# map q850-cause through mgcp package-capability

- map q850-cause, on page 4
- map resp-code, on page 6
- max1 lookup, on page 8
- max1 retries, on page 10
- max2 lookup, on page 12
- max2 retries, on page 14
- max-bandwidth, on page 16
- max-calls, on page 17
- max-conn (dial peer), on page 19
- max-concurrent-sessions, on page 20
- max-connection, on page 21
- max-forwards, on page 23
- max-redirects, on page 25
- max-subscription, on page 26
- maximum buffer-size, on page 27
- maximum cdrflush-timer, on page 29
- maximum conference-participants, on page 31
- maximum fileclose-timer, on page 33
- maximum retry-count, on page 35
- maximum sessions (DSP farm profile), on page 36
- mdn, on page 38
- media, on page 39
- media-address voice-vrf , on page 44
- mediacard, on page 45
- media class, on page 46
- media-inactivity-criteria, on page 47
- media disable-detailed-stats, on page 49
- media profile asp, on page 50
- media profile nr, on page 51
- media profile video, on page 52
- media profile police, on page 53

- media profile recorder, on page 54
- media profile stream-service, on page 55
- media-recording, on page 57
- media recording proxy, on page 58
- media service, on page 59
- meetme-conference, on page 60
- member (dial peer cor list), on page 62
- memory-limit (trace), on page 63
- message-exchange max-failures, on page 65
- method, on page 66
- mgcp, on page 68
- mgcp behavior, on page 70
- mgcp behavior comedia-check-media-src, on page 77
- mgcp behavior comedia-role, on page 78
- mgcp behavior comedia-sdp-force, on page 79
- mgcp behavior g729-variants static-pt, on page 80
- mgcp bind, on page 81
- mgcp block-newcalls, on page 83
- mgcp call-agent, on page 84
- mgcp codec, on page 87
- mgcp codec gsmamr-nb, on page 89
- mgcp codec ilbc, on page 91
- mgcp crypto rfc-preferred, on page 92
- mgcp dns stale threshold, on page 94
- mgcp debug-header, on page 95
- mgcp default-package, on page 96
- mgcp disconnect-delay, on page 99
- mgcp dtmf-relay, on page 100
- mgcp endpoint offset, on page 103
- mgcp explicit hookstate, on page 104
- mgcp fax rate, on page 105
- mgcp fax-relay, on page 107
- mgcp fax t38, on page 109
- mgcp ip qos dscp, on page 112
- mgcp ip-tos, on page 114
- mgcp lawful-intercept, on page 116
- mgcp max-waiting-delay, on page 117
- mgcp modem passthrough codec, on page 118
- mgcp modem passthrough mode, on page 120
- mgcp modem passthrough voip redundancy, on page 122
- mgcp modem passthru, on page 124
- mgcp modem relay voip gateway-xid, on page 125
- mgcp modem relay voip latency, on page 127
- mgcp modem relay voip mode, on page 128
- mgcp modem relay voip mode sse, on page 130
- mgcp modem relay voip sprt retries, on page 132

- mgcp modem relay voip sprt v14, on page 133
- mgcp package-capability, on page 135

# map q850-cause

To play a customized tone to PSTN callers if a call disconnects with a specific Q.850 call-disconnect cause code and release source, use the **map q850-cause** command in voice-service configuration mode. To disable the code-to-tone mapping, use the **no** form of this command.

**map q850-cause** *code-id* **release-source** {**local** | **remote** | **all**} **tone** *tone-id*
**no map q850-cause** *code-id* **release-source** {**local** | **remote** | **all**} **tone** *tone-id*

## Syntax Description

| | |
|---|---|
| *code-id* | Q.850 call-disconnect cause code. Range: 1 to 15, 17 to 127 (16 is not allowed). |
| **release-source** | Source from which the cause code is generated. Choices are the following:<br>• **local** --Originating gateway or gatekeeper<br>• **remote** --Terminating gateway or gatekeeper<br>• **all** --Any gateway or gatekeeper |
| **tone** *tone-id* | Tone to play for this cause code. Choices are the following:<br>• **1** --Busy tone<br>• **2** --Congestion tone<br>• **3** --Special-information tone (a three-tone sequence at 950, 1400, and 1800 MHz) (not supported on IP phones) |

## Command Default

No mapping occurs.

## Command Modes

Voice-service

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Use this command to cause a particular tone to play when a call disconnects for a particular reason.

The tone plays to callers only if the call-disconnect and wait-to-release timers are set to values greater than 0 by entering the **timeouts call-disconnect** and **timeouts wait-release** commands.

## Examples

The following example maps Q.850 call-disconnect cause code 21 to tone 3 on the local gateway and to tone 2 on the remote gateway:

```
Router(config)# voice service pots
Router(conf-voi-serv)# map q850-cause 21 release-source local tone 3
Router(conf-voi-serv)# map q850-cause 21 release-source remote tone 2
```

## Related Commands

| Command | Description |
|---|---|
| **progress_ind** | Sets a specific PI in call setup, progress, or connect messages from an H.323 VoIP gateway. |
| **q850-cause** | Maps a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code. |
| **scenario-cause** | Configures new Q.850 call-disconnect cause codes for use if an H.323 call fails. |
| **timeouts call-disconnect** | Configures the delay timeout before an FXO voice port disconnects an incoming call after disconnect tones are detected. |
| **timeouts wait-release** | Configures the delay timeout before the system starts the process for releasing voice ports. |

# map resp-code

To globally configure a Cisco Unified Border Element (CUBE) to map specific received Session Initiation Protocol (SIP) provisional response messages to a different SIP provisional response message on the outgoing SIP dial peer, use the **map resp-code** command in voice service SIP configuration mode or voice class tenant configuration mode. To disable mapping of received SIP provisional response messages, use the **no** form of this command.

**map resp-code 181 to 183**
**no map resp-code 181**

## Syntax Description

| | |
|---|---|
| **181** | The code representing the specific incoming SIP provisional response messages to be mapped and replaced. |
| **to** | The designator for specifying that the specified incoming SIP provisional response message should be mapped to and replaced with a different SIP provisional response message on the outgoing SIP dial peer. |
| **183** | The code representing the specific SIP provisional response message on the outgoing dial peer to which incoming SIP message responses should be mapped. |

## Command Default

Incoming SIP provisional response messages are passed, as is to the outgoing SIP leg.

## Command Modes

Voice service SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)XA | This command was introduced. |
| 15.1(1)T | This command was integrated into Cisco IOS Release 5.1(1)T. |
| Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S. |
| 15.6(2)T and IOS XE Denali 16.3.1 | This command is now available under voice class tenants. |

## Usage Guidelines

Use the **map resp-code** command in voice service SIP configuration mode to globally enable a Cisco UBE to map incoming SIP 181 provisional response messages to SIP 183 provisional response messages on the outgoing SIP dial peer.

**Note** If the **block** command is configured for incoming SIP 181 messages, either globally or at the dial-peer level, the messages may be dropped before they can be passed or mapped to a different message--even when the **map resp-code** command is enabled. To globally configure whether and when incoming SIP 181 messages are dropped, use the **block** command in voice service SIP configuration mode (or use the **voice-class sip block** command in dial peer voice configuration mode to configure drop settings on individual dial peers).

To configure mapping of SIP provisional response messages for an individual dial peer on a CUBE, use the **voice-class sip map resp-code** command in dial peer voice configuration mode. To disable mapping of SIP 181 message globally on a CUBE, use the **no map resp-code** command in voice service SIP configuration mode.

