editor.
<b>src-address</b>	Enables entry into the Source address mode to set the priority of the header or headers from which to derive a calling party address (inbound only).



# srtp-fallback

To configure support for the Session Initiation Protocol (SIP) X-cisco-srtp-fallback header, use the **srtp-fallback** command in SBE configuration mode.

## **srtp-fallback**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** SBE configuration (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 3.1.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how the **srtp-fallback** command is used to configure support for SIP X-cisco-srtp-fallback header in SBE configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip pc-150
Router(config-sbc-sbe-adj-sip)# srtp-fallback
```

# srtp branch

To configure SRTP for a caller or a callee in a CAC policy, use the **srtp branch** command in the CAC table entry configuration mode. To unconfigure SRTP for a caller or a callee, use the **no** form of this command.

**srtp branch forbid | mandate | allow | prefer**

**no srtp branch forbid | mandate | allow | prefer**

Syntax Description		
	<b>forbid</b>	Specifies that SRTP is not supported on the caller side of the call. Any incoming signaling from the caller side that proposes SRTP is rejected. All outbound signaling on the caller side containing media descriptions proposes RTP.
	<b>mandate</b>	Specifies that SRTP is mandatory on the caller side of the call. Any incoming signaling from the caller side of the call with media descriptions that do not propose SRTP is rejected. All outbound signaling on the caller side of the call containing media descriptions proposes SRTP.
	<b>allow</b>	Allows the caller or callee to use SRTP optionally. No incoming signaling is rejected as a result of the presence or absence of SRTP proposal in any media description. Outbound signaling may or may not propose SRTP in media descriptions according to the requirements of the call.
	<b>prefer</b>	Specifies that SRTP is preferred on this adjacency. SBC accepts either RTP or SRTP from inbound offers, but only offers SRTP outbound.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.5S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure SRTP in a CAC policy:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
```

```

Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp branch allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit

```

#### Related Commands

Command	Description
<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
<b>srtp media interworking</b>	Configures SRTP-to-RTP media interworking in a CAC policy.
<b>srtp interworking</b>	Configures SRTP-to-RTP interworking in a CAC policy.
<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP-to-RTP interworking after it has rejected an SRTP offer.
<b>srtp response downgrade</b>	Configures a SIP endpoint to support a nonstandard offer and answer SRTP downgrade.
<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

# srtp callee

To configure SRTP for the callee in a CAC policy, use the **srtp callee** command in CAC table entry configuration mode. To remove the SRTP configuration, use the no form of this command.

**srtp callee forbid | mandate | allow**

**no srtp callee forbid | mandate | allow**

## Syntax Description

<b>forbid</b>	SRTP is not supported on the callee side of the call. Any incoming signaling from the callee side that proposes SRTP is rejected. All outbound signaling on the callee side containing media descriptions proposes RTP.
<b>mandate</b>	SRTP is mandatory on the callee side of the call. Any incoming signaling from the callee side of the call with media descriptions that do not propose SRTP is rejected. All outbound signaling on the callee side of the call containing media descriptions proposes SRTP.
<b>allow</b>	Allows the callee to use SRTP optionally. No incoming signaling is rejected as a result of the presence or absence of SRTP proposal in any media description. Outbound signaling may or may not propose SRTP in media descriptions according to the requirements of the call.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure SRTP for the callee in a CAC policy:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
```

```
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp callee allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
<b>srtp media interworking</b>	Configures SRTP to RTP media interworking in a CAC policy.
<b>srtp interworking</b>	Configures SRTP to RTP interworking in a CAC policy.
<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer.
<b>srtp response downgrade</b>	Configures configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade.
<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

# srtp caller

To configure SRTP for the caller in a CAC policy, use the **srtp caller** command in CAC table entry configuration mode. To remove the SRTP configuration, use the no form of this command.

**srtp caller forbid | mandate | allow | prefer**

**no srtp caller forbid | mandate | allow | prefer**

## Syntax Description

<b>forbid</b>	SRTP is not supported on the caller side of the call. Any incoming signaling from the caller side that proposes SRTP is rejected. All outbound signaling on the caller side containing media descriptions proposes RTP.
<b>mandate</b>	SRTP is mandatory on the caller side of the call. Any incoming signaling from the caller side of the call with media descriptions that do not propose SRTP is rejected. All outbound signaling on the caller side of the call containing media descriptions proposes SRTP.
<b>allow</b>	Allows the caller to use SRTP optionally. No incoming signaling is rejected as a result of the presence or absence of SRTP proposal in any media description. Outbound signaling may or may not propose SRTP in media descriptions according to the requirements of the call.
<b>prefer</b>	SRTP is preferred on this adjacency. SBC accepts either RTP or SRTP from inbound offers, but it only offers SRTP outbound.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure SRTP for the caller in a CAC policy:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
```

```

Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp caller allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit

```

Related Commands	Command	Description
	<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
	<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
	<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
	<b>srtp media interworking</b>	Configures SRTP to RTP media interworking in a CAC policy.
	<b>srtp interworking</b>	Configures SRTP to RTP interworking in a CAC policy.
	<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer.
	<b>srtp response downgrade</b>	Configures configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade.
	<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
	<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

# srtp interworking

To configure SRTP to RTP interworking in a CAC policy, use the **srtp interworking** command in CAC table entry configuration mode. To remove the SRTP interworking configuration, use the no form of this command.

**srtp interworking forbid | allow**

**no srtp interworking forbid | allow**

## Syntax Description

forbid	Forbid SRTP to RTP interworking on this call.
allow	Allow SRTP to RTP interworking on this call.

## Command Default

No default behavior or values are available.

## Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure SRTP to RTP interworking in a CAC policy:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp interworking allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```



<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
	<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
	<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
	<b>srtp media interworking</b>	Configures SRTP to RTP media interworking in a CAC policy.
	<b>srtp interworking</b>	Configures SRTP to RTP interworking in a CAC policy.
	<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer.
	<b>srtp response downgrade</b>	Configures configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade.
	<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
	<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

# srtp media interworking

To configure SRTP to RTP media interworking in a CAC policy, use the **srtp media interworking** command in CAC table entry configuration mode. To remove the SRTP media interworking configuration, use the no form of this command.

**srtp media interworking forbid | allow**

**no srtp media interworking forbid | allow**

Syntax Description	forbid	Prohibits SRTP to RTP media interworking on a call.
	allow	Allows SRTP to RTP media interworking on a call.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure SRTP to RTP media interworking in a CAC policy:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp media interworking allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
	<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
	<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
	<b>srtp media interworking</b>	Configures SRTP to RTP media interworking in a CAC policy.
	<b>srtp interworking</b>	Configures SRTP to RTP interworking in a CAC policy.
	<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer.
	<b>srtp response downgrade</b>	Configures configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade.
	<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
	<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

# srtp response downgrade

To configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade (in which an SRTP offer is responded to with an RTP answer), use the **srtp response downgrade** command in CAC table entry configuration mode. To remove the SRTP response downgrade configuration, use the no form of this command.

**srtp {callee | caller} response downgrade**

**no srtp {callee | caller} response downgrade**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If this is set, SBC may respond to an SRTP (RTP/SAVP) offer with an RTP (RTP/AVP) answer. If this is not set, SBC will provide strict adherence to the offer/answer protocol and reject an SRTP offer that is not supported.

**Examples** The following example shows how to configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp caller response downgrade
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
	<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
	<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
	<b>srtp media interworking</b>	Configures SRTP to RTP media interworking in a CAC policy.
	<b>srtp interworking</b>	Configures SRTP to RTP interworking in a CAC policy.
	<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer.
	<b>srtp response downgrade</b>	Configures configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade.
	<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
	<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

## srtp retry rtp

To configure SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer, use the **srtp retry rtp** command in CAC table entry configuration mode. To remove the SRTP retry configuration, use the no form of this command.

```
srtp {callee | caller} retry rtp
```

```
no srtp {callee | caller} retry rtp
```

### Syntax Description

**callee**

**caller**

### Command Default

No default behavior or values are available.

### Command Modes

CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

### Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

If this is set on the side that has generated a 415/488 Reject to an SRTP (RTP/SAVP) offer, SBC reissues the offer using RTP (RTP/AVP) enabling RTP/SRTP interworking (as long as the SRTP configuration allows this).

### Examples

The following example shows how to configure SBC to retry to enable SRTP to RTP interworking on the callee side after it has rejected an SRTP offer:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp callee retry rtp
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
	<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
	<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
	<b>srtp media interworking</b>	Configures SRTP to RTP media interworking in a CAC policy.
	<b>srtp interworking</b>	Configures SRTP to RTP interworking in a CAC policy.
	<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer.
	<b>srtp response downgrade</b>	Configures configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade.
	<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
	<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

# srtp support allow

To configure SRTP support in a CAC policy, use the **srtp caller** command in CAC table entry configuration mode. To remove the SRTP support configuration, use the no form of this command.

**srtp support allow**

**no srtp support allow**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure SRTP support:

```
Router# configure terminal
Router(config)# sbc mine
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table my_table
Router(config-sbc-sbe-cacpolicy)# first-cac-scope call
Router(config-sbc-sbe-cacpolicy)# cac-table my_table
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# srtp support allow
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
```

Related Commands	Command	Description
	<b>srtp support allow</b>	Configures SRTP support in a CAC policy.
	<b>srtp caller</b>	Configures SRTP for the caller in a CAC policy.
	<b>srtp callee</b>	Configures SRTP for the callee in a CAC policy.
	<b>srtp media interworking</b>	Configures SRTP to RTP media interworking in a CAC policy.
	<b>srtp interworking</b>	Configures SRTP to RTP interworking in a CAC policy.



<b>Command</b>	<b>Description</b>
<b>srtp retry rtp</b>	Configures SBC to retry to enable SRTP to RTP interworking after it has rejected an SRTP offer.
<b>srtp response downgrade</b>	Configures configure a SIP endpoint to support a non-standard offer/answer SRTP downgrade.
<b>show sbc sbe call-stats</b>	Lists the statistics for all the calls on the specified SBE.
<b>show sbc sbe calls (srtp)</b>	Displays all the calls on the SBEs.

# standard

To define a standard codec variant name, use the **standard** command in the Codec variant configuration mode. To remove a standard codec variant name, use the **no** form of this command.

**standard** *standard-codec-name*

**no standard**

## Syntax Description

<i>standard-codec-name</i>	Describes the standard system codec name.  The <i>standard-codec-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
----------------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Codec variant configuration (config-sbc-sbe-codec-var-codec)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to define the standard codec variant name using the **standard** command in the Codec variant configuration mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant codec G723-H-1
Router(config-sbc-sbe-codec-var-codec)# standard G723
```

# start

To configure either the H.323 slow start or H.323 fast start mode of operation for an adjacency, use the **start** command in adjacency h323 configuration mode. The **no** form of the command resets to the default of outgoing call start mode is the same as the incoming call start mode.

*start [ fast | slow ]*

*no start*

## Syntax Description

<i>fast</i>	Specifies H.323 fast start mode of operation where the SBC only uses the fast start mode for outgoing calls on the adjacency. However, incoming slow start calls are converted to fast start mode as they cross the SBC.
<i>slow</i>	Specifies H.323 slow start mode of operation where the SBC only uses the slow start mode for outgoing calls on the adjacency. However, incoming fast start calls are converted to slow start as they cross the SBC.

## Command Default

Default is outgoing call start mode is the same as the incoming call start mode

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

When the fast start mode is configured, the SBC only uses the fast start mode for outgoing calls. However, incoming slow start calls are converted to fast start mode as they cross the SBC.

When the slow start mode is configured, the SBC only uses the slow start mode for outgoing calls. However, incoming fast start calls are converted to slow start as they cross the SBC.

If neither fast start nor slow start mode is configured on the adjacency, the default is that the outgoing call start is the same as the incoming call start. The mode of operation can be modified while the adjacency is active but the change will only affect new calls.

## Examples

The following example shows how to configure slow start mode of operation on the adjacency h323:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router (config-sbc-sbe)# adjacency h323
Router (config-sbc-sbe-adj-h323)# start slow
```

Related Commands	Command	Description
	adjacency	Configures an adjacency on the SBC.

# statistics-setting

To configure an adjacency to support SIP method statistics, use the **statistics-setting** command in adjacency SIP configuration mode. To return to the default behavior, use the **no** form of this command.