As an example, to enable interworking of SIP endpoints that do not support the handling of SIP 181 provisional response messages, you could use the **block** command to configure a CUBE to drop SIP 181 provisional response messages received on the SIP trunk or you can use the **map resp-code** command to configure the CUBE to map the incoming messages to and send out, instead, SIP 183 provisional response messages to the SIP line in Cisco Unified Communications Manager Express (Unified CME).

**Note** This command is supported only for SIP-to-SIP calls and will have no effect on H.323-to-SIP or time-division multiplexing (TDM)-to-SIP calls.

## Examples

The following example shows how to configure mapping of incoming SIP 181 provisional response messages on the CUBE to SIP 183 provisional response messages on the outbound dial peer:

```
Router> enable
Router# configure
 terminal
Router(config)# voice
 service
 voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# map resp-code 181 to 183
```

## Related Commands

| Command | Description |
|---|---|
| **block** | Configures global settings for dropping specific SIP provisional response messages on a Cisco IOS voice gateway or CUBE. |
| **voice-class sip block** | Configures an individual dial peer on a Cisco IOS voice gateway or CUBE to drop specified SIP provisional response messages. |
| **voice-class sip map resp-code** | Configures a specific dial peer on a CUBE to map specific incoming SIP provisional response messages to a different SIP response message. |

# max1 lookup

To enable Domain Name System (DNS) lookup for a new call-agent address when the suspicion threshold value is reached, use the **max1 lookup**command inMGCP profile configuration mode. To disable lookup, use the **no** form of this command.

**max1 lookup**
**no max1 lookup**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Lookup is enabled.

## Command Modes

MGCP profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XA | This command was introduced. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |

## Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

Call-agent redundancy can be provided when call agents are identified by DNS name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the *suspicion threshold* . If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries**command;this number is known as the *disconnect threshold* . If the number of retries specified in the **max2 retries**command is reached and there is still no response and the **max2 lookup**command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

## Examples

The following example enables DNS lookup and sets the suspicion retransmission counter to 7:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max1 lookup
Router(config-mgcp-profile)# max1 retries 7
```

## Related Commands

| Command | Description |
|---|---|
| **call -agent** | Specifies a call-agent address and protocol for an MGCP profile. |
| **max1 retries** | Sets the MGCP suspicion threshold value. |
| **max2 lookup** | Enables DNS lookup for an MGCP call agent when the disconnect threshold is reached. |
| **max2 retries** | Sets the MGCP disconnect threshold value. |
| **mgcp** | Starts and allocates resources for the MGCP daemon. |
| **mgcp profile** | Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile. |

# max1 retries

To set the Media Gateway Control Protocol (MGCP) suspicion threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for retransmission), use the **max1 retries**command inMGCP profile configuration mode. To reset to the default, use the **no** form of this command.

**max1 retries** *number*
**no max1 retries**

## Syntax Description

| | |
|---|---|
| *number* | Number of times to attempt to resend messages. Range is from 3 to 30. The default is 5. |

## Command Default

5 attempts

## Command Modes

MGCP profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XA | This command was introduced and replaces the **mgcp request retries**command, which is no longer supported. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850 platforms. The maximum number of retries was increased to 30. |

## Usage Guidelines

This command is used when configuring values for an MGCP profile.

Call-agent redundancy can be provided when call agents are identified by Domain Name System (DNS) name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries**command; this is known as the *suspicion threshold* . If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent.

If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached. This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries**command;this is known as the *disconnect threshold* . If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

## Examples

The following example enables DNS lookup and sets the suspicion retransmission counter to 7:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max1 lookup
Router(config-mgcp-profile)# max1 retries 7
```

## Related Commands

| Command | Description |
|---|---|
| **call -agent** | Specifies a call-agent address and protocol for an MGCP profile. |
| **max1 lookup** | Enables DNS lookup for an MGCP call agent when the suspicion threshold is reached. |
| **max2 lookup** | Enables DNS lookup for an MGCP call agent when the disconnect threshold is reached. |
| **max2 retries** | Sets the MGCP disconnect threshold value. |
| **mgcp** | Starts and allocates resources for the MGCP daemon. |
| **mgcp profile** | Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile. |

# max2 lookup

To enable Domain Name System (DNS) lookup for a new call-agent address after the disconnect threshold timeout value is reached, use the **max2 lookup**command inMGCP profile configuration mode. To disable DNS lookup, use the **no** form of this command.

**max2 lookup**
**no max2 lookup**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Lookup is enabled.

## Command Modes

MGCP profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XA | This command was introduced. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |

## Usage Guidelines

This command is used when configuring values for a Media Gateway Control Protocol (MGCP) profile.

Call-agent redundancy can be provided when call agents are identified by DNS name rather than by IP address in the **call-agent** command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the suspicion threshold. If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries** command; this is known as the disconnect threshold. If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

## Examples

The following example enables DNS lookup and sets the disconnect retransmission counter to 9:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent ca1@exp.example.com
Router(config-mgcp-profile)# max2 lookup
Router(config-mgcp-profile)# max2 retries 9
```

## Related Commands

| Command | Description |
|---|---|
| **call -agent** | Specifies a call-agent address and protocol for an MGCP profile. |
| **max1 lookup** | Enables DNS lookup for an MGCP call agent when the suspicion threshold is reached. |
| **max1 retries** | Sets the MGCP suspicion threshold value. |
| **max2 retries** | Sets the MGCP disconnect threshold value. |
| **mgcp** | Starts and allocates resources for the MGCP daemon. |
| **mgcp profile** | Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile. |

# max2 retries

To set the Media Gateway Control Protocol (MGCP) disconnect threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for further retransmission), use the **max2 retries**command inMGCP profile configuration mode. To disable the disconnect threshold or to return the number of retries to the default, use the **no** form of this command.

**max2 retries** *number*
**no max2 retries**

## Syntax Description

| | |
|---|---|
| *number* | Number of times to attempt to resend messages. Range is from 3 to 30. The default is 7. |

## Command Default

7 attempts

## Command Modes

MGCP profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XA | This command was introduced and replaced the **mgcp request retries**command, which is no longer supported. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. The maximum number of retries was increased to 30. |

## Usage Guidelines

This command is used when configuring values for an MGCP profile.

Call-agent redundancy can be provided when call agents are identified by Domain Name System (DNS) name rather than by IP address in the **call-agent**command, because each DNS name can have more than one IP address associated with it.

When the active call agent does not respond to a message from the media gateway, the gateway tests to determine whether the call agent is out of service. The gateway retransmits the message to the call agent for the number of times specified in the **max1 retries** command; this is known as the *suspicion threshold* . If there is no response and the **max1 lookup** command is enabled, the gateway examines the DNS lookup table to find the IP address of another call agent. If a second call agent is listed, the gateway retransmits the message to the second call agent until a response is received or the number of retries specified in the **max1 retries** command is reached.

This process is repeated for each IP address in the DNS table until the final address is reached. For the final address, the number of retries is specified by the **max2 retries**command;this is known as the *disconnect threshold* . If the number of retries specified in the **max2 retries** command is reached and there is still no response and the **max2 lookup** command is enabled, the gateway performs one final DNS lookup. If any new IP addresses have been added, the gateway starts the retransmission process again. Otherwise, the gateway places the endpoint in a disconnected state.

## Examples

The following example sets the disconnect retransmission counter to 9:

```
Router(config)# mgcp profile nyc-ca
Router(config-mgcp-profile)# call-agent igloo.northpole.net
Router(config-mgcp-profile)# max2 retries 9
```

## Related Commands

| Command | Description |
|---|---|
| **call -agent** | Specifies a call-agent address and protocol for an MGCP profile. |
| **max1 lookup** | Enables DNS lookup for an MGCP call agent after the suspicion threshold value is reached. |
| **max1 retries** | Sets the MGCP suspicion threshold value. |
| **max2 lookup** | Enables DNS lookup for an MGCP call agent after the disconnect threshold value is reached. |
| **mgcp** | Starts and allocates resources for the MGCP daemon. |
| **mgcp profile** | Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints, or to configure the default profile. |

# max-bandwidth

To configure the bandwidth threshold for VoIP media traffic, use the **max-bandwidth** command in dial peer configuration mode. To disable the configuration, use the **no** form of this command.

**max-bandwidth** *bandwidth-value* [{**midcall-exceed**}]
**no max-bandwidth**

## Syntax Description

| | |
|---|---|
| *bandwidth-value* | Aggregate bandwidth in kbps (Kilobits per second). The range is from 8 to 2000000. |
| **midcall-exceed** | (Optional) Allows exceeding the bandwidth threshold during a midcall media renegotiation. |

## Command Default

By default the bandwidth threshold is not configured for VoIP media traffic.

## Command Modes

Dial peer configuration (config-dial-peer)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

Use the **max-bandwidth** command to configure the Bandwidth-Based Call Admission Control feature at the dial peer level and reject SIP calls when the aggregate bandwidth threshold is exceeded.

## Examples

The following example shows how to configure a bandwidth threshold of 24 kbps for VoIP media traffic:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 2000 voip
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# max-bandwidth 24 midcall-exceed
```

## Related Commands

| Command | Description |
|---|---|
| **session protocol sipv2** | Specifies the SIP Version 2 protocol for calls between local and remote routers using the packet network. |

# max-calls

To set the maximum number of calls that a trunk group can handle, use the **max-calls** command in trunk group configuration mode. To reset to the default, use the **no** form of this command.

**max-calls** {**any** | **data** | **voice**} *number* [**direction** [{**in** | **out**}]]
**no max-calls** {**any** | **data** | **voice**} *number* [**direction** [{**in** | **out**}]]

## Syntax Description

| | |
|---|---|
| **any** | Assigns the maximum number of calls that the trunk group can handle, regardless of the type of call. |
| **data** | Assigns the maximum number of data calls to the trunk group. |
| **voice** | Assigns the maximum number of voice calls to the trunk group. |
| *number* | Range is from 0 to 1000. |
| **direction** | (Optional) Specifies direction of calls. |
| **in** | (Optional) Allows only incoming calls. |
| **out** | (Optional) Allows only outgoing calls. |

## Command Default

No limit when the command is not set.

## Command Modes

Trunk group configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced. |

## Usage Guidelines

Use this command to set the maximum number of calls to be handled by the trunk group. If the command is not set the maximum is infinite.

If the maximum is reached, the trunk group becomes unavailable for more calls. When the number of calls falls below the maximum, the trunk group will accept more calls.

## Examples

The following example assigns a maximum number of 500 calls of any type to trunk group gw15:

```
Router(config)# trunk group gw15
Router(config-trunk-group)# max-calls any 500
```

The following example assigns a maximum of 200 data calls and 750 voice calls to trunk group 32:

```
Router(config)# trunk group 32
Router(config-trunk-group)# max-calls data 200
Router(config-trunk-group)# max-calls voice 750
```

## Related Commands

| Command | Description |
|---|---|
| show trunk group | Displays the configuration of one or more trunk groups. |
| trunk group | Initiates a trunk group definition. |

# max-conn (dial peer)

To specify the maximum number of incoming or outgoing connections for a particular Multimedia Mail over IP (MMoIP), plain old telephone service (POTS), Voice over Frame Relay (VoFR), or Voice over IP (VoIP) dial peer, use the **max-conn** command in dial peer configuration mode. To set an unlimited number of connections for this dial peer, use the **no** form of this command.

**max-conn** *number*
**no max-conn**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of connections for this dial peer. Range is 1–2147483647. Default is an unlimited number of connections. |

## Command Default

The **no** form of this command is the default, meaning an unlimited number of connections

## Command Modes

Dial peer configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(1)T | This command was introduced. |
| 12.0(4)XJ | This command was modified for store-and-forward fax. |
| 12.0(4)T | This command was integrated into Cisco IOS Release 12.0(4)T. |
| 12.1(1)T | This command was integrated into Cisco IOS Release 12.1(1)T. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(4)T | This command was implemented on the Cisco 1750. |
| 12.2(8)T | This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Usage Guidelines

Use this command to define the maximum number of connections used simultaneously to send or receive fax-mail. This command applies to off-ramp store-and-forward fax functions.

## Examples

The following example configures a maximum of 5 connections for VoIP dial peer 10:

```
dial-peer voice 10 voip
 max-conn 5
```

## Related Commands

| Command | Description |
|---|---|
| **mta receive maximum -recipients** | Specifies the maximum number of recipients for all SMTP connections. |

# max-concurrent-sessions

To specify the maximum number of concurrent TFTP sessions for the specific phone proxy, use the **max-concurrent-sessions** command in phone proxy configuration mode. To remove the maximum number of concurrent TFTP sessions, use the **no** form of the command.

**max-concurrent-sessions** *number-of-sessions*
**no max-concurrent-sessions**

## Syntax Description

| | |
|---|---|
| *number-of-sessions* | Maximum number of concurrent TFTP sessions. The range is 0 to 500. The default is 200. |

## Command Default

200 concurrent TFTP sessions are configured.

## Command Modes

Phone proxy configuration mode (config-phone-proxy)

## Command History

| Release | Modification |
|---|---|
| 15.3(3)M | This command was introduced. |

## Usage Guidelines

### Example

The following example shows how to specify a maximum of 400 concurrent TFTP sessions:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# max-concurrent-sessions 300
```

# max-connection

To set the maximum number of simultaneous connections to be used for communication with a settlement provider, use the **max-connection** command in settlement configuration mode. To reset to the default, use the **no** form of this command.

**max-connection** *number*
**no max-connection** *number*

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of HTTP connections to a settlement provider. |

## Command Default

10 connections

## Command Modes

Settlement configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(4)XH1 | This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300. |
| 12.1(1)T | This command was integrated into Cisco IOS Release 12.1(1)T. |

## Examples

The following command sets the maximum number of simultaneous connections to 10:

```
settlement 0
 max-connection 10
```

## Related Commands

| Command | Description |
|---|---|
| **connection -timeout** | Configures the time that a connection is maintained after completing a communication exchange. |
| **customer -id** | Sets the customer identification. |
| **device -id** | Specifies a gateway associated with a settlement provider. |
| **encryption** | Sets the encryption method to be negotiated with the provider. |
| **response -timeout** | Configures the maximum time to wait for a response from a server. |
| **retry -delay** | Sets the time between attempts to connect with the settlement provider. |
| **retry -limit** | Sets the maximum number of connection attempts to the provider. |
| **session -timeout** | Sets the interval for closing the connection when there is no input or output traffic. |
| **settlement** | Enters settlement configuration mode and specifies the attributes specific to a settlement provider. |

| Command | Description |
|---|---|
| **shutdown** | Brings up the settlement provider. |
| **type** | Configures an SAA-RTR operation type. |
| **url** | Configures the ISP address. |

# max-forwards

To globally set the maximum number of hops, that is, proxy or redirect servers that can forward the Session Initiation Protocol (SIP) request, use the **max-forwards** command in SIP user-agent configuration mode or voice class tenant configuration mode. To reset the default number of hops, use the no form of this command.

**max-forwards** *number-of-hops* **[system]**
**no max-forwards** *number-of-hops* **[system]**

## Syntax Description

| | |
|---|---|
| *number-of-hops* | Number of hops. Range is from 1 to 70. Default is 70. |
| **system** | Specifies that the hops use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations |

## Command Default

70 hops

## Command Modes

SIP user-agent configuration

Voice class tenant configuration (config-class)

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300. |
| 12.2(2)XA | This command was implemented on Cisco AS5350 and AS5400 platforms. |
| 12.2(2)XB1 | This command was introduced on the Cisco AS5850. |
| 12.2(8)T | This command was implemented on Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release. |
| 12.3(8)T | This command was enhanced with a greater configurable range and a higher default value (compliant with RFC 3261). |
| 15.6(2)T and IOS XE Denali 16.3.1 | This command was modified to include the keyword: **system**. |
| Cisco IOS XE Dublin 17.10.1a | Introduced support for YANG models. |

## Usage Guidelines

To reset this command to the default value, you can also use the default command.

## Examples

The following example sets the number of forwarding requests to 65:

```
sip-ua
 max-forwards 65
```

The following example sets the number of forwarding requests in the voice class tenant configuration mode:

```
Router(config-class)# max-forwards system
```

## Related Commands

| Command | Description |
|---|---|
| **max -redirects** | Sets the maximum number of redirects that the user agent allows. |

# max-redirects

To set the maximum number of redirect servers that the user agent allows, use the **max-redirects** command in dial-peer configuration mode. To reset to the default, use the no form of this command.

**max-redirects** *number*
**no max-redirects**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of redirect servers that a call can traverse. Range is from 1 to 10. The default is 1. |

## Command Default

1 redirect

## Command Modes

Dial-peer configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300. |
| 12.2(2)XA | This command was implemented on the Cisco AS5400 and Cisco AS5350 platforms. |
| 12.2(2)XB1 | This command was implemented on the Cisco AS5850. |
| 12.2(8)T | This command was implemented on the Cisco 7200 series. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release. |
| 12.2(11)T | This command was integrated into Cisco IOS Release 12.2(11)T. |

## Examples

The following is an example of setting the maximum number of redirect servers that the user agent allows:

```
dial-peer voice 102 voip
 max-redirects 2
```

## Related Commands

| Command | Description |
|---|---|
| **dial -peer voice** | Enters dial-peer configuration mode and specifies the method of voice-related encapsulation. |

# max-subscription

To set the maximum number of concurrent watch sessions that are allowed, use the **max-subscription** command in presence configuration mode. To return to the default, use the **no** form of this command.

**max-subscription** *number*
**no max-subscription**

## Syntax Description

| | |
|---|---|
| *number* | Maximum watch sessions. Range: 100 to 500. Default: 100. |

## Command Default

Maximum subscriptions is 100.

## Command Modes

Presence configuration (config-presence)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)XJ | This command was introduced. |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

## Usage Guidelines

This command sets the maximum number of concurrent presence subscriptions for both internal and external subscribe requests.

## Examples

The following example shows the maximum subscriptions set to 150:

```
Router(config)# presence
Router(config-presence)# max-subscription 150
```

## Related Commands

| Command | Description |
|---|---|
| **allow watch** | Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service. |
| **allow subscribe** | Allows internal watchers to monitor external presence entities (directory numbers). |
| **presence enable** | Allows incoming presence requests from SIP trunks. |
| **server** | Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities. |
| **watcher all** | Allows external watchers to monitor internal presence entities (directory numbers). |

# maximum buffer-size

To set the maximum size of the file accounting buffer, use the **maximum buffer-size**command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

**maximum buffer-size** *kbytes*
**no maximum buffer-size**

## Syntax Description

| | |
|---|---|
| *kbytes* | Maximum buffer size, in kilobytes. Range: 6 to 40. Default: 20. |

## Command Default

Maximum buffer size is 20 kilobytes.

## Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)XY | This command was introduced. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

The file accounting process writes call detail records (CDRs) to a memory buffer instead of writing each record independently to the accounting file. Two buffers are allocated for file accounting and their size is set by this command. After the accounting records in the buffer reach the size limit set by this command, the system flushes the first buffer and writes the records to the accounting file. While the first buffer is busy being flushed, the system uses the second buffer to hold new data. After the flush process, the buffer is available again.

The buffer size must be large enough to accommodate incoming CDRs without the system filling up both buffers completely.

## Examples

The following example sets the maximum buffer size to 25 kilobytes:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

## Related Commands

| Command | Description |
|---|---|
| **cdr-format** | Selects the format of the CDRs generated for file accounting. |
| **file-acct flush** | Manually flushes the CDRs from the buffer to the accounting file. |
| **maximum fileclose-timer** | Sets the maximum time for saving records to an accounting file before closing the file and creating a new one. |

| Command | Description |
|---|---|
| **primary** | Sets the primary location for storing the CDRs generated for file accounting. |
| **secondary** | Sets the backup location for storing CDRs if the primary location becomes unavailable. |

# maximum cdrflush-timer

To set the maximum time to hold call records in the buffer before appending the records to the accounting file, use the **maximum cdrflush-timer** command in gateway accounting configuration mode. To reset to the default, use the **no** form of this command.

**maximum cdrflush-timer** *minutes*
**no maximum cdrflush-timer**

## Syntax Description

| | |
|---|---|
| *minutes* | Maximum time, in minutes, to hold call records in the accounting buffer. Range: 1 to 1,435. Default: 60 (1 hour). |

## Command Default

Records are held in the buffer for 60 minutes (1 hour).

## Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)XY | This command was introduced. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

After the time period set with this command expires, the router flushes the buffer and writes the call detail records (CDRs) to the accounting file.

The file accounting process sends CDRs to a memory buffer instead of writing each record independently to the accounting file. The system flushes the buffer automatically either after this timer expires or when the records in the buffer reach the size set by the **maximum buffer-size** command.

Set this flush timer to at least five minutes less than the file close timer set with the **maximum fileclose-timer** command.

To manually flush the CDRs from the buffer to the accounting file, use the **file-acct flush** command.

## Examples

The following example shows that call records are held in the accounting file for three hours, after which the records are appended to the accounting file:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

## Related Commands

| Command | Description |
|---|---|
| **file-acct flush** | Manually flushes the CDRs from the buffer to the accounting file. |

| Command | Description |
|---|---|
| **maximum buffer-size** | Sets the maximum size of the file accounting buffer. |
| **maximum fileclose-timer** | Sets the maximum time for saving records to an accounting file before closing the file and creating a new one. |
| **primary** | Sets the primary location for storing the CDRs generated for file accounting. |
| **secondary** | Sets the backup location for storing CDRs if the primary location becomes unavailable. |

# maximum conference-participants

To configure the maximum number of conference participants allowed in each meet-me conference, use the **maximum conference-participants** command in DSP farm profile configuration mode. To reset the maximum to the default number, use the **no** form of this command.

**maximum conference-participants** *max-participants* [**video-cap-class** *number*]
**no maximum conference-participants** *max-participants* [**video-cap-class** *number*]

## Syntax Description

| | |
|---|---|
| *max-participants* | Maximum number of participants allowed in each meet-me conference session. One DSP can support the following maximums:<br>• G.711--32 participants<br>• G.729--16 participants<br>• Video (H.263 or H.264)--4, 8, or 16 participants |
| **video-cap-class** *number* | (Optional) Reserves the DSP resources needed to support a video participant requiring video format conversion. The range for video port number is from 2 to 4. The default is 2. |

## Command Default

The default maximum number of participants for a video conference is 4. The default maximum number of participants for an audio conference is 8.

## Command Modes

DSP farm profile configuration (config-dspfarm-profile)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)XJ2 | This command was introduced. |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |
| 15.1(4)M | This command was modified. The **video-cap-class** keyword was added. |

## Usage Guidelines

The maximum number of participants allowed for hardware conferencing is dependent on the codec used in the DSP farm profile. Use the **codec** command in DSP farm profile configuration mode to specify the codecs supported by the DSP farm profile. Use the **show dspfarm profile**command to display the DSP farm profile.

## Examples

The following example configures a DSP farm profile that has a maximum of 16 participants for hardware conferences using the G.711 codec:

```
Router(config)# dspfarm profile conference 1
Router(config-dspfarm-profile)# maximum conference-participants 16
Router(config-dspfarm-profile)# codec g711alaw
```

### Related Commands

| Command | Description |
|---|---|
| **codec (DSP Farm profile)** | Specifies the codecs supported by a DSP farm profile. |
| **dspfarm profile** | Enters DSP farm profile configuration mode and defines a profile for DSP farm services. |
| maximum sessions | Specifies the maximum number of sessions that are supported by the profile. |
| **show dspfarm profile** | Displays configured DSP farm profile information. |

# maximum fileclose-timer

To set the maximum time for writing call detail records (CDRs) to an accounting file before closing the file and creating a new one, use the **maximum fileclose-timer**command in gateway accounting configuration mode. To reset to the default, use the **no** form of this command.

**maximum fileclose-timer** *minutes*
**no maximum fileclose-timer**

## Syntax Description

| | |
|---|---|
| *minutes* | Maximum time, in minutes, to write records to an accounting file. Range: 60 (1 hour) to 1,440 (24 hours). Default: 1,440. |

## Command Default

Records are saved to an accounting file for 1,440 minutes (24 hours).

## Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)XY | This command was introduced. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

After the timer set with this command expires, the current accounting file is closed and a new file with a new time stamp is opened to write CDRs. The name and location of the accounting file is set by the **primary** command, or the **secondary** command if in failover mode.

Set this file close timer to at least five minutes longer than the flush timer set with the **maximum cdrflush-timer** command.

To manually flush the CDRs from the buffer to the accounting file, use the **file-acct flush** command.

## Examples

The following example shows that call records are saved to the currently open accounting file for 12 hours, after which a new accounting file is created:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

## Related Commands

| Command | Description |
|---|---|
| **file-acct flush** | Manually flushes the CDRs from the buffer to the accounting file. |
| **maximum buffer-size** | Sets the maximum size of the file accounting buffer. |

| Command | Description |
|---|---|
| **maximum cdrflush-timer** | Sets the maximum time to hold call records in the buffer before appending the records to the accounting file. |
| **primary** | Sets the primary location for storing the CDRs generated for file accounting. |
| **secondary** | Sets the backup location for storing CDRs if the primary location becomes unavailable. |

# maximum retry-count

To set the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device, use the **maximum retry-count**command in gateway accounting file configuration mode. To reset to the default value, use the **no** form of this command.

**maximum retry-count** *number*
**no maximum retry-count**

## Syntax Description

| | |
|---|---|
| *number* | Number of connection attempts. Range: 1 to 5. Default: 2. |

## Command Default

Maximum connection attempts is 2.

## Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)XY | This command was introduced. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

This command specifies the number of times that the router attempts to connect to the primary file device defined in the **primary** command before it attempts to connect to the backup file device specified with the **secondary** command.

## Examples

The following example shows the maximum retries set to 3:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 cdr-format compact
```

## Related Commands

| Command | Description |
|---|---|
| **file-acct reset** | Manually switches back to the primary device for file-based accounting. |
| **primary** | Sets the primary location for storing the call detail records generated for file accounting. |
| **secondary** | Sets the backup location for storing CDRs if the primary location becomes unavailable. |

# maximum sessions (DSP farm profile)

To specify the maximum number of sessions that are supported by the profile, use the **maximum sessions** command in DSP farm profile configuration mode. To reset to the default, use the **no** form of this command.

**Command Syntax When Conferencing or Transcoding Is Configured**
**maximum sessions** *number*
**no maximum sessions**

**Command Syntax When MTP Is Configured**
**maximum sessions** {**hardware** | **software**} *number*
**no maximum sessions**

## Syntax Description

| | |
|---|---|
| *number* | Number of session supported by the profile. Range is 0 to *x* . Default is 0. The *x* value is determined at run time depending on the number of resources available with the resource provider. |
| **hardware** | Number of sessions that media termination points (MTP) hardware resources will support. |
| **software** | Number of sessions that MTP software resources will support. |

## Command Default

The maximum number of supported sessions is 0.

## Command Modes

DSP farm profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.4(22)T | Support for IPv6 was added. |

## Usage Guidelines

When using the MTP service type, you must specify the number of sessions separately for software MTP and hardware MTP. The hardware MTP needs digital signal processor (DSP) resources. Use hardware MTP when the codecs are the same and the packetization period is different.

Active profiles must be shut down before any parameters can be changed.

**Note** The syntax of the command will vary based on the type of profile that you are configuring. The keywords work only when MTP is configured.

## Examples

The following example shows that four sessions are supported by the DSP farm profile:

```
Router(config-dspfarm-profile)#
maximum sessions
```

## Related Commands

| Command | Description |
|---|---|
| **associate application** | Associates the SCCP protocol to the DSP farm profile. |
| **codec** (dspfarm-profile) | Specifies the codecs supported by a DSP farm profile. |
| **description** (dspfarm-profile) | Includes a specific description about the DSP farm profile. |
| **dspfarm profile** | Enters DSP farm profile configuration mode and defines a profile for DSP farm services. |
| **shutdown** (dspfarm-profile) | Allocates DSP farm resources and associates with the application. |
| **voice-card** | Enters voice-card configuration mode. |

# mdn

To request that a message disposition notification (MDN) be generated when a message is processed (opened), use the **mdn** command in dial-peer configuration mode. To disable generation of an MDN, use the **no** form of this command.

**mdn**
**no mdn**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Dial-peer configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(4)XJ | This command was introduced. |
| 12.0(4)T | This command was integrated into Cisco IOS Release 12.0(4)T. |
| 12.1(1)T | This command was integrated into Cisco IOS Release 12.1(1)T. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(4)T | This command was implemented on the Cisco 1750 access router. |
| 12.2(8)T | This command was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745. |

## Usage Guidelines

Message disposition notification is an e-mail message that is generated and sent to the sender when the message is opened by the receiver. Use this command to request that an e-mail response message be sent to the sender when the e-mail that contains the fax TIFF image has been opened.

This command applies to on-ramp store-and-forward fax functions.

## Examples

The following example requests that a message disposition notification be generated by the recipient:

```
dial-peer voice 10 mmoip
 mdn
```

## Related Commands

| Command | Description |
|---|---|
| **mta receive generate -mdn** | Specifies that the off-ramp gateway process a response MDN from an SMTP server. |
| **mta send return -receipt-to** | Specifies the address to which MDNs are sent. |

# media

To enable media packets to pass directly between the endpoints, without the intervention of the Cisco Unified Border Element (Cisco UBE) and to enable signaling services, enter the **media** command in dial peer voice, voice class, or voice service configuration mode. To return to the default behavior, use the **no** form of this command.

**media** [{**bulk-stats** | **flow-around** | **flow-through** | **forking** | **monitoring [video]** [*max-calls*] | **statistics** | **transcoder high-density** | **anti-trombone** | **sync-streams**}]
**no media** [{**bulk-stats** | **flow-around** | **flow-through** | **forking** | **monitoring [video]** [*max-calls*] | **statistics** | **transcoder high-density** | **anti-trombone** | **sync-streams**}]

## Syntax Description

| | |
|---|---|
| **bulk-stats** | (Optional) Enables a periodic process to retrieve bulk call statistics. |
| **flow-around** | (Optional) Enables media packets to pass directly between the endpoints, without the intervention of the Cisco UBE. The media packet is to flow around the gateway. |
| **flow-through** | (Optional) Enables media packets to pass through the endpoints, without the intervention of the Cisco UBE. |
| **forking** | (Optional) Enables the media forking feature for all calls. |
| **monitoring** | (Optional) Monitors the media voice stream quality for all calls or a maximum number of calls. |
| **video** | (Optional) Specifies video quality monitoring. |
| *max-calls* | (Optional) Maximum number of calls that are monitored. |
| **statistics** | (Optional) Enables media monitoring. |
| **transcoder high-density** | (Optional) Converts media codecs from one voice standard to another to facilitate the interoperability of devices using different media standards. |
| **anti-trombone** | (Optional) Enables media anti-trombone for all calls. Media trombones are media loops in SIP entity due to call transfer or call forward. |
| **sync-streams** | (Optional) Specifies that both audio and video streams go through the DSP farms on Cisco UBE and Cisco Unified CME. |

## Command Default

The default behavior of the Cisco UBE is to receive media packets from the inbound call leg, terminate them, and then reoriginate the media stream on an outbound call leg.

## Command Modes

Dial peer voice configuration (config-dial-peer)
Voice class configuration (config-class)
Voice service configuration (config-voi-serv)

## Command History

| Release | Modification |
|---|---|
| 12.3(1)T | This command was introduced. |
| 12.4(11)XJ2 | This command was modified. The **statistics** keyword was introduced. |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |
| 12.4(20)T | This command was modified. The **transcoder**and **high-density** keywords were introduced. |
| 15.0(1)M | This command was modified. The **forking**and **monitoring** keywords and the *max-calls* argument were introduced. |
| 15.1(3)T | This command was modified. The **anti-trombone** keyword was introduced. |
| 15.1(4)M | This command was modified. The **sync-stream** keyword was added. |
| 15.2(1)T | This command was modified. The **video** keyword was added. |
| Cisco IOS XE Release 15.0(1)S | The **bulk-stats** keyword was added. |
| Cisco IOS XE Amsterdam 17.2.1r | Introduced support for YANG models. |

## Usage Guidelines

**Note** **media bulk-stats** and **media statistics** are only supported.

With the default configuration, the Cisco UBE receives media packets from the inbound call leg, terminates them, and then reoriginates the media stream on an outbound call leg. Media flow-around enables media packets to be passed directly between the endpoints, without the intervention of the Cisco UBE. The Cisco UBE continues to handle routing and billing functions. Media flow-around for SIP-to-SIP calls is not supported.

**Note** The Cisco UBE must be running Cisco IOS Release 12.3(1) or a later release to support media flow-around.

You can specify media flow-around for a voice class, all VoIP calls, or individual dial peers.

The **transcoder high-density** keyword can be enabled in any of the configuration modes with the same command format. If you are configuring the **transcoder high-density** keyword for dial peers, make sure that the **media transcoder high-density** command is configured on both the in and out-legs.

The software does not support configuring the **transcoder high-density** keyword on any dial peer that is to handle video calls. The following scenarios are not supported:

- Dial peers used for video at any time. Configuring the **media transcoder high-density**command directly under the dial-peer or a voice-class media configuration mode is not supported.
- Dial peers configured on a Cisco UBE used for video calls at any time. The global configuration of the **media transcoder high-density** command under voice service configuration mode is not supported.

**Note** The**media bulk-stats** command may impact performance when there are a large number of active calls. For networks where performance is crucial in customer's applications, it is recommended that the **media bulk-stats** command not be configured.

To enable the **media** command on a Cisco 2900 or Cisco 3900 series Unified Border Element voice gateway, you must first enter the **mode border-element** command. This enables the **media forking** and **media monitoring** commands. Do not configure the **mode border-element** command on the Cisco 2800 or Cisco 3800 series platform.

You can specify media anti-trombone for a voice class, all VoIP calls, or individual dial peers.

The **anti-trombone** keyword can be enabled only when no media interworking is required in both the out-legs. The anti-trombone will not work if call leg is flow-through and another call leg is flow-around.

## Examples

### Media Bulk-Stats Examples

The following example shows media bulk-stats being configured for all VoIP calls:

```
Device(config)# voice service voip
Device(config-voi-serv)# allow-connections sip to sip
Device(config-voi-serv)# media statistics
```

### Media Flow-around Examples

The following example shows media flow-around configured on a dial peer:

```
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# media flow-around
```

The following example shows media flow-around configured for all VoIP calls:

```
Device(config)# voice service voip
Device(config-voi-serv)# media flow-around
```

The following example shows media flow-around configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-class)# media flow-around
```

### Media Flow-through Examples

The following example shows media flow-through configured on a dial peer:

```
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# media flow-through
```

The following example shows media flow-through configured for all VoIP calls:

```
Device(config)# voice service voip
Device(config-voi-serv)# media flow-through
```

The following example shows media flow-through configured for voice class calls:

```
Device(config)# voice class media 2
Device(config-class)# media flow-through
```

### Media Statistics Examples

The following example shows media monitoring configured for all VoIP calls:

```
Device(config)# voice service voip

Device(config-voi-serv)# media statistics
```

The following example shows media monitoring configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-class)# media
 statistics
```

### Media Transcoder High-density Examples

The following example shows the **media transcoder** command configured for all VoIP calls:

```
Device(config)# voice service voip

Device(conf-voi-serv)# media transcoder high-density
```

The following example shows the **media transcoder**command configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-voice-class)# media transcoder high-density
```

The following example shows the **media transcoder**command configured on a dial peer:

```
Device(config)# dial-peer voice 36 voip
Device(config-dial-peer)# media transcoder high-density
```

### Media Monitoring on a Cisco UBE Platform

The following example shows how to configure audio call scoring for a maximum of 100 calls:

```
mode border-element
media monitoring 100
```

### Media Antitrombone Examples

The following example shows the **media anti-trombone**command configured for all VoIP calls:

```
Device(config)# voice service voip
Device(conf-voi-serv)# media anti-trombone
```

The following example shows the **media anti-trombone**command configured for voice class calls:

```
Device(config)# voice class media 1
Device(config-voice-class)# media anti-trombone
```

The following example shows the **media anti-trombone**command configured on a dial peer:

```
Device(config)# dial-peer voice 36 voip
Device(config-dial-peer)# media anti-trombone
```

### Media Transcoder Examples

The following example specifies that both audio and video RTP streams go through the DSP farms when either audio or video transcoding is needed:

```
Device(config)# voice service voip
Device(config-voi-serv)# media transcoder sync-streams
```

The following example specifies that both audio and video RTP streams go through the DSP farms when either audio or video transcoding is needed and the RTP streams flow around Cisco Unified Border Element.