```
statistics-setting {detail | summary}
```

```
no statistics-setting {detail | summary}
```

Syntax Description	detail	summary
	Allows the <b>show sbc sbe sip-method-stats</b> command to display statistics about SIP response codes and SIP request names, such as INVITE.	Allows the <b>show sbc sbe sip-method-stats</b> command to display statistics about SIP request names only, such as INVITE.

**Command Default** Adjacencies are not configured to support SIP method statistics.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.4.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** The **statistics-setting** command must be configured on an adjacency before using the **show sbc sbe sip-method-stats** command to display SIP method statistics.

**Examples** The following example configures the sipGW adjacency to support detailed SIP method statistics:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip sipGW
Router(config-sbc-sbe-adj-sip)# statistics-setting detail
```

Related Commands	Command	Description
	<b>clear sbc sbe adjacency statistics</b>	Clears the SIP method statistics counters and resets them to zero.
	<b>show sbc sbe sip-method-stats</b>	Displays summary or detailed statistics for a SIP method.

# statistics

To specify the QoS statistic for which alert levels must be set, use the **statistics** command in the SBE configuration mode. To remove this configuration, use the **no** form of this command.

**statistics** {lcl-jit | mos-cqe | mpd-pct | mpl-pct | rmt-jit | rtd | ucr}

**no statistics** [lcl-jit | mos-cqe | mpd-pct | mpl-pct | rmt-jit | rtd | ucr]

## Syntax Description

lcl-jit	Specifies the average local packet jitter.
mos-cqe	Specifies the MOS-CQE score.
mpd-pct	Specifies the ratio of media packets that are dropped to the total number of media packets received.
mpl-pct	Specifies the ratio of media packets that are lost to the total number of media packets sent.
rmt-jit	Specifies the average remote media packet jitter.
rtd	Specifies the average round trip delay.
ucr	Specifies the ratio of unanswered calls to the total number of calls.

## Command Default

*No default behavior or values are available.*

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **statistics** command is used to specify that you want to configure alert levels for the average local packet jitter:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# statistics lcl-jit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>calc-mosqcqe</b>	Specifies the percentage of calls that must be used to calculate the MOS-CQE score.
	<b>current15minutes</b>	Specifies that QoS statistics must be calculated for 15-minute intervals.
	<b>current5minutes</b>	Specifies that QoS statistics must be calculated for 5-minute intervals.
	<b>currentday</b>	Specifies that statistics must be calculated for 24-hour intervals.
	<b>currenthour</b>	Specifies that QoS statistics must be calculated for 60-minute intervals.
	<b>currentindefinite</b>	Specifies that statistics must be calculated indefinitely, starting from the last explicit reset.
	<b>g107 bpl</b>	Sets a value for the Packet-Loss Robustness (Bpl) factor.
	<b>g107 ie</b>	Sets a value for the Equipment Impairment (Ie) factor.
	<b>g107a-factor</b>	Sets a value for the Advantage (A) factor.
	<b>local-jitter-ratio</b>	Specifies the percentage of calls that must be used to calculate the local jitter ratio.
	<b>show sbc sbe adjacencies</b>	Displays details of the adjacencies configured on the SBE.
	<b>show sbc sbe call-stats</b>	Displays the statistics pertaining to all the calls on a the SBE.
	<b>snmp-server enable traps sbc</b>	Enables SBC notification types.

# store-rule

To create a store rule to extract variables from headers, use the **store-rule** command in the SIP Header Editor configuration mode. To remove a store rule, use the **no** form of this command.

**store-rule** [**entry** *entry-number*]

**no store-rule** [**entry** *entry-number*]

## Syntax Description

<b>entry</b>	Specifies the filtered entry number. By default, it is 1.
<b>entry-number</b>	Entry number that can range from 1 to 99.

## Command Default

By default, the entry number is 1.

## Command Modes

SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

## Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

The following example shows how to create a store rule:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor Myeditor
Router(config-sbc-sbe-mep-hdr)# store-rule
```

## Related Commands

Command	Description
<b>blacklist</b>	Configures a SIP header or method blacklist editor on a SIP message.
<b>description</b>	Configures descriptive text for a SIP header.
<b>sip header-editor</b>	Configures a header editor.



# stream-list

To configure a stream list, use the **stream-list** command in the signaling border element (SBE) configuration mode. To remove the stream list, use the **no** form of this command.

**stream-list** *stream-list-name*

**no stream-list** *stream-list-name*

<b>Syntax Description</b>	<p><i>stream-list-name</i> Specifies the name of the stream list.</p> <p>The <i>stream-list-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.</p> <p><b>Note</b> Except for the underscore character, do not use any special character to specify field names.</p>
---------------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE configuration (config-sbc-sbe)
----------------------	------------------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 3.3S</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure a stream list:
-----------------	---

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# stream-list my-stream
Router(config-sbc-sbe-stream-list)#
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>generic-stream media-type</b></td> <td>Configures the media type for a generic stream.</td> </tr> <tr> <td><b>show sbc sbe stream-list</b></td> <td>Displays the stream lists that are present on the SBE.</td> </tr> </tbody> </table>	Command	Description	<b>generic-stream media-type</b>	Configures the media type for a generic stream.	<b>show sbc sbe stream-list</b>	Displays the stream lists that are present on the SBE.
Command	Description						
<b>generic-stream media-type</b>	Configures the media type for a generic stream.						
<b>show sbc sbe stream-list</b>	Displays the stream lists that are present on the SBE.						



# subscriber

To define a unique subscriber for whom you want to configure Provisioned Delegate Registration, use the **subscriber** command in SBE configuration mode. To remove a subscriber for whom you have configured Provisioned Delegate Registration, use the **no subscriber** command.

```
subscriber {aor}
```

```
no subscriber {aor}
```

## Syntax Description

<i>aor</i>	This is the address of record of the delegate client and defines the unique subscriber for whom you want to configure Provisioned Delegate Registration.  It is a string field with a 62 characters maximum length.
------------	---

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

Delegate registration is done underneath the SBE configuration for globally unique subscribers. The subscriber must have one or more SIP contacts or Uniform Resource Identifiers (URIs) associated with it.

## Examples

The following example configures a delegate registration profile that can be applied to a delegate registration subscriber:

```
sbc mySbc sbe
  delegate-profile my-profile
  dur 1000
  retry-cnt 5
  retry-interval 60
  refresh-timeout 200
```

The following example configures a SIP contact for a subscriber, for whom a subscriber detail table exists, and for whom, after the SIP contact is configured, Provisioned Delegate Registration can be configured:

```
sbc mySbc
  sbe
    subscriber sip:bob@isp.example
    sip-contact sip:steve@10.1.1.2
```

```
adjacency CallMgrB
exit
```

The following example configures a delegate registration aor= sip:bob@isp.example

```
(config)# sbc mySbc
(config)# sbe
(config-sbc-sbe)# subscriber sip:bob@isp.example
(config-sbc-sbe-subscriber-entry)# sip-contact sip:steve@10.1.1.2
(config-sbc-sbe-subscriber-contact)# adjacency CallMgrB
(config-sbc-sbe-subscriber-contact)# exit
(config-sbc-sbe-subscriber-entry)# delegate-registration sip:registrar@1.1.1.1
(config-sbc-sbe-subscriber-delegate)# adjacency CallMgrA
(config-sbc-sbe-subscriber-delegate)# profile my-profile
(config-sbc-sbe-subscriber-delegate)# activate
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>delegate-profile</b>	Configures a delegate registration profile that is applied to a delegate registration subscriber.
<b>sip-contact</b>	Configures the SIP contact information for a specified Uniform Resource Identifier (URI) for a delegate subscriber
<b>delegate-registration</b>	Configures a delegate registration for a delegate client.
<b>adjacency</b>	Configures the adjacency facing the registrar.
<b>profile</b>	Applies a delegate registration profile to a delegate registration subscriber.
<b>show sbc sbe sip delegate-profile</b>	Displays subscriber profiles for whom Provisioned Delegate Registration has been configured.
<b>show sbc sbe sip subscribers</b>	Displays subscribers for whom Provisioned Delegate Registration has been provisioned.

# sync

To synchronize the configuration file from active box to standby box, use the **sync** command in inter-chassis redundancy mode.

**sync**

**Syntax Description** There is no keyword or argument.

**Command Default** No default behavior or values are available.

**Command Modes** SBC configuration mode (config-sbc)

Command History	Release	Modification
	Cisco IOS XE Release 3.3.0	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Customer need to use **sync** command in the active box to sync the configuration file from active box to standby box in inter-chassis redundancy mode so that the latest configuration of CUBE-SP will be synchronized in the running configuration file in the standby box.

**Examples** The following example shows how to synchronize the configuration file from active box to standby box:

```
enable
configure terminal
sbc foo
sync
```

# table-type

To configure a Call Admission Control (CAC) table type that enables the priority of the call to be used as a criterion in CAC policy, use the **table-type** command in CAC table configuration mode. To delete the CAC Policy Set or Limit table, use the **no** form of this command.

**table-type** {*policy-set* | *limit* {*list of limit tables*}}

**no table-type** {*policy-set* | *limit* {*list of limit tables*}}

## Syntax Description

policy-set	Specifies a Policy Set table type.  For a Policy Set table type, the event is applied <i>to all entries</i> in the CAC table. You can define the scope at which CAC policy limits are applied using the <b>cac-scope</b> command in each entry.
limit	Specifies a Limit table type.  For a Limit table type, the event matches a <i>single, most specific entry</i> . Only one entry is matched in a limit table type. You can define the match-value within the entry in the Limit table using the <b>match-value</b> command. A limit table type inherits its scope from its parent table.
<i>list of limit tables</i>	Specifies the type of Limit table. This parameter governs the syntax of the match-value fields of the entries in the table.  The Limit table types are: <ul style="list-style-type: none"> <li>• <i>account</i>—Compare the name of the account.</li> <li>• <i>adj-group</i>—Compare the name of the adjacency group.</li> <li>• <i>adjacency</i>—Compare the name of the adjacency.</li> <li>• <i>all</i>—No comparison type. All events match this type.</li> <li>• <i>call-priority</i>—Compare with call priority.</li> <li>• <i>category</i>—Compare the number analysis assigned category.</li> <li>• <i>dst-account</i>—Compare the name of the destination account.</li> <li>• <i>dst-adj-group</i>—Compare the name of the destination adjacency group.</li> <li>• <i>dst-adjacency</i>—Compare the name of the destination adjacency.</li> <li>• <i>dst-prefix</i>—Compare the beginning of the dialed digit string.</li> <li>• <i>event-type</i>—Compare with CAC policy event types.</li> <li>• <i>src-account</i>—Compare the name of the source account.</li> <li>• <i>src-adj-group</i>—Compare the name of the source adjacency group.</li> <li>• <i>src-adjacency</i>—Compare the name of the source adjacency.</li> <li>• <i>src-prefix</i>—Compare the beginning of the calling number string.</li> <li>• <i>sub-category</i>—Compare events sent to or received from members of the same subscriber category.</li> <li>• <i>sub-category-pfx</i>—Compare events sent to or received from members of the same subscriber category prefix.</li> </ul>

**Command Default** No default behavior or values are available.

**Command Modes** CAC table configuration (config-sbc-sbe-cacpolicy-cactable)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.5	The <i>sub-category</i> and <i>sub-category-pfx</i> Limit table types were added.

**Usage Guidelines** When creating a CAC table, you must configure the table type parameter as a Policy Set table type or Limit table type.

You cannot modify the table type if entries are currently configured for a different table type. You will receive the error message “Cannot modify table-type with entries currently configured for previous type.”

For Policy Set tables, the event is applied to all entries in the Policy Set table. You can define the scope at which CAC limits are applied within each entry with the **cac-scope** command. The **cac-scope** command is only available to entries defined within a Policy Set table type.

For Limit tables, the event matches only a single entry. With Limit tables, you can define the match-value within the entry with the **match-value** command. A Limit table inherits its scope from its parent table.

To define a CAC policy, you must define the limit and the scope at which the policy is applied. For example, you can define a policy such that not more than 10 concurrent calls (limit) could ever be made from a single account (scope).