```
Device(config)# voice service voip
Device(config-voi-serv)# media transcoder high-density sync-streams
```

## Related Commands

| Command | Description |
|---|---|
| **dial-peer voice** | Enters dial peer voice configuration mode. |
| **mode border-element** | Enables the media monitoring capability of the **media** command. |
| **voice class** | Enters voice class configuration mode. |
| **voice service** | Enters voice service configuration mode. |

# media-address voice-vrf

To associate RTP port-range with VRF, use the **media-adderss voice-vrf** command in voice-service-voip configuration mode. To disable use **no** form of this command.

**media-adderss voice-vrf** *vrf name* **port-range**{*min max*}

**no media-adderss voice-vrf** *vrf name* **port-range**{*min max*}

## Syntax Description

| | |
|---|---|
| *vrf name* | Specifies the VRF name. |
| **port-range** | Specifies RTP port-range. |
| *min-max* | Specifies the minimum and maximum RTP port range. |

## Command Default

No media-address range is associated with VRF.

## Command Modes

voice-serv-voip

## Command History

| Release | Modification |
|---|---|
| Cisco IOS 15.6(2)T | This command was introduced. |
| Cisco IOS XE Denali 16.3.1 | This command was integrated with Cisco IOS XE Denali 16.3.1 |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Usage Guidelines

Use this command to associate RTP port-range with VRF.

### Examples

Port-range configured on the same line as the media address:

```
Device(conf-voi-serv)# media-address voice-vrf VRF1 6000 7000
```

Multiple port-range lines are configured under the media address:

```
Device(conf-voi-serv)# media-address voice-vrf VRF1
Device(cfg-media-addr-vrf)# port-range 6000 7000
Device(cfg-media-addr-vrf)# port-range 8000 10000
Device(cfg-media-addr-vrf)# port-range 11000 20000
```

# mediacard

To enter mediacard configuration mode and configure a Communications Media Module (CMM) media card, use the **mediacard** command in global configuration mode.

**mediacard** *slot*

## Syntax Description

| | |
|---|---|
| *slot* | Specifies the slot number for the media card to be configured. Valid values are from 1 to 4. |

## Command Default

No default behavior or values

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.3(8)XY | This command was introduced on the Communication Media Module. |
| 12.3(14)T | This command was integrated into Cisco IOS Release 12.3(14)T. |
| 12.4(3) | This command was integrated into Cisco IOS Release 12.4(3). |

## Usage Guidelines

Mediacard configuration mode is used to configure parameters related to the selected media card, such as digital signal processor (DSP) resource pools.

## Examples

The following example shows how you configure DSP resources on the media card in slot 1:

```
mediacard 1
```

## Related Commands

| Command | Description |
|---|---|
| **debug mediacard** | Displays debugging information for Digital Signal Processor Resource Manager (DSPRM). |
| **show mediacard** | Displays information about the selected media card. |

# media class

To configure a media class and to enter media class configuration mode, use the **media class** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**media class** *tag*
**no media class** *tag*

## Syntax Description

| | |
|---|---|
| *tag* | Media class tag. The range is 1–10000. |

## Command Default

No media class is configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Bengaluru 17.6.1a | This command was modified to add **stream-service** as a sub-command. |

## Usage Guidelines

Use the **media class** command to combine different profiles, such as media forking, and apply the profile to a dial peer if required.

## Examples

The following example shows how to configure a media class for tag 100:

```
Router(config)# media class 100
```

## Related Commands

| Command | Description |
|---|---|
| **recorder profile** | Configures the media profile recorder. |

# media-inactivity-criteria

To specify the mechanism for detecting media inactivity (silence) on a voice call, use the **media-inactivity-criteria** command in a gateway configuration mode. To disable detection, use the **no** form of this command.

**media-inactivity-criteria** {**rtp** | [**receive**] | **rtcp** | **all** | [**receive**] | **rtplib**}
**no media-inactivity-criteria**

## Syntax Description

| | |
|---|---|
| **rtp** | Real-Time Transport Protocol (RTP) (default) |
| **rtcp** | RTP Control Protocol (RTCP) |
| **all** | Both RTP and RTCP |
| **receive** | (Optional) Changes the media inactivity criteria to check for received packets only. |
| **rtplib** | RTP (comfort noise is considered as an activity) |

## Command Default

Media-inactivity detection is performed by RTP.

## Command Modes

Global configuration mode.

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| 15.4(03)M | This command was modified. The **receive** keyword was added. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Usage Guidelines

Use this command to specify the mechanism for detecting silence on a voice call. After doing so, you can configure silent calls to disconnect by entering the related commands listed below.

Use this command, with the **application**, **package callfeature**, **param**, and **paramspace** commands, to configure callfeature parameters at the package level and to override them as needed for specific applications or dial peers.

The mechanism that you explicitly specify with this command takes precedence over any mechanism that you might implicitly have specified with the **ip rtcp report interval** command with the **timer media-inactive** or **timer receive-rtcp** command.

For SIP-to-SIP IPv4 calls, if the CLI command **media-inactivity-criteria rtp** is configured under a gateway configuration mode, then call is cleared due to media inactivity although two way RTP and RTCP are present. As a workaround, it is mandatory that you configure **media-inactivity-criteria** as **rtplib** or **rtcp**or **all**. For a sample configuration, see example.

## Examples

The following example shows a **media-inactivity-criteria** configuration to ensure that call is not cleared due to media inactivity although RTP and RTCP are present.

```
Router(config)#gateway
Router(config-gateway)#media-inactivity-criteria rtcp|rtplib|all
```

The following example specifies the use of RTCP for silence detection:

```
Router(config)# gateway
Router(config-gateway)# media-inactivity-criteria rtcp
```

The following example shows a configuration that might result from the use of this and related commands:

```
voice service pots
map q850-cause 44 release-source local tone 3
application
 package callfeature
  param med-inact-disc-cause 44
  param med-inact-det enable
  param med-inact-action disconnect
ip rtcp report interval 9000
dial-peer voice 5 voip
destination-pattern .T
 progress_ind disconnect enable 8
 session target ras
 codec g711ulaw
gateway
 media-inactivity-criteria rtcp
 timer media-inactive 5
```

## Related Commands

| Command | Description |
|---|---|
| **application** | Enables a specific application on a dial peer. |
| **ip rtcp report interval** | Configures the average reporting interval between subsequent RTCP report transmissions. |
| **package callfeature** | Enters application-parameter configuration mode. |
| **param** | Loads and configures parameters in a package or a service (application) on the gateway. |
| **paramspace** | Enables an application to use parameters from the local parameter space of another application. |
| **timer media-inactive** | Sets the media-inactivity disconnect timer. |
| **timer receive-rtcp** | Sets the RTCP timer and configures a multiplication factor for the RTCP timer interval for SIP or H.323 calls. |

# media disable-detailed-stats

To disable detailed statistics collection about the calls present.

**media disable-detailed-stats**
**no media disable-detailed-stats**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Global configuration mode

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

# media profile asp

To create a media profile to configure acoustic shock protection parameters, use the **media profile asp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**media profile asp** *tag*
**no media profile asp** *tag*

## Syntax Description

| | |
|---|---|
| *tag* | Media profile tag. The range is from 1 to 10000. |

## Command Default

Media profile for acoustic shock protection is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.2(3)T | This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Usage Guidelines

Use the **media profile asp** command to configure media profile for acoustic shock protection parameters. You can configure acoustic shock protection parameters after creating a media profile.

## Examples

The following example shows how to create a media profile to configure acoustic shock protection parameters:

```
Device> enable
Device# configure terminal
Device(config)# media profile asp 200
Device(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| **media profile nr** | Creates a media profile to configure noise reduction parameters. |

# media profile nr

To create a media profile to configure noise reduction parameters, use the **media profile nr** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**media profile nr** *tag*
**no media profile nr** *tag*

## Syntax Description

| | |
|---|---|
| *tag* | Media profile tag. The range is from 1 to 10000. |

## Command Default

Media profile for noise reduction is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.2(3)T | This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Usage Guidelines

Use the **media profile nr** command to configure media profile for noise reduction parameters. You can configure noise reduction parameters after creating a media profile.