**Examples** The following example shows how to configure the CAC policy-set table TAB1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# first-cac-table TAB1
Router(config-sbc-sbe-cacpolicy)# cac-table TAB1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# cac-scope call
Router(config-sbc-sbe-cacpolicy-cactable-entry)# max-num-calls 20
Router(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
Router(config-sbc-sbe-cacpolicy-cactable-entry)# exit
Router(config-sbc-sbe-cacpolicy-cactable)# exit
Router(config-sbc-sbe-cacpolicy)# complete
```

Related Commands	Command	Description
	<b>cac-table</b>	Configures CAC tables.

<b>Command</b>	<b>Description</b>
<b>match-value</b>	Configures the match-value of an entry in a Limit table.
<b>cac-scope</b>	Allows you to choose a scope at which CAC limits are applied within each entry in a Policy Set table.



# tcp-connect-timeout

To configure the time that SBC waits for a SIP TCP connection to a remote peer to complete before failing that connection, use the **tcp-connect-timeout** command in SIP timer mode. To return to the default value, use the **no** form of this command.

**tcp-connect-timeout** *interval*

**no tcp-connect-timeout**

<b>Syntax Description</b>	<i>interval</i>	Specifies the time, in milliseconds, that the SIP TCP connection to a remote peer stays alive before timing out.
---------------------------	-----------------	--

<b>Command Default</b>	Default interval is 30000 milliseconds
------------------------	--

<b>Command Modes</b>	SIP timer (config-sbc-sbe-sip-tmr)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to set the TCP connection timeout to 30 seconds:
-----------------	--

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# tcp-connect-timeout 30000
```

# tcp-idle-timeout

To configure the length of time that the TCP connection should stay active when in the idle state, use the **tcp-idle-timeout** command in SIP timer mode. To return to the default value, use the no form of this command.

**tcp-idle-timeout** *interval*

**no tcp-idle-timeout**

## Syntax Description

*interval* Specifies the minimum time, in milliseconds, that the TCP connection stays active when it is not processing any traffic. After this time, the TCP connection closes. Range is 1 to 4294967295 ms.

**Note** The value for this command might not be precise since the idle timers are checked every 12 seconds.

## Command Default

Default value is 120000 ms (2 minutes).

## Command Modes

SIP timer (config-sbc-sbe-sip-tmr)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the minimum TCP idle timeout value to 10000 ms:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# tcp-idle-timeout 10000
```

# tcp (blacklist)

To enter the mode for configuring blacklisting for TCP protocol only, use the **tcp** command in the SBE blacklist IPv4 configuration mode.

*tcp port number*

<b>Syntax Description</b>	<i>port number</i>	Port number to blacklist. Range is 0-65535.
---------------------------	--------------------	---

<b>Command Default</b>	No default behavior or values are available.
------------------------	--

<b>Command Modes</b>	SBE blacklist IPv4 configuration (config-sbc-sbe-blacklist-ipv4)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following example shows how to enter the mode for configuring blacklisting for TCP protocol only:
-----------------	---

```
Router# config
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 1.1.1.1
Router(config-sbc-sbe-blacklist-ipv4)# tcp 1
Router(config-sbc-sbe-blacklist-ipv4-tcp)#
```

<b>Related Commands</b>	<b>blacklist</b>	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	<b>address-default</b>	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	<b>clear sbc sbe blacklist</b>	Clears the blacklist for the specified SBC service.
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source.

# tcp timer giveup

To configure a giveup time period that controls how long a TCP connection retries active connections, use the **tcp timer giveup** command in SBE configuration mode. To disable the giveup timer, use the **no** form of this command.

```
tcp timer giveup {1-2400}
```

```
no tcp timer giveup
```

<b>Syntax Description</b>	1-2400	Specifies number of seconds that a TCP connection continues to retry on active connections. The TCP connection is dropped when the giveup time period is reached.
---------------------------	--------	---

**Command Default** By default, the giveup timer is disabled.

**Command Modes** SBE configuration (config-sbc-sbe)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** You use the **tcp timer giveup** command to specify a time period in seconds that controls how long a TCP connection continues to retry on active connections before giving up. On the Cisco ASR 1000 Series Routers, TCP connections will retry for a few minutes due to excessive default retry counts and retry intervals. If the giveup time period is reached without a reply from the peer, the TCP connection is dropped. By default, the giveup timer is disabled which means TCP retries based on the platform default. Because the TCP connection timeout may vary depending on the network, a recommended timeout value must be based on how the endpoints are configured. It is recommended that the timeout value is chosen, such that it is not less than the timer B value that is used by the endpoints and defined in section 17.1.1.2 of RFC3261.

**Examples** The following example shows that a giveup timer has been configured for 40 seconds:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# tcp timer giveup 40
Router(config-sbc-sbe)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>tcp-connect-timeout</b>	Configures the time that SBC waits for a SIP TCP connection to a remote peer to complete before failing that connection.
<b>tcp-idle-timeout</b>	Configures the length of time that the TCP connection should stay active when in the idle state.

# tcs-extra-codecs

To configure a codec list used to announce media capabilities on behalf of either the SIP caller or callee in a SIP to H.323 or H.323 to SIP interworking call, use the **tcs-extra-codecs** command in CAC table entry configuration mode. To remove the codec list, use the **no tcs-extra-codecs** command.

**tcs-extra-codecs** *{code-list-name}*

**no tcs-extra-codecs** *{code-list-name}*

<b>Syntax Description</b>	<i>code-list-name</i>	This is a string text of a maximum length of 30 characters. Describes the extra codecs that a SIP callee or SIP caller can announce to the H.323 side.
---------------------------	-----------------------	--

**Command Default** No default behavior or values are available.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.5.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command configures a codec list and assigns the list to a CAC table. Once a codec list has been assigned, it may not be deleted until it is removed from the CAC table entry. A codec list must exist before it can be assigned to an entry in a CAC table. For a description of the “H.323 TCS Codecs” feature, see the “Codec Handling” chapter in the [Cisco Unified Border Element \(SP Edition\) Configuration Guide: Unified Model](#).

**Examples** The following example configures a codec list called “tcs-extra-caps-list” and assigns that list to the CAC table “cac-tbl-1” in entry 1 to announce extra codecs capability on behalf of the SIP side, whether it is the SIP caller or callee:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec list tcs-extra-caps-list
Router(config-sbc-sbe-codec-list)# exit
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table cac-tbl-1
Router(config-sbc-sbe-cacpolicy-cactable)# table-type policy-set
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# tcs-extra-codecs tcs-extra-caps-list
```

Related Commands	Command	Description
	<b>caller-media-caps</b>	Configures a codec list used to announce media capabilities on behalf of a SIP caller in a SIP to H.323 or H.323 to SIP interworking call.
	<b>callee-media-caps</b>	Configures a codec list used to announce media capabilities on behalf of a SIP callee in a SIP to H.323 or H.323 to SIP interworking call.

# tech-prefix (session border controller)

To configure the RAS tech prefix on an H.323 adjacency, use the **tech-prefix** command in adjacency H.323 configuration mode. To deconfigure RAS Tech Prefix, use the **no** form of this command.

**tech-prefix** *tech-prefix name*

**no tech-prefix** *tech-prefix name*

## Syntax Description

<i>tech-prefix name</i>	Specifies the name of the tech prefix. Use a combination of the numbers from 0-9 and the special characters star (*), hash (#), and comma (,).
-------------------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how the **tech-prefix** command is used to configure RAS tech prefix on an H.323 adjacency named H323ToIsp42:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 H323ToIsp42
Router(config-sbc-sbe-adj-h323)# tech-prefix 2334
```



# test sbc message sip filename script-set editors

To test the message editing functionality of the SBC, use the **test sbc message sip filename script-set editors** command in the privileged EXEC mode.

```
test sbc message sip filename device-type:file-name script-set script-set-number {after-send | before-receive} editors {editor1-name [editor2-name] [editor3-name] . . . [editor8-name]}
```

Syntax Description	
<i>device-type</i>	One of the following or any other storage device installed on the router: <ul style="list-style-type: none"> <li>• <b>bootflash:</b></li> <li>• <b>flash:</b></li> <li>• <b>fpd:</b></li> <li>• <b>nvr:</b></li> <li>• <b>obfl:</b></li> </ul> The list of file system devices is dynamically generated and displayed. Other devices, such as a hard disk, that are available on the platform can also be used in this command.
<i>file-name</i>	Name of the file containing the SIP message on which you want to test the editors.
<i>script-set-number</i>	Number of the script set containing the editors that you want to test.
<b>after-send</b>	Specifies that the outgoing message must be edited after the message is processed by the adjacency and just before it is forwarded from the adjacency.
<b>before-receive</b>	Specifies that the incoming message must be edited just after it is received on the adjacency and before the adjacency begins processing it.
<i>editor1-name</i> . . . <i>editor8-name</i>	Names of the editors. You can specify up to eight editors. You must specify at least one editor.

**Command Default** No default behavior or values are available.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the privileged EXEC mode.

**Examples**

In the following **test sbc message sip filename script-set editors** command, **sdp\_add\_after** has been defined in script-set 123 and **my\_header\_editor** has been configured by using the **sip header-editor** command. In the output of this command, the lines highlighted in bold show the actions performed by the editors.

```
Router# test sbc message sip filename bootflash:inv script-set 123 after-send editors  
sdp_add_after my-header-editor
```

```
INVITE sip:john@example.com:55060 SIP/2.0  
Via: SIP/2.0/UDP 192.0.2.195;branch=z9hG4bKff9b46fb055c0521cc24024da96cd290  
Via: SIP/2.0/UDP 192.0.2.195:55061;branch=z9hG4bK291d90e31a47b225bd0ddff4353e9c  
c0  
From: <sip:192.0.2.195:55061;user=phone>;tag=GR52RWG346-34  
To: "john@example.com" <sip:john@example.com:55060>  
Call-ID: 12013223@192.0.2.195  
CSeq: 1 INVITE  
Contact: <sip:192.0.2.195:5060>  
Content-Type: application/sdp  
Content-Length: 229
```

```
v=0  
o=Clarent 120386 120387 IN IP4 192.0.2.196  
s=Clarent C5CM  
c=IN IP4 192.0.2.196  
t=0 0  
m=audio 40376 RTP/AVP 8 18 4 0  
a=rtpmap:8 PCMA/8000  
a=rtpmap:18 G729/8000  
a=rtpmap:4 G723/8000  
a=rtpmap:0 PCMU/8000  
a=SendRecv
```

```
%Test successful, edited message:  
INVITE sip:john@example.com:55060 SIP/2.0  
Via: SIP/2.0/UDP 192.0.2.195;branch=z9hG4bKff9b46fb055c0521cc24024da96cd290  
Via: SIP/2.0/UDP 192.0.2.195:55061;branch=z9hG4bK291d90e31a47b225bd0ddff4353e9c  
c0  
From: <sip:192.0.2.195:55061;user=phone>;tag=GR52RWG346-34  
To: "john@example.com" <sip:john@example.com:55060>  
Call-ID: 12013223@192.0.2.195  
CSeq: 1 INVITE  
Contact: <sip:192.0.2.195:5060>  
Content-Type: application/sdp  
Content-Length: 258
```

```
name: cisco
```

```
v=0  
o=Clarent 120386 120387 IN IP4 192.0.2.196  
s=Clarent C5CM  
c=IN IP4 192.0.2.196  
t=0 0  
m=audio 40376 RTP/AVP 8 18 4 0  
a=rtpmap:8 PCMA/8000  
a=rtpmap:18 G729/8000  
a=rtpmap:4 G723/8000  
a=rtpmap:0 PCMU/8000  
a=SendRecv
```

```
Editor after adds this line
```

Related Commands	Command	Description
	<b>active-script-set</b>	Activates a script set,
	<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
	<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
	<b>editor</b>	Specifies the order in which a particular editor must be applied.
	<b>editor-list</b>	Specifies the stage at which the editors must be applied.
	<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
	<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
	<b>load-order</b>	Specifies the load order of a script in a script set.
	<b>script</b>	Configures a script written using the Lua programming language.
	<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
	<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
	<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
	<b>sip header-editor</b>	Configures a header editor.
	<b>sip method-editor</b>	Configures a method editor.
	<b>sip option-editor</b>	Configures an option editor.
	<b>sip parameter-editor</b>	Configures a parameter editor.
	<b>test script-set</b>	Tests the working of a script set.
	<b>type</b>	Specifies the type of a script written using the Lua programming language.

# test sbc profile-to-editor sip

To display the editor that is inherited from a Session Initiation Protocol (SIP) profile when the SIP profile is enabled instead of the SIP editor, use the **test sbc profile-to-editor sip** command in the privileged EXEC mode.

```
test sbc profile-to-editor sip profile-type profile-name
```

## Syntax Description

<i>profile-type</i>	Type of SIP profile. It can be one of the following values: <ul style="list-style-type: none"> <li>body-profile</li> <li>default-profiles</li> <li>header-profile</li> <li>method-profile</li> <li>option-profile</li> <li>parameter-profile</li> </ul>
<i>profile-name</i>	Name of SIP profile.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.7.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

We recommend that you enable SIP editor instead of SIP profile. Customers who have already deployed SIP profile can use the **test sbc profile-to-editor sip** command during the transition from SIP profile to SIP editor.



### Note

The **test sbc profile-to-editor sip** command only displays the editor that is inherited from the SIP profile for customers' reference when migrating from SIP profile to SIP editor. Customers must configure the editor manually using the **sip editor-type** command.

## Examples

The following is a sample output of the **test sbc profile-to-editor sip** command:

```
Router# test sbc profile-to-editor sip header-profile dtmf-notify

whitelist
  header event entry 1
  action pass
  header call-info entry 1
  action pass
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip</b> <i>editor-type</i>	Sets a default editor type to be applied to an adjacency that has not been explicitly set.

# test script-set

To perform live testing of script-based editors, use the **test script-set** command in the adjacency SIP configuration mode.

**test script-set** *script-set-number*

## Syntax Description

<i>script-set-number</i>	Script set number.
--------------------------	--------------------

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

The script set on which you run this command need not be the one that is currently active. The only criterion is that the script set must be one that is operational. In other words, when the **show sbc sbe script-set** command is run on the script set, the Status field must display `ok`.

## Examples

In the following example, the **test script-set** command is run on script set 10:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip my_adjacency
Router(config-sbc-sbe-adj-sip)# test script-set 10
```

## Related Commands

Command	Description
<b>active-script-set</b>	Activates a script set.
<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
<b>editor</b>	Specifies the order in which a particular editor must be applied.
<b>editor-list</b>	Specifies the stage at which the editors must be applied.

<b>Command</b>	<b>Description</b>
<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
<b>load-order</b>	Specifies the load order of a script in a script set.
<b>script</b>	Configures a script written using the Lua programming language.
<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.
<b>sip parameter-editor</b>	Configures a parameter editor.
<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
<b>type</b>	Specifies the type of a script written using the Lua programming language.

# tgid-context

To define trunk-group ID context and trunk-group ID values to match the entries of the routing table, use the **tgid-context** command in RTG routing table configuration mode. To delete the TGID values of the given entry in the routing table, use the no form of this command.

**tgid-context** *tgid-context-name* {**tgid** *tgid-name*}

**no tgid-context** *tgid-context-name* {**tgid** *tgid-name*}

## Syntax Description

<i>tgid-context-name</i>	Specifies trunk-group ID context to match on.
<i>tgid-name</i>	Specifies trunk-group ID to match on complete.

## Command Default

No default behavior or values are available.

## Command Modes

RTG routing table configuration (config-sbc-sbe-rtgpolicy-rtgtable-entry)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example configures the trunk-group ID context and trunk-group ID to match in the new routing table MyRtgTable:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# tgid-routing
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-trunk-group-id-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# action complete
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# dst-adjacency SIP-AS540-PSTN-GW2
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# match-type tgid
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# tgid-context example-domain tgid
trunkgroup1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)#
```



<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>call-policy-set</b>	Enters the mode of a routing policy configuration within an SBE entity.
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>rtg-src-trunk-group-id-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the source TGID or TGID context parameters of an SBE policy set.
	<b>rtg-dst-trunk-group-id-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the destination TGID or TGID context parameters of an SBE policy set.
	<b>tgid-routing</b>	Enables parsing the trunk-group identifier for call routing.

# tgid-routing

To enable parsing the trunk-group identifier for call routing, use the **tgid-routing** command in adjacency SIP configuration mode. Use the **no** form of this command to disable the parsing.

**tgid-routing**

**no tgid-routing**

**Command Default** No default behavior or values are available.

**Command Modes** Adjacency SIP configuration (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following command enables parsing the trunk-group identifier for call routing.

```
Router# configure terminal
Router(config)# sbc mysvc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# tgid-routing
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)#
```

Related Commands	Command	Description
	<b>sbc</b>	Creates a new SBC service and enters a new SBC configuration mode. Alternatively, enters the configuration mode of an existing service.
	<b>sbe</b>	Enters the mode of an SBE entity within an SBC service.
	<b>rtg-src-trunk-group-id-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the source TGID or TGID context parameters of an SBE policy set.
	<b>rtg-dst-trunk-group-id-table</b>	Enters the configuration mode of an existing routing table or creates a new table whose entries match the destination TGID or TGID context parameters of an SBE policy set.

# time-offset

Use the time-offset specified by the **timezone-offset** command. To disable using the time-offset specified by the **timezone-offset** command, use the **no** form of this command.

**time-offset hour hr min min** [*negative*]

**no time-offset**

Syntax Description	hr:hour_offset	Range: h: -23 to +23
	min: minute_offset	Range: m: -59 to +59
	negative	Specifies behind the local time.

**Command Default** No default behavior or values are available.

**Command Modes** RTG routing table entry configuration (config-sbc-sbe-rtgpolicy-rtgtable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Without this command the time-offset specified by the **timezone-offset** command under the SBE configuration mode is unused.

**Examples** The following example shows how to configure the destination adjacency of an entry in the new routing table MyRtgTable to softswitch1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# use-time-offset
```

Related Commands	Command	Description
	<b>timezone-offset</b>	Configures the number of hours and minutes that the desired time zone is ahead of or behind the local time.

# timeout

To define the length of time that packets from the source are blocked if the number of authentication requests exceed the set limit, use the **timeout** command in blacklist reason mode. The **no** form of this command releases the limit duration for blacklisting the source.

**timeout** *time-period*

**no timeout**

<b>Syntax Description</b>	<i>time-period</i>	Duration for which the source is blacklisted after activation of blacklisting. <ul style="list-style-type: none"> <li>• 0 = source not blacklisted</li> <li>• never = blacklisting is permanent</li> <li>• number {<b>milliseconds</b>   <b>seconds</b>   <b>minutes</b>   <b>hours</b>   <b>days</b>}</li> </ul> <p><b>Note</b> Period must be less than 23 days.</p>
---------------------------	--------------------	--

<b>Command Default</b>	<ul style="list-style-type: none"> <li>• The address-default value defaults to its initial settings. The port-default values default to zero.</li> <li>• If this field is omitted on explicit ports, it defaults to the value given in the port-default for this address.</li> <li>• If this field is omitted on explicit addresses, this field defaults to the value in the address-default for this address.</li> <li>• If this field is omitted for VPN, it defaults to the value for global addresses.</li> <li>• If this field is omitted for the global address space, it defaults to the initial settings.</li> </ul>
------------------------	--

<b>Command Modes</b>	Blacklist address-default mode (config-sbc-sbe-blacklist-addr-default-reason) Blacklist global mode (config-sbc-sbe-blacklist-global-reason) Blacklist ipv4 mode (config-sbc-sbe-blacklist-ipv4-reason) Blacklist vpn mode (config-sbc-sbe-blacklist-vpn-reason)
----------------------	---

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 2.4</td> <td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.
-------------------------	--

<b>Examples</b>	The following command configures a new blacklist on the SBE to affect all packets arriving from address 125.12.12.15 for three minutes:
-----------------	---

```

Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 125.12.12.15
Router(config-sbc-sbe-blacklist-ipv4)# reason authentication-failure
Router(config-sbc-sbe-blacklist-ipv4-reason)# timeout 180 seconds
Router(config-sbc-sbe-blacklist-ipv4-reason)# exit

```

Related Commands	Command	Description
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
	<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
	<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
	<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.
	<b>show sbc sbe blacklist</b>	Lists the limits in force for a particular source (whether they are from defaults or explicitly configured) in a form in which they can be entered into the CLI. Also listed are any defaults for a smaller scope configured at this address.
	<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# timezone-offset

To configure the number of hours and minutes that the desired time zone is ahead of or behind the local time, use the **timezone-offset** command in SBE configuration mode. To remove the time-zone offset, use the **no** form of this command.

**timezone-offset h:hour\_offset m: minute\_offset {positive | negative}**

**no timezone-offset h:hour\_offset m: minute\_offset**

## Syntax Description

<b>h:hour_offset</b>	Range: h: -23 to +23
<b>m: minute_offset</b>	Range: m:-59 to +59
positive	Specifies ahead of the local time.
negative	Specifies behind the local time.

## Command Default

*Zero is the default.*

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the offset timezone to 11 hours and 45 minutes behind the local time:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-domain-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# timezone-offset 11 45 negative
```

## Related Commands

Command	Description
<b>use-time-offset</b>	Uses the time-offset specified by the <b>timezone-offset</b> command.

# tls mutual authentication

To enable TLS Mutual Authentication on a SIP adjacency, use the *tls mutual-authentication* command. Use the **no** form of this command to disable TLS Mutual Authentication on a SIP adjacency.

**tls mutual-authentication**

**no tls mutual-authentication**

**Syntax Description** This command does not have any syntax or keywords.

**Command Default** TLS Mutual Authentication is disabled.

**Command Modes** Configure SBC SBE Adjacency SIP (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** This command helps the SBC to decide whether to send a CertificateRequest message to the client side to get the client's certificate for client authentication.

This configuration is valid only when the SBC acts as the TLS Server Side. When SBC acts as a TLS Client Side, you need not configure the SBC explicitly to respond to mutual authentication request.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following command enables TLS mutual-authentication on the SIP adjacency adj1:

```
Router# configure terminal
Router# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# tls mutual-authentication
Router(config-sbc-sbe)# exit
Router(config-sbc)# exit
```

# total resource maximum

To specify the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources, use the **total resource maximum** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

**total resource maximum** *number*

## Syntax Description

<i>number</i>	Maximum total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption.
---------------	--

## Command Default

The default weighted number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption at any point of time is 4294967295. When you use the **no** form of this command, any maximum limit set earlier is changed to this default value.

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the total resource number is set to 800. The maximum number of calls that can use audio transcoding, video transcoding, and SRTP interworking are also set in this example.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
Router(config-sbc-sbe-media-pol)# type cac-policy
Router(config-sbc-sbe-media-pol)# transcode audio maximum 200
Router(config-sbc-sbe-media-pol)# transcode video maximum 200
Router(config-sbc-sbe-media-pol)# interwork srtp maximum 500
Router(config-sbc-sbe-media-pol)# total resource maximum 800
```



Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# trace filter endpoint address ipv4 (session border controller)

To configure the trace filter for the H.248 Border Access Controller (BAC) on the Session Border Controller (SBC), use the **trace filter endpoint address ipv4** command in the H248 BAC configuration mode. To unconfigure the trace filter for the H.248 BAC, use the **no** form of this command.

**trace filter endpoint address ipv4** *ip-address port* [**vrf** *vrf-name*]

**no trace filter endpoint address ipv4** *ip-address port* [**vrf** *vrf-name*]

Syntax Description		
<i>ip-address</i>		IPv4 address of the endpoint for the trace filter on the SBC.
<i>port</i>		Port number of the endpoint for the trace filter on the SBC. Range: 1 to 65535.
<b>vrf</b>		Specifies virtual routing and forwarding (VRF) for the endpoint for the trace filter on the SBC.
<i>vrf-name</i>		Name of VRF.

**Command Default** None

**Command Modes** H248 BAC configuration (config-h248-bac)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** The *vrf-name* should match the name configured using the **ip vrf** command or the **ip vrf** forwarding command in the Gi interface.

To support VRF, enable Cisco Express Forwarding (CEF) switching on the router, using the **ip cef** command.

If you are also configuring the DHCP services at the access point name (APN), use the **dhcp-server ip-address vrf** command.

**Examples** The following example shows how to configure the trace filter for the H.248 BAC on the SBC:

```
Router> enable
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# trace filter endpoint address ipv4 10.0.0.1 245 vrf vrfex
```

# transcode-deny

To forbid transcoding for an entry in the admission control table, use the **transcode-deny** command in CAC table entry configuration mode. To allow transcoding for this entry in the admission control table, use the **no** form of this command.

**transcode-deny**

**no transcode-deny**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, transcoding for this entry in the admission control table is allowed.

**Command Modes** CAC table entry configuration (config-sbc-sbe-cacpolicy-cactable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to configure the entry to forbid transcoding in the new admission control table MyCacTable:

```
Router# config
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# cac-policy-set 1
Router(config-sbc-sbe-cacpolicy)# cac-table MyCacTable
Router(config-sbc-sbe-cacpolicy)# table-type limit dst-prefix
Router(config-sbc-sbe-cacpolicy-cactable)# entry 1
Router(config-sbc-sbe-cacpolicy-cactable-entry)# transcode-deny
```

# transcoder

To configure that the media gateway is a **transcoder**, use the **transcoder** command in media gateway codecs configuration mode. To return to the default behavior, use the **no** form of this command.

**transcoder**

**no transcoder**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, this command assumes the media gateway has no transcoding features.

**Command Modes** Media gateway codecs configuration (config-sbc-sbe-mg-codecs)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to set media gateway 10.0.0.1 to be a transcoder:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway ipv4 10.0.0.1
Router(config-sbc-sbe-mg)# codecs m=audio 1234 RTP/AVP 0 2 8 18,a=rtpmap:0
PCMU/8000,a=rtpmap:a=rtpmap:8 PCMA/8000,a=rtpmap:18 G729/80002 G72 6-32/8000,a=rtpmap:8
PCMA/8000,a=rtpmap:18 G729/8000
Router(config-sbc-sbe-mg-codecs)# transcoder
```

# transcode cost

To specify the resource cost for transcoding an audio or video stream, use the **transcode cost** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

**transcode {audio | video} cost** *number*

**no transcode {audio | video} cost**

## Syntax Description

<b>audio</b>	Specifies that the resource cost is to be set for an audio stream.
<b>video</b>	Specifies that the resource cost is to be set for a video stream.
<i>number</i>	Resource cost. The range is from 1 to 4294967295.

## Command Default

The default resource cost for transcoding an audio stream is 10. Similarly, the default resource cost for transcoding a video stream is 50. When you use the **no** form of this command, the resource cost is changed to the default value.

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the **transcode cost** command is used to set the resource cost for transcoding audio and video to 5 and 15, respectively.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway policy type remote ipv4 192.0.2.26 6886
Router(config-sbc-sbe-media-pol)# transcode audio cost 5
Router(config-sbc-sbe-media-pol)# transcode video cost 15
```

Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# transcode maximum

To specify the maximum number of audio or video streams that can use the transcoding resource, use the **transcode maximum** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

```
transcode {audio | video} maximum number
```

```
no transcode {audio | video} maximum
```

## Syntax Description

<i>number</i>	Maximum number of audio or video streams that can use the transcoding resource at any point of time.
---------------	--

## Command Default

The default number of audio or video streams that can use the transcoding resource, at any point of time, is 4294967295. When you use the **no** form of this command, any maximum limit set earlier is changed to this default value.

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the maximum number of media streams that can use audio transcoding is set to 200. Similarly, the maximum number of media streams that can use video transcoding is also set to 200.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
Router(config-sbc-sbe-media-pol)# type cac-policy
Router(config-sbc-sbe-media-pol)# transcode audio maximum 200
Router(config-sbc-sbe-media-pol)# transcode video maximum 200
```

Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.



# transcoding-stats enable

To enable the transcoding-related statistics on a router, use the **transcoding-stats enable** command in the Signaling Border Element (SBE) configuration mode. To disable the transcoding-related statistics, use the **no** form of this command.

**transcoding-stats enable**

**no transcoding-stats enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, the transcoding-related statistics are enabled.

**Command Modes** SBE configuration mode (config-sbc-sbe)

Command History	Release	Modification
	Cisco IOS XE Release 3.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to disable the transcoding-related statistics:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# no transcoding-stats enable
```

Related Commands	Command	Description
	<b>clear sbc sbe transcoding-stats</b>	Clears the voice transcoding-related statistics.
	<b>show sbc sbe transcoding-stats</b>	Displays the voice transcoding-related statistics.

# transcoding

To configure the transcoding options, use the **transcoding** command in virtual data border element (VDBE) configuration mode. To prevent the Session Border Controller (SBC) from performing a transcoding check of the incoming Session Description Protocol (SDP) and to disable the configuration, use the **no** form of this command.

**transcoding check** {**match** | **none** | **overlap**}

**no transcoding check**

## Syntax Description

<b>check</b>	Enables transcoding checking.
<b>match</b>	Specifies the exact codec matching check.
<b>none</b>	Specifies no codec matching check.
<b>overlap</b>	Specifies overlapping codec matching check.

## Command Default

By default, the **transcoding check overlap** command is configured.

## Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to disable the transcoding options in VDBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# transcoding check none
```

# translate (session border controller)

To configure IP-to-FQDN or FQDN-to-IP translation on signaling border elements (SBEs), use the **translate** command in the adjacency SIP configuration mode.

```
translate {request-uri | to | from} {inbound | outbound} {ip-fqdn | fqdn-ip}
```

## Syntax Description

<b>request-uri</b>	Performs translation on Request-URI
<b>to</b>	Performs translation on To header
<b>from</b>	Performs translation on From header
<b>inbound</b>	Inbound direction
<b>outbound</b>	Outbound direction
<b>ip-fqdn</b>	Performs IP-to-FQDN translation
<b>fqdn-ip</b>	Performs FQDN-to-IP translation

## Command Default

SIP IP-FQDN translation is disabled

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure the IP-to-FQDN translation on Request-URI for inbound request:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# translate request-uri inbound ip-fqdn
Router(config-sbc-sbe-adj-sip)#
```

The following example shows how to configure the FQDN-to-IP translation on To header for outbound request:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# translate to outbound fqdn-ip
```

The following example shows how to configure the FQDN-to-IP translation on From header for inbound request:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# sbc test
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip adj1
Router(config-sbc-sbe-adj-sip)# translate from inbound fqdn-ip
```

## transport (session border controller)

To configure a data border element (DBE) to use either UDP or TCP for H.248 control signaling with the specified H.248 controller and to configure the Interim Authentication Header (IAH) to authenticate and check the integrity of packets, use the **transport** command in Controller H.248 configuration mode. To remove the configuration, use the **no** form of this command.

```
transport {udp | tcp} [interim-auth-header] [ah-md5-hmac | ah-sha-hmac]
```

```
no transport
```

Syntax Description	
<b>udp</b>	Specifies UDP transport for H.248 signaling with the H.248 controller. UDP is the default if the <b>transport</b> command is not used.
<b>tcp</b>	Specifies TCP transport for H.248 signaling with the H.248 controller.
<i>interim-auth-header</i>	(Optional) Specifies the H.248 controller should insert the interim authentication header into the H.248 messages to authenticate packets and provide security.  If you specify the <b>interim-auth-header</b> keyword, but do not specify either <b>ah-md5-hmac</b> or <b>ah-sha-hmac</b> type of authentication, then the DBE uses zero authentication where the interim authentication header is inserted in the packet and all fields in the IAH header are set to zeroes. The DBE checks the packet syntactically, however, the DBE does not authenticate whether there is an IAH header or if it's correct.
ah-md5-hmac	Specifies the DBE uses for packet authentication the hashing scheme, HMAC-MD5 (Hashing for Message Authentication-Message Digest 5). Enters into IAH Key configuration mode. MD5 produces a 128 bit hash value.  If you specify a hashing scheme, you need to configure <b>inbound</b> and <b>outbound</b> options for incoming and outgoing packets, as well as specify the Security Parameters Index (SPI) and hex-key. See the <b>inbound</b> and <b>outbound</b> commands for more details.
ah-sha-hmac	Specifies the DBE uses for packet authentication the hashing scheme, HMAC-SHA (Hashing for Message Authentication-Secure Hash Algorithm). Enters into IAH Key configuration mode. SHA-1 produces a message digest that is 160 bits long.  If you specify a hashing scheme, you need to configure <b>inbound</b> and <b>outbound</b> options for incoming and outgoing packets, as well as specify the Security Parameters Index (SPI) and hex-key. See the <b>inbound</b> and <b>outbound</b> commands for more details.

**Command Default** If the **transport** command is not specified, UDP transport is used for H.248 signaling.

**Command Modes** Controller H.248 configuration (config-sbc-dbe-vdbe-h248)

**Command History**

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	The <b>ah-md5-hmac</b> and <b>ah-sha-hmac</b> keywords were added.

**Usage Guidelines**

The **transport (session border controller)** command is used in conjunction with the **inbound** and **outbound** commands. The three commands are used together to enable Interim Authentication Header (IAH) authentication of inbound and outbound call packets. If you specify a hashing scheme (**ah-md5-hmac** or **ah-sha-hmac** authentication) using the **transport (session border controller)** command, you need to configure incoming and outgoing call packets using both **inbound** and **outbound** commands. The **inbound** and **outbound** commands are used to specify the Security Parameters Index (SPI) and hex-key.

MD5 hashing is faster to calculate, but provides less secure authentication than SHA hashing does. The hash calculation includes a synthesized IP header consisting of a 32 bit source IP address, a 32 bit destination address, and a 16 bit UDP or TCP destination port encoded as 20 hexadecimal digits.

For the MD5 or SHA hashing scheme to work, both inbound and outbound SPI need to be configured. If only the inbound or outbound SPI key or neither inbound or outbound SPI key is configured, the authentication reverts back to zero authentication and the DBE issues a warning message “Both inbound and outbound keys must be configured to enable authentication.” In this event, the DBE sets all fields in the IAH header to zeroes and accepts any IAH without authentication.

**Examples**

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, creates an H.248 controller with index 1, enters into Controller H.248 configuration mode, and configures the H.248 controller to use TCP as the transport:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# transport tcp
Router(config-sbc-dbe-vdbe-h248)# end
```

The following example shows you how to configure the DBE to specify TCP for H.248 control signaling, and to configure the IAH to use the HMAC-SHA hashing scheme, set the inbound Security Parameters Index (SPI) to 300 and the outbound SPI to 400, and hash key to “myInboundKey45” and “myOutboundKey89” respectively:

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# local-port 2970
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.40
Router(config-sbc-dbe-vdbe)# controller h248 2
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254
Router(config-sbc-dbe-vdbe-h248)# remote-port 2970
Router(config-sbc-dbe-vdbe-h248)# transport tcp interim-auth-header ah-sha-hmac
Router(config-sbc-dbe-vdbe-h248-iah)# inbound 300 myInboundKey45
Router(config-sbc-dbe-vdbe-h248-iah)# outbound 400 myOutboundKey89
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers
```

Related Commands	Command	Description
	<b>inbound</b>	Configures inbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an incoming packet is bound when the Interim Authentication Header (IAH) is enabled.
	<b>outbound</b>	Configures outbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an outgoing packet is bound when the Interim Authentication Header (IAH) is enabled.

# transport (SBE H.248)

To configure an SBE to use a transport for H.248 communications when acting as a media gateway controller, use the **transport** command in H.248 control address mode. To delete a given IPv4 H.248 transport, use the **no** form of this command.

**transport** [tcp | udp]

**no transport** [tcp | udp]

## Syntax Description

<b>udp</b>	Configures the UDP transport for H.248 signaling.
<b>vrf</b> <i>vrf name</i>	Configures the VRF name for H.248 association.

## Command Default

No default behavior or values are available.

## Command Modes

H.248 control address (config-sbc-sbe-ctrl-h248)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following example shows how to configure an SBE to use udp transport:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc-sbe)# control address h248 index 0
Router(config-sbc-sbe-ctrl-h248)# ipv4 1.1.1.1
Router(config-sbc-sbe-ctrl-h248)# transport udp
```

## Related Commands

Command	Description
<b>control address h248 index</b>	Selects index value and enters H.248 control address mode.
<b>ipv4 (SBE H.248)</b>	Configures an SBE to use a given IPv4 H.248 control address.
<b>port (SBE H.248)</b>	Configures an SBE to use a given IPv4 H.248 port.



# transrate audio cost

To specify the resource cost for transrating an audio stream, use the **transrate audio cost** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

**transrate audio cost** *number*

**no transrate audio cost**

## Syntax Description

<i>number</i>	Resource cost. The range is from 1 to 4294967295.
---------------	---

## Command Default

The default resource cost for transrating an audio stream is 6. Similarly, the default resource cost for transcoding a video stream is 50. When you use the **no** form of this command, the resource cost is changed to the default value.

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the **transrate audio cost** command is used to set the resource cost for transrating audio to 10.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-gateway policy type local
Router(config-sbc-sbe-media-pol)# transrate audio cost 10
```

Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# transrate audio maximum

To specify the maximum number of audio streams that can use the transrating resource, use the **transrate** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

**transrate audio maximum** *number*

**no transrate audio maximum**

## Syntax Description

<i>number</i>	Maximum number of audio streams that can use the transrating resource at any point of time.
---------------	---

## Command Default

The default number of audio streams that can use the transrating resource, at any point of time, is 4294967295. When you use the **no** form of this command, any maximum limit set earlier is changed to this default value.

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the maximum number of audio streams that can use the transrating resource is set to 300:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
Router(config-sbc-sbe-media-pol)# type cac-policy
Router(config-sbc-sbe-media-pol)# transrate audio maximum 300
```

Related Commands	Command	Description
	<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
	<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.
	<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
	<b>media-gateway policy type</b>	Configures a media gateway policy.
	<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
	<b>media-policy</b>	Configures a media policy.
	<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
	<b>show sbc sbe media-policy</b>	Displays the details of media policies.
	<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
	<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
	<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
	<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
	<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
	<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# transrating

To configure the transrating options, use the **transrating** command in controller H.248 configuration mode. To prevent the Session Border Controller (SBC) from performing a transrating check of the incoming Session Description Protocol (SDP) to disable the configuration, use the **no** form of this command.

```
transrating /check [none | remote] | exit/
```

```
no transrating check
```

Syntax Description	check	Enables transrating checking.
	exit	Exits from the sbc-dbe-vdbe-h248 configuration mode.
	none	Specifies no transrating matching check.
	remote	Specifies remote descriptor matching check.

**Command Default** By default, the **transrating check none** command is configured. After the **associate dspfarm profile** command is also configured, transrating check remote becomes the default configuration.

**Command Modes** Controller H.248 configuration (sbc-dbe-vdbe-h248)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Examples** The following example shows how to disable the transrating options in virtual data border element (VDBE) configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# no transrating check
```

Related Commands	Command	Description
	<b>controller h248</b>	Configures an H.248 controller for a data border element (DBE).

# trigger-period

To define the period over which events are considered, use the **trigger-period** command in blacklist reason mode. For more detailed information, see the related **trigger-size** command description.

The **no** form of this command releases the previously configured trigger period in which events should be considered.

**trigger-period** *time*

**no trigger-period**

## Syntax Description

<i>time</i>	The number of milliseconds for the trigger period. This can be any value from 0 to 65535.
-------------	---

## Command Default

- The address-default value defaults to its initial settings. The port-default values default to zero.
- If this field is omitted on explicit ports, it defaults to the value given in the port-default for this address.
- If this field is omitted on explicit addresses, this field defaults to the value in the address-default for this address.
- If this field is omitted for VPN, it defaults to the value for global addresses.
- If this field is omitted for the global address space, it defaults to the initial settings.

## Command Modes

Blacklist address-default mode (config-sbc-sbe-blacklist-addr-default-reason)

Blacklist global mode (config-sbc-sbe-blacklist-global-reason)

Blacklist ipv4 mode (config-sbc-sbe-blacklist-ipv4-reason)

Blacklist vpn mode (config-sbc-sbe-blacklist-vpn-reason)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

## Examples

The following command configures the source to be blacklisted if authentication failures have occurred at a recent steady rate of over 200 per second (or 40 in a 100-ms burst):

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
```

```

Router(config-sbc-sbe-blacklist)# ipv4 125.12.12.15
Router(config-sbc-sbe-blacklist-ipv4)# reason authentication-failure
Router(config-sbc-sbe-blacklist-ipv4-reason)# trigger-period 100 milliseconds
Router(config-sbc-sbe-blacklist-ipv4-reason)# exit

```

Related Commands	Command	Description
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
	<b>trigger-size</b>	Defines the number of the specified events from the specified source that are allowed before the blacklisting is triggered, and blocks all packets from the source.
	<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
	<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.
	<b>show sbc sbe blacklist</b>	Lists the limits in force for a particular source (whether they are from defaults or explicitly configured) in a form in which they can be entered into the CLI. Also listed are any defaults for a smaller scope configured at this address. Values not explicitly configured (and therefore inherited from other defaults) are bracketed.
	<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# trigger-size

To define the allowable number of events from the specified source before blacklisting is triggered, and to block all packets from reaching the source, use the **trigger-size** command in blacklist reason mode.

The **no** form of this command releases the previously configured number of allowable events before blacklisting is triggered.

**trigger-size** *number*

**no trigger-size**

## Syntax Description

<i>number</i>	The minimum number of consecutive events that must occur faster on average than the trigger rate to activate the blacklist. Can be any value from 0 to 65535.
---------------	---

## Command Default

- The address-default value defaults to its initial settings. The port-default values default to zero.
- If this field is omitted on explicit ports, it defaults to the value given in the port-default for the given address.
- If this field is omitted on explicit addresses, it defaults to the value given in the address-default for the given address.
- If this field is omitted for VPN, it defaults to the values of global addresses.
- If this field is omitted for the global address space, it defaults to the initial settings.

## Command Modes

Blacklist address-default mode (config-sbc-sbe-blacklist-addr-default-reason)

Blacklist global mode (config-sbc-sbe-blacklist-global-reason)

Blacklist ipv4 mode (config-sbc-sbe-blacklist-ipv4-reason)

Blacklist vpn mode (config-sbc-sbe-blacklist-vpn-reason)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The number of events recorded decays linearly to zero to give a leaky bucket average over the trigger period. The steady-state maximum event rate therefore equals this trigger size divided by the trigger period. See also the description of the **trigger-period** command. The maximum number of events in a much shorter period is this trigger size.

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



**Examples**

The following command configures the source to be blacklisted if a burst of more than 20 authentication failures enter within a time period smaller than the trigger period:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 125.12.12.15
Router(config-sbc-sbe-blacklist-ipv4)# reason authentication-failure
Router(config-sbc-sbe-blacklist-ipv4-reason)# trigger-size 20
Router(config-sbc-sbe-blacklist-ipv4-reason)# exit
```

**Related Commands**

Command	Description
<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source (in other words, a port, IP address, VPN, global address space).
<b>trigger-period</b>	Defines the period over which events are considered. For details, see the description of the trigger-size command.
<b>timeout</b>	Defines the length of time that packets from the source are blocked, should the limit be exceeded.
<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured. Any values not explicitly defined for each source are in brackets.
<b>show sbc sbe blacklist</b>	Lists the limits in force for a particular source (whether they are from defaults or explicitly configured) in a form in which they can be entered into the CLI. Also listed are any defaults for a smaller scope configured at this address. Values not explicitly configured (and therefore inherited from other defaults) are bracketed.
<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# trunk trusted

To configure an H.323 adjacency as trusted, use the **trunk trusted** command in the H.323 Adjacency configuration mode. To change an H.323 adjacency to untrusted, use the **no** form of this command.

**trunk trusted**

**no trunk trusted**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, all the H.323 adjacencies are untrusted.

**Command Modes** H.323 Adjacency configuration mode (config-sbc-sbe-adj-h323)

## Command History

Release	Modification
3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

The Secure SIP calls over an H.323 interface is implemented logically by defining the H.323 adjacency as trusted using the **trunk trusted** command in the H.323 Adjacency configuration mode. By default, all the H.323 adjacencies are untrusted.



### Note

SBC does not signal secure H.323 calls using the procedures described in H.235. Moreover, the SBC does not use a TLS or IPSec connection to send call signalling for the secure H.323 calls.

To mark an H.323 adjacency as untrusted, use the **no trunk trusted** command from the H.323 Adjacency configuration mode.



### Note

To change an H.323 adjacency from trusted to untrusted, configure the inbound calls as insecure using the **no inbound secure** command.

## Examples

The following example shows how to configure an H.323 adjacency as trusted, which is helpful to handle the Secure SIP calls received from a SIP adjacency and routed to an H.323 adjacency:

```
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h.323 trust-h323-adj
Router(config-sbc-sbe-adj-h323)# trunk trusted
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>inbound secure</b>	Configures the incoming calls from an H.323 adjacency as secure calls.

# type (media policy)

To configure a media policy as a CAC-policy type policy or a gateway type policy, use the **type** command in the SBE media policy configuration mode. To remove this configuration, use the **no** form of this command.

**type** {cac-policy | gateway}

**no type** {cac-policy | gateway}

## Syntax Description

<b>cac-policy</b>	Specifies that the media policy is a CAC-policy type policy.
<b>gateway</b>	Specifies that the media policy is a gateway type policy.

## Command Default

No default behavior or values are available.

## Command Modes

SBE media policy configuration (config-sbc-sbe-media-pol)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

## Examples

In the following example, the **type** command is used to specify that the media policy table is of the gateway type:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# media-policy my_media_policy
Router(config-sbc-sbe-media-pol)# type gateway
```

## Related Commands

Command	Description
<b>interwork maximum</b>	Specifies the maximum number of media streams that can use the inband DTMF interworking resource or the SRTP interworking resource at any point of time.
<b>interwork cost</b>	Specifies the resource cost for an audio stream using inband DTMF interworking or specifies the resource cost for an audio or video stream using SRTP encryption and decryption.

<b>Command</b>	<b>Description</b>
<b>ipsec maximum</b>	Specifies the maximum number of endpoint registrations that can use IPsec encryption and decryption on their signaling link to the SBC or the maximum number of calls that can use IPsec-protected signaling, at any point of time.
<b>media-gateway policy type</b>	Configures a media gateway policy.
<b>media limits</b>	Specifies the media policy to be associated with the CAC policy table entry or applied on the media gateway.
<b>media-policy</b>	Configures a media policy.
<b>show sbc sbe media-gateway-policy</b>	Displays the details of media gateway policies.
<b>show sbc sbe media-policy</b>	Displays the details of media policies.
<b>total resource maximum</b>	Specifies the total number of video and audio streams that can use transcoding, transrating, inband DTMF interworking, and SRTP encryption and decryption—weighted by the costs assigned to each of these resources.
<b>transcode cost</b>	Specifies the resource cost for transcoding an audio or video stream.
<b>transcode maximum</b>	Specifies the maximum number of audio or video streams that can use the transcoding resource at any point of time.
<b>transrate audio cost</b>	Specifies the resource cost for transrating an audio stream.
<b>transrate audio maximum</b>	Specifies the maximum number of audio streams that can use the transrating resource at any point of time.
<b>type</b>	Configures a media policy as a CAC-policy type policy or a gateway type policy.

# type (script)

To specify the type of a script written using the Lua programming language, use the **type** command in the SBE script-set script configuration mode. To set the type to the default type (full), use the **no** form of this command.

**type {full | wrapped edit-point {after-send | before-receive | both}}**

**no type**

## Syntax Description

<b>full</b>	Specifies a full script and that there is no autogeneration.
<b>wrapped</b>	Specifies that the script must be autogenerated from the file.
<b>edit-point</b>	Specifies the edit point that is used in autoregistration.
<b>after-send</b>	Specifies that the outgoing message must be edited after the message is processed by the adjacency and just before it is forwarded from the adjacency.
<b>before-receive</b>	Specifies that the incoming message must be edited just after it is received on the adjacency and before the adjacency begins processing it.
<b>both</b>	Enables editing of the SBC message both after it is sent and before it is received.

## Command Default

The default type is full.

## Command Modes

SBE script-set script configuration (config-sbc-sbe-scrpset-script)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced on the Cisco ASR 100 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run this command.

## Examples

In the following example, the **type** command specifies that the script is to be autogenerated from the file and that the edit points for editing the message are both after the message is sent and before it is received:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# script-set 10 lua
Router(config-sbc-sbe-script-set)# script mySBCScript.lua
Router(config-sbc-sbe-scrpset-script)# load-order 2
Router(config-sbc-sbe-scrpset-script)# type wrapped edit-point both
```

Related Commands	Command	Description
	<b>active-script-set</b>	Activates a script set,
	<b>clear sbc sbe script-set-stats</b>	Clears the stored statistics related to a script set.
	<b>complete</b>	Completes a CAC policy set, call policy set, or script set after committing the full set.
	<b>editor</b>	Specifies the order in which a particular editor must be applied.
	<b>editor-list</b>	Specifies the stage at which the editors must be applied.
	<b>editor type</b>	Configures an editor type to be applied on a SIP adjacency.
	<b>filename</b>	Specifies the path and name of the script file written using the Lua programming language.
	<b>load-order</b>	Specifies the load order of a script in a script set.
	<b>script</b>	Configures a script written using the Lua programming language.
	<b>show sbc sbe editors</b>	Displays a list of all the editors registered on the SBC.
	<b>show sbc sbe script-set</b>	Displays a summary of the details pertaining to all the configured script sets or the details of a specified script set.
	<b>script-set lua</b>	Configures a script set composed of scripts written using the Lua programming language.
	<b>sip header-editor</b>	Configures a header editor.
	<b>sip method-editor</b>	Configures a method editor.
	<b>sip option-editor</b>	Configures an option editor.
	<b>sip parameter-editor</b>	Configures a parameter editor.
	<b>test sbc message sip filename script-set editors</b>	Tests the message editing functionality of the SBC.
	<b>test script-set</b>	Tests the working of a script set.

# udp-first-retransmit-interval

To configure the time that the SBC waits for a UDP response or ACK before sending a retransmission of the relevant signal, use the **udp-first-retransmit-interval** command in SIP timer mode. To return to the default value, use the **no** form of this command.

**udp-first-retransmit-interval** *interval*

**no udp-first-retransmit-interval** *interval*

<b>Syntax Description</b>	<i>interval</i>	Time to wait, in milliseconds, before sending the first retransmission of a UDP signal.
---------------------------	-----------------	---

**Command Default** Default interval is 500 milliseconds

**Command Modes** SIP timer (config-sbc-sbe-sip-tmr)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.1S	This command and the <b>udp-max-retransmit-interval</b> command were together replaced by the <b>udp-retransmit-interval</b> command on the Cisco ASR 1000 Series Aggregation Services Routers in a release earlier than Release 3.1S.  As mentioned in the Usage Guidelines section, the values of the <b>udp-first-retransmit-interval</b> command and the <b>udp-max-retransmit-interval</b> command are interdependent. There are defaults for these commands that are not at the extremes of the range of values for these commands. There may be valid combinations of these commands that would be rejected on reboot because the value of the first command in a pair of these commands may be configured beyond the default value of the other command. The introduction of the <b>udp-retransmit-interval</b> command addresses this issue.

## Usage Guidelines

The interval set by the **udp-first-retransmit-interval** command corresponds to the T1 interval detailed in RFC 3261. Similarly, the interval set by the **udp-max-retransmit-interval** command corresponds to the T2 interval detailed in the same RFC. The SBC uses these two intervals as follows:

- If the SBC sends an INVITE request and does not receive a response, the retransmission interval is first set to **udp-first-retransmit-interval** (T1) and then doubled each time until the interval reaches 64 times T1.
- If the SBC sends a non-INVITE request and does not receive a response, the retransmission interval is first set to **udp-first-retransmit-interval** (T1) and then doubled each time until the interval reaches **udp-max-retransmit-interval** (T2).



- If the SBC sends 300(INVITE) to 699(INVITE) response and does not receive an ACK, the retransmission interval is first set to `udp-first-retransmit-interval` (T1) and then doubled each time until the interval reaches `udp-max-retransmit-interval` (T2).

To use the **udp-first-retransmit-interval** command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

---

### Examples

The following command configures the SBC to send the first UDP retransmission after waiting for 1000 milliseconds.

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# udp-first-retransmit-interval 1000
Router(config-sbc-sbe-sip-tmr)# exit
```

# udp-max-retransmit-interval

To configure the maximum interval at which the SBC will retransmit, use the **udp-max-retransmit-interval** command in SIP timer mode. To return to the default value, use the **no** form of this command.

**udp-max-retransmit-interval** *interval*

**no udp-max-retransmit-interval** *interval*

## Syntax Description

<i>interval</i>	Maximum retransmission interval, in milliseconds.
-----------------	---

## Command Default

Default interval is 4000 milliseconds.

## Command Modes

SIP timer (config-sbc-sbe-sip-tmr)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.1S	This command and the <b>udp-first-retransmit-interval</b> command were together replaced by the <b>udp-retransmit-interval</b> command on the Cisco ASR 1000 Series Aggregation Services Routers in a release earlier than Release 3.1S.  As mentioned in the Usage Guidelines section, the values of the <b>udp-first-retransmit-interval</b> command and the <b>udp-max-retransmit-interval</b> command are interdependent. There are defaults for these commands that are not at the extremes of the range of values for these commands. There may be valid combinations of these commands that would be rejected on reboot because the value of the first command in a pair of these commands may be configured beyond the default value of the other command. The introduction of the <b>udp-retransmit-interval</b> command addresses this issue.

## Usage Guidelines

The interval set by the **udp-first-retransmit-interval** command corresponds to the T1 interval detailed in RFC 3261. Similarly, the interval set by the **udp-max-retransmit-interval** command corresponds to the T2 interval detailed in the same RFC. The SBC uses these two intervals as follows:

- If the SBC sends an INVITE request and does not receive a response, the retransmission interval is first set to **udp-first-retransmit-interval** (T1) and then doubled each time until the interval reaches 64 times T1.
- If the SBC sends a non-INVITE request and does not receive a response, the retransmission interval is first set to **udp-first-retransmit-interval** (T1) and then doubled each time until the interval reaches **udp-max-retransmit-interval** (T2).

- If the SBC sends 300(INVITE) to 699(INVITE) response and does not receive an ACK, the retransmission interval is first set to `udp-first-retransmit-interval` (T1) and then doubled each time until the interval reaches `udp-max-retransmit-interval` (T2).

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

---

### Examples

The following command sets the maximum retransmission interval to 8000 milliseconds:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# udp-max-retransmit-interval 8000
Router(config-sbc-sbe-sip-tmr)# exit
```

# udp-response-linger-period

To configure the period for which SBC will retain negative UDP responses to INVITE requests, use the **udp-response-linger-period** command in SIP timer mode. To return to the default value, use the **no** form of this command.

**udp-response-linger-period** *interval*

**no udp-response-linger-period** *interval*

<b>Syntax Description</b>	<i>interval</i>	The time to retain negative INVITE responses, in milliseconds.
---------------------------	-----------------	--

<b>Command Default</b>	Default interval is 32 seconds.	
------------------------	---------------------------------	--

<b>Command Modes</b>	SIP timer (config-sbc-sbe-sip-tmr)	
----------------------	------------------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.	
-------------------------	--	--

<b>Examples</b>	The following command sets negative INVITE responses to be retained for 10 seconds:	
-----------------	---	--

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# udp-response-linger-period 10000
Router(config-sbc-sbe-sip-tmr)# exit
```

# udp-retransmit-interval

To configure the time that the session border controller (SBC) waits for a UDP response or ACK before sending a retransmission of the relevant signal and the maximum interval up to which the SBC will retransmit, use the **udp-retransmit-interval** command in SIP timer mode. To return to the default value of the retransmit time and interval, use the **no** form of this command.

**udp-retransmit-interval** [**first** *first-interval*] [**maximum** *max-interval*]

**no udp-retransmit-interval** [**first**] [**maximum**]

Syntax Description	first	Specifies the time to wait before sending the first retransmission of a UDP signal.
	<i>first-interval</i>	Time to wait, in milliseconds, before sending the first retransmission of a UDP signal. This interval corresponds to the T1 interval detailed in RFC 3261. The default is 500.
	<b>maximum</b>	Specifies the maximum interval, in milliseconds, up to which the SBC will retransmit.
	<i>max-interval</i>	Time to wait, in milliseconds, before sending the first retransmission of a UDP signal. This interval corresponds to the T2 interval detailed in RFC 3261. The default is 4000.

**Command Default** The default is that the SBC waits for 500 milliseconds before first retransmitting and then continues retransmitting at every 500 milliseconds intervals for up to 4000 milliseconds.

**Command Modes** SIP timer (config-sbc-sbe-sip-tmr)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 3.1S	This command was introduced in a release earlier than Release 3.1S. This command replaces the <b>udp-first-retransmit-interval</b> command and the <b>udp-max-retransmit-interval</b> command.

**Usage Guidelines** The interval set by the *first-interval* argument of the command corresponds to the T1 interval detailed in RFC 3261. Similarly, the interval set by the *max-interval* argument of the command corresponds to the T2 interval detailed in the same RFC. The SBC uses these two intervals as follows:

- If the SBC sends an INVITE request and does not receive a response, the retransmission interval is first set to T1 and then doubled each time until the interval reaches 64 times T1.
- If the SBC sends a non-INVITE request and does not receive a response, the retransmission interval is first set to T1 and then doubled each time until the interval reaches T2.

- If the SBC sends 300(INVITE) to 699(INVITE) response and does not receive an ACK, the retransmission interval is first set to T1 and then doubled each time until the interval reaches T2.

To use the **udp-retransmit-interval** command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

---

## Examples

The following command configures the SBC to send the first UDP retransmission after waiting for 500 milliseconds and to continue retransmission up to 8000 milliseconds:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip timer
Router(config-sbc-sbe-sip-tmr)# udp-retransmit-interval first 500 maximum 8000
Router(config-sbc-sbe-sip-tmr)# exit
```

# udp (blacklist)

To enter the mode for configuring blacklisting for UDP protocol only, use the **udp** command in the SBE blacklist IPv4 configuration mode.

*udp port number*

<b>Syntax Description</b>	<i>port number</i>	Port number to blacklist. Range is 0-65535.
---------------------------	--------------------	---

**Command Default** No default behavior or values are available.

**Command Modes** SBE blacklist IPv4 configuration (config-sbc-sbe-blacklist-ipv4)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how to enter the mode for configuring blacklisting for UDP protocol only:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# ipv4 1.1.1.1
Router(config-sbc-sbe-blacklist-ipv4)# udp 1
Router(config-sbc-sbe-blacklist-ipv4-udp)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>blacklist</b>	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	<b>address-default</b>	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	<b>clear sbc sbe blacklist</b>	Clears the blacklist for the specified SBC service.
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source.

# unexpected-source-alerting (session border controller)

To enable the generation of alerts when media packets for a call are received from an unexpected source address and port, use the **unexpected-source-alerting** command in VDBE configuration mode. Use the **no** form of this command to delete the unexpected-source-alerting.

**unexpected-source-alerting**

**no unexpected-source-alerting**

**Syntax Description** This command has no arguments or keywords.

**Command Default** If the **unexpected-source-alerting** command is not specified, unexpected source alerting is disabled.

**Command Modes** VDBE configuration (config-sbc-dbe-vdbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The **vdbe unexpected-source-alerting** command should be enabled only on trusted networks, where any occurrence of packets from an unexpected source might indicate a threat to network security.

Alerts on the same flow and the total number of alerts reported at any one time are both rate-limited to ensure management systems are not flooded with reports. (As a result, there is not a one-to-one correspondence between alerts and incorrect packets.)

Diagnosing and resolving the issue of rogue packets is beyond the scope of SBC function; SBC simply serves as the messenger to notify you of the existence of the rogue packets.

Any and all packets from unexpected sources are dropped.

## Examples

The following example creates a DBE service on an SBC called mySbc, enters into DBE configuration and VDBE configuration modes, and enables the generation of alerts when unexpected source address packets are received by a virtual data border element (vDBE):

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# unexpected-source-alerting
Router(config-sbc-dbe-vdbe)# exit
```

## Related Commands

Command	Description
<b>vdbe</b>	Enters into VDBE configuration mode.



## uri username parameters parse

To parse and search the user names in the SIP and SIPS URIs for the user name parameters, use the **uri username parameters parse** command in SBC SBE Adjacency SIP mode. Use the **no** form of this command to disable parsing.

**uri username parameters parse**

**no uri username parameters parse**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** SBC SBE Adjacency SIP (config-sbc-sbe-adj-sip)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** User name parameters in SIP and SIPS URIs in messages received on an adjacency are treated as regular URI parameters. The username is taken to exclude the username parameters. This applies to SIP and SIPS URIs within the Request-URI, and the To and From headers for INVITE requests and out-of-dialog requests.

**Examples** *The following command parses the SIP and SIPS URIs in messages received on the adjacency mySIP:*

```
Router# config terminal
Router(config)# sbc mySBC
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip mySIP
Router(config-sbc-sbe-adj-sip)# uri username parameters parse
```

# use-any-local-port

To configure a DBE to use any available local port when connecting to the default Media Gateway Control (MGC), use the **use-any-local-port** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

**use-any-local-port**

**no use-any-local-port**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The default behavior is to use any local port.

**Command Modes** VDBE configuration (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** The local port cannot be modified once any controller has been configured on the vDBE. You must delete the controller before you can modify or configure the local port.



**Note**

Do not use the **use-any-local-port** command when there is a redundant SBC because the connection to the MGC may be lost with an SBC switch over.

**Examples** The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures the DBE to use any local port:

```
Router# configure terminal
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# use-any-local-port
Router(config-sbc-dbe-vdbe)# exit
```

Related Commands	Command	Description
	<b>local-port</b>	Configures a DBE to use a specific local port when connecting to the default Media Gateway Control (MGC).

# use-time-offset

Use the time-offset specified by the **timezone-offset** command. To disable using the time-offset specified by the **timezone-offset** command, use the **no** form of this command.

**use-time-offset time-offset**

**no use-time-offset**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes** RTG routing table entry configuration (config-sbc-sbe-rtgpolicy-rtgtable-entry)

Command History	Release	Modification
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

Without this command the time-offset specified by the **timezone-offset** command under the SBE configuration mode is unused.

**Examples** The following example shows how to configure the destination adjacency of an entry in the new routing table MyRtgTable to softswitch1:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# call-policy-set 1
Router(config-sbc-sbe-rtgpolicy)# rtg-dst-address-table MyRtgTable
Router(config-sbc-sbe-rtgpolicy-rtgtable)# entry 1
Router(config-sbc-sbe-rtgpolicy-rtgtable-entry)# use-time-offset
```

Related Commands	Command	Description
	<b>timezone-offset</b>	Configures the number of hours and minutes that the desired time zone is ahead of or behind the local time.

# variant

To define an encoded codec variant name, use the **variant** command in the Codec variant configuration mode. To remove an encoded codec variant name, use the **no** form of this command.

**variant** *variant-codec-encoded-name*

**no variant**

## Syntax Description

*variant-codec-encoded-name* The variant nonstandard codec string.

## Command Default

No default behavior or values are available.

## Command Modes

Codec variant configuration (config-sbc-sbe-codec-var-codec)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.



### Note

# is reserved for base variants. Therefore, the variant name cannot start with #

## Examples

The following example shows how to define the codec variant using the **variant** command in the Codec variant configuration mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant codec G723-H-1
Router(config-sbc-sbe-codec-var-codec)# variant G723-H-1
```

# variant (codec variant profile)

To add the variant name, use the **variant** command in the codec variant profile configuration mode. To remove the encoded codec variant name, use the **no** form of this command.

**variant** *variant-name*

**no variant** *variant-name*

## Syntax Description

<i>variant-name</i>	The variant nonstandard codec string. The <i>variant-name</i> can have a maximum of 30 characters which can include the underscore character (_) and alphanumeric characters.
<b>Note</b>	Except for the underscore character, do not use any special character to specify field names.

## Command Default

No default behavior or values are available.

## Command Modes

Codec variant profile configuration (config-sbc-sbe-codec-var-prf)

## Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.



### Note

'#' is reserved for base variants. Therefore, the variant name cannot start with '#'

## Examples

The following example shows how to add the codec variant using the **variant** command in the codec variant profile configuration mode:

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# codec variant profile profile-1
Router(config-sbc-sbe-codec-var-prof)# variant G723-H-1
```

# vdb (session border controller)

To enter into VDBE configuration mode, use the **vdb** command in SBC-DBE or SBE configuration mode. To delete the entire virtual data border element (vDBE) from the running configuration, use the **no** form of this command

```
vdb [global]
```

```
no vdb [global]
```

## Syntax Description

global	The name of the DBE that is configured. Only one DBE can be configured. This is given the name <i>global</i> . If specified, the DBE name must be <i>global</i> . If not specified, <i>global</i> is assumed.
--------	--

## Command Default

No default behavior or values are available.

## Command Modes

SBE configuration (config-sbc-sbe)

## Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.4	This command is supported in the unified model.

## Usage Guidelines

In the initial release only one DBE (the global DBE) is supported, and DBE resources cannot be partitioned. As such, the vdb name is not required. If specified it must be **global**.

## Examples

The following example enters into the VDBE configuration mode:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# vdb
Router(config-sbc-sbe-vdb)# global
Router(config-sbc-sbe-vdb-global)#
```

## Related Commands

Command	Description
<b>sbe</b>	Creates the SBE on the SBC.

# vpn (session border controller)

To enter the mode for configuring the event limits for a given VPN, use the **vpn** command in the SBE blacklist configuration mode.

*vpn word*

<b>Syntax Description</b>	<i>word</i>	Optional. VPN name or <i>default</i> for the global VPN. Maximum size is 80 characters.
---------------------------	-------------	---

**Command Default** No default behavior or values are available.

**Command Modes** SBE blacklist configuration (config-sbc-sbe-blacklist)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

**Examples** The following example shows how the **vpn** command is used to enter the mode for configuring the event limits for a given VPN:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# blacklist
Router(config-sbc-sbe-blacklist)# vpn test
Router(config-sbc-sbe-blacklist-vpn)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>address-default</b>	Enters the mode for configuring the default event limits for the source addresses in a given VPN.
	<b>clear sbc sbe blacklist</b>	Clears the blacklist for the specified SBC service.
	<b>reason</b>	Enters a mode for configuring a limit to a specific event type on the source.
	<b>show sbc sbe blacklist configured-limits</b>	Lists the explicitly configured limits, showing only the sources configured.
	<b>show sbc sbe blacklist current-blacklisting</b>	Lists the limits causing sources to be blacklisted.

# vrf

To configure an H.323 or SIP adjacency as tied to a specific VPN, use the **vrf** command in the appropriate configuration mode. To remove this configuration, use the **no** form of this command.

**vrf** *vrf\_name*

**no vrf**

## Syntax Description

<i>vrf_name</i>	Specifies the VRF of this adjacency.  The <i>vrf_name</i> can have a maximum of 32 characters which can include the underscore character (_) and alphanumeric characters.  <b>Note</b> Except for the underscore character, do not use any special character to specify field names.
-----------------	--

## Command Default

No default behavior or values are available.

## Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)  
Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.

The adjacency will only receive incoming signaling from this VPN. The adjacency's outgoing signaling is routed in the relevant VRF.

## Examples

The following example shows how to assign the H.323 adjacency h323ToIsp42 to VRF vpn3:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 h323ToIsp42
Router(config-sbc-sbe-adj-h323)# vrf vpn3
```

The following example shows how to configure the SIP adjacency SipToIsp42 to VPN using VRF vpn3:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp42
```



```
Router(config-sbc-sbe-adj-sip)# vrf vpn3
```

## vrf (session border controller)

To configure virtual routing and forwarding (VRF) on a Border Access Controller (BAC) adjacency, use the **vrf** command in the H248 BAC adjacency configuration mode. To disable VRF on a BAC adjacency, use the **no** form of this command.

**vrf** *vrf-name*

**no vrf** *vrf-name*

Syntax Description	<i>vrf-name</i>	Name of VRF.
--------------------	-----------------	--------------

Command Default	None
-----------------	------

Command Modes	H248 BAC adjacency configuration (config-h248-bac-adj)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	<p>The <i>vrf-name</i> should match the name configured using the <b>ip vrf</b> command or the <b>ip vrf</b> forwarding command in the Gi interface.</p> <p>To support VRF, enable Cisco Express Forwarding (CEF) switching on the router, using the <b>ip cef</b> command.</p> <p>If you are also configuring the DHCP services at the access point name (APN), use the <b>dhcp-server ip-address vrf</b> command.</p>
------------------	---

Examples	The following example shows how to configure VRF on a BAC adjacency.:
----------	---

```
Router> enable
Router# configure terminal
Router(config)# sbc h248 bac
Router(config-h248-bac)# adjacency h248 access vrfex
Router(config-h248-bac-adj)# control-address ipv4 10.0.0.1 port 1
Router(config-h248-bac-adj)# vrf vrfex
```

# warrant match-order

To configure lawful enforcement warrant information in a Session Initiation Protocol (SIP) adjacency, and to specify the order of the fields used to match the corresponding warrant, use the **warrant match-order** command in adjacency SIP configuration mode. To deconfigure the lawful enforcement warrant information, use the **no** form of this command.

```
warrant match-order [ destination [ source [ diverted-by ] | diverted-by [ source ] ] ]
```

```
warrant match-order [ source [ destination [ diverted-by ] | diverted-by [ destination ] ] ]
```

```
warrant match-order [ diverted-by [ destination [ source ] | source [ destination ] ] ]
```

```
no warrant
```

## Syntax Description

<b>destination</b>	Specifies the destination field to match the warrant.
<b>source</b>	Specifies the source field to match the warrant.
<b>diverted-by</b>	Specifies the diverted-by field to match the warrant.

## Command Default

By default, the incoming Access adjacency matches the source information and the Core adjacency matches the destination information.

## Command Modes

Adjacency SIP configuration (config-sbc-sbe-adj-sip)

## Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

## Examples

The following example shows how to configure lawful enforcement warrant information in a SIP adjacency, and specifies that the warrant will be matched to the destination field, a source field, and diverted-by field, in that order:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency sip SipToIsp4
Router(config-sbe-adj-sip)# warrant match-order destination source diverted-by
```

## warrant match-order (h323)

To configure lawful enforcement warrant information in an H.323 adjacency, and to specify the order of fields used for matching the corresponding warrant, use the **warrant match-order** command in adjacency H.323 configuration mode. To deconfigure the lawful enforcement warrant information, use the **no** form of this command.

```
warrant match-order [ destination [ source [ destination ] ] ]
```

```
warrant match-order [ source [ destination [ source ] ] ]
```

```
no warrant
```

### Syntax Description

<b>destination</b>	Specifies the destination field for matching the warrant.
<b>source</b>	Specifies the source field for matching the warrant.

### Command Default

By default, the incoming Access adjacency matches the source information, and the Core adjacency matches the destination information.

### Command Modes

Adjacency H.323 configuration (config-sbc-sbe-adj-h323)

### Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes and modes required to run the command.

### Examples

The following example shows how to configure lawful enforcement warrant information in an H.323 adjacency, and specifies that the warrant will be matched first to the destination field, and then to the source field:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# adjacency h323 adj1h323
Router(config-sbc-sbe-adj-h323)# warrant match-order destination source
```

# weight (session border controller)

To assign a weight to this route, use the **weight** command in RTG routing table configuration entry configuration mode. To remove this configuration, use the **no** form of this command.

*weight weight*

*no weight weight*

<b>Syntax Description</b>	<i>weight</i>	Range: [1-65535]
<b>Command Default</b>	The default is 1.	
<b>Command Modes</b>	RTG routing table configuration entry (config-sbc-sbe-rtgpolicy-rtgtable-entry)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
<b>Usage Guidelines</b>	To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of modes required to run the command.	
<b>Examples</b>	<p>The following example shows how.</p> <pre>Router# <b>configure terminal</b> Router(config)# <b>sbc mySbc</b> Router(config-sbc)# <b>sbe</b> Router(config-sbc-sbe)# <b>call-policy-set 1</b> Router(config-sbc-sbe-rtgpolicy)# <b>rtg-least-cost-table MyRtgTable</b> Router(config-sbc-sbe-rtgpolicy-rtgtable)# <b>entry 1</b> Router(config-sbc-sbe-rtgpolicy-rtgtable)# <b>weight 33</b> Router(config-sbc-sbe-rtgpolicy)# <b>end</b></pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>entry</b>	Creates or modifies an entry in a table.

# whitelist (editor)

To set an editor to be whitelisted, use the **whitelist** command in the appropriate editor configuration mode. To remove whitelist from this editor, use the **no** form of this command.

**whitelist**

**no whitelist**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values are available.

**Command Modes**

- SIP Method Editor configuration (config-sbc-sbe-mep-mth)
- SIP Option Editor configuration (config-sbc-sbe-mep-opt)
- SIP Header Editor configuration (config-sbc-sbe-mep-hdr)

Command History	Release	Modification
	Cisco IOS XE Release 3.7S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** To use this command, you must be in the correct configuration mode. The Examples section shows the hierarchy of the modes required to run the command.

**Examples** The following example shows how to whitelist an option editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip option-editor option1
Router(config-sbc-sbe-mep-opt)# whitelist
```

The following example shows how to whitelist a method editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip method-editor Method1
Router(config-sbc-sbe-mep-mth)# whitelist
```

The following example shows how to whitelist a header editor:

```
Router# configure terminal
Router(config)# sbc mySbc
Router(config-sbc)# sbe
Router(config-sbc-sbe)# sip header-editor header1
Router(config-sbc-sbe-mep-hdr)# whitelist
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>sip header-editor</b>	Configures a header editor.
<b>sip method-editor</b>	Configures a method editor.
<b>sip option-editor</b>	Configures an option editor.

# xml (billing)

To configure an XML billing instance, use the **xml** *method-index* command in the SBE billing configuration mode. To disable an XML instance, use the **no** form of this command.

**xml** *method-index*

**no xml** *method-index*

## Syntax Description

*method-index*

The number of the XML method instances to which other parameters such as cdr path, ldr-check, cdr alarm, deact-mode, flipped-interval, and flipped-size are attached. The range of valid values for method-index are 0 to 7.

**Note** Only one XML instance can be configured at a given time. If you try to configure more than one instance, the 'More than one XML instance cannot be configured' error message is displayed.

## Command Default

No default behavior or values

## Command Modes

SBE billing configuration (config-sbc-sbe-billing)

## Command History

### Release

### Modification

Cisco IOS XE Release 3.2S This command was introduced on the Cisco ASR 1000 Series Routers.

## Usage Guidelines

After configuring an XML billing method, an XML instance is defined using the **xml** *method-index* command to attach the parameters to the XML instance. Configuring the XML method index changes the command mode to SBE XML billing (config-sbc-sbe-billing-xml) mode. If the Billing Manager does not have an XML method configured, **xml** *method-index* command will not succeed.



### Note

A maximum of only one XML instance can be defined.

## Examples

The following example defines an XML instance:

```
Router(config)# sbc sbcbilling
Router(config-sbc)# sce
Router(config-sbc-sce)# billing
Router(config-sbc-sce-billing)# xml method
Router(config-sbc-sce-billing)# xml 1
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>method xml</b>	Configures the billing method as XML.
<b>cdr path</b>	Indicates the path in which to store the CDR billing records.
<b>ldr-check</b>	Configures the time at which long duration records are checked.