## Examples

The following example shows how to create a media profile to configure noise reduction parameters:

```
Device> enable
Device# configure terminal
Device(config)# media profile nr 200
Device(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| **media profile asp** | Creates a media profile to configure acoustic shock protection parameters. |

# media profile video

To create a media profile video, use the **media profile video** command in dial-peer voice configuration mode.

**media profile video** *tag*
**no media profile video** *tag*

## Syntax Description

| | |
|---|---|
| *tag* | Media profile video tag. The range is from 1 to 10000. |

## Command Modes

Dial-peer configuration (config).

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Related Commands

| Command | Description |
|---|---|
| **media profile nr** | Creates a media profile to configure noise reduction parameters. |
| **media profile asp** | Creates a media profile to configure acoustic shock protection parameters. |

# media profile police

To configure the media policing profile, use the **media profile police** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**media profile police** *tag*
**no media profile police** *tag*

## Syntax Description

| | |
|---|---|
| *tag* | Media profile tag. The range is from 1 to 10000. |

## Command Default

Media policing profiles are not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

Use the **media profile police** command to configure a media policing profile. You must apply the profile to a dial peer or globally after configuring the media policing profile.

## Examples

The following example shows how to configure the media policing profile:

```
Router> enable
Router# configure terminal
Router(config)# media profile police 1
```

## Related Commands

| Command | Description |
|---|---|
| **media police-profile** | Applies the media policing profile at the global level. |
| **media-class** | Applies the media policing profile at the dial peer level. |
| **police profile** | Applies the media bandwidth policing profile to a media class. |

# media profile recorder

To configure the media recorder profile, use the **media profile recorder** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**media profile recorder** *profile-tag*
**no media profile recorder** *profile-tag*

## Syntax Description

| | |
|---|---|
| *profile-tag* | Media profile tag. The range is from 1 to 10000. |

## Command Default

Media profile recorder is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Usage Guidelines

You can use the **media profile recorder** command to configure the recorder profile. Here, you will be saving the dial peer tag that points to the recording server on the Cisco Unified Border Element (Cisco UBE).

Configuring the **media profile recorder** command is a method to define media recording globally. This configuration provides a profile for the recorder to define media recording.

## Examples

The following example shows how to configure the media profile recorder:

```
Router# configure terminal
Router(config)# media profile recorder 100
```

## Related Commands

| Command | Description |
|---|---|
| **media-recording** | Sets voice class recording parameters. |
| **show voip recmsp session** | Displays active recording MSP session information. |

# media profile stream-service

To enable stream-service on CUBE, use the **media profile stream-service** *tag* command in global configuration mode. To disable stream-service, use the **no** form of this command.

**media profile stream-service** *tag*
**no media profile stream-service** *tag*

## Syntax Description

| | |
|---|---|
| *tag* | The media profile stream-service tag. Range is 1–10000. |

## Command Default

Stream service isn’t enabled by default.

## Command Modes

Global configuration mode (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Bengaluru 17.6.1a | This command was introduced on Cisco Unified Border Element. |
| Cisco IOS XE Cupertino 17.7.1a | Introduced support for YANG models. |

## Usage Guidelines

When you configure **media profile stream-service** *tag* , the media profile configuration mode is enabled.

```
router(config)#media profile stream-service <tag>
router(cfg-mediaprofile)#?
MEDIAPROFILE configuration commands:
connection stream service connection
description Mediaprofile specific description
exit Exit from media profile configuration mode
help Description of the interactive help system
no Negate a command or set its defaults
proxy Websocket Proxy Server
source-ip local source-ip for the websocket connection
```

Configure the required stream-service profile within the corresponding **media-class** to enable stream-service functionality using the **media profile stream-service** *tag* command on CUBE. Further, you must associate the **media-class** with the dial-peer pointing towards CVP. If **media-class** isn’t associated with the dial-peer pointing towards CVP, CUBE rejects the forking request and sends an INFO message to CVP to inform that it’s an unsupported flow.

CUBE uses the local IP address configured under source-interface for establishing WebSocket connection. When proxy is configured with host name instead of IP address, CUBE performs DNS resolution for proxy before sending the WebSocket request. However, when proxy is configured and json from CVP contains host name for speech server, DNS resolution isn’t performed.

## Examples

The following is a sample configuration for enabling stream-service functionality in CUBE:

```
media profile stream-service 99
connection idle-timeout 1(This can be 1-60 mins)

media class 9
stream-service profile 99

dial-peer voice 42 voip
```

```
destination-pattern 5678
session protocol sipv2
session target ipv4:8.41.17.71:8001
session transport udp
voice-class codec 40
voice-class sip bind control source-interface GigabitEthernet1
voice-class sip bind media source-interface GigabitEthernet1
media-class 9
```

## Related Commands

| Command | Description |
|---|---|
| **connection (media-profile)** | Configures idle timeout and call threshold for a media profile. |
| **proxy (media-profile)** | Configures IP address or hostname of proxy in media profile. |
| **source-ip (media-profile)** | Configures local source IP address of a WebSocket connection. |
| **media class** | Applies the media class at the dial peer level. |
| **stream-service profile** | Associates a stream service profile with media class. |

# media-recording

To configure voice class recording parameters, use the **media-recording** command in media profile or media class recorder parameter configuration mode. To disable the configuration, use the **no** form of this command.

**media-recording** *dial-peer-tag* [*dial-peer-tag2* . . . *dial-peer-tag5*]
**no media-recording** *dial-peer-tag* [*dial-peer-tag2* . . . *dial-peer-tag5*]

## Syntax Description

| | |
|---|---|
| *dial-peer-tag* | Dial peer tag to be matched on the forked leg. The range is from 1 to 1073741823.<br>• You can specify a maximum of five dial peers. |

## Command Default

No voice class recording parameter is configured.

## Command Modes

Media profile configuration (cfg-mediaprofile)
Media class recorder parameter configuration (cfg-mediaclass-recorder)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Amsterdam 17.2.1r | Introduced support for YANG models. |

## Usage Guidelines

Use the **media-recording** command to define a dial peer tag for recording. This command configures the dial peer that points to the recording server.

## Examples

The following example shows how to configure voice class recording parameters:

```
Router# configure terminal
Router(config)# media profile recorder 100
Router(cfg-mediaprofile)# media-recording 1000 1001 1002 1003 1004
```

## Related Commands

| Command | Description |
|---|---|
| **media profile recorder** | Configures the media recorder profile. |
| **show voip recmsp session** | Displays active recording MSP session information. |

# media recording proxy

Configures the dial-peers for forking.

**Note** You can specify maximum of five dial peer tags.

**media-recording proxy** [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]

**media-recording proxy secure** [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]

## Syntax Description

| | |
|---|---|
| **media-recording proxy** [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*] | The proxy configures the first dial-peer of the sequence for establishing a back-to-back (B2B) call, and the remaining dial-peers for media forking. |
| **media-recording proxy secure** [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*] | You can configure dial-peers for either secure or nonsecure forking. You may configure up to five secure or nonsecure dial-peers. The first available secure target is used for establishing a back-to-back call. Earlier behaviour remains unchanged if there are no secure dial peers configured. Configure all secure dial peers with the same voice class srtp-crypto profile. |

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1a | This command was introduced. |
| Cisco IOS XE Bengaluru 17.5.1a | Introduced support for secure forking. |

## Examples

```
Device(cfg-mediaprofile)# media-recording proxy 8000 8001 8002
```

```
Device(cfg-mediaprofile)# media-recording proxy secure 8003 8004
```

# media service

To apply a media class for noise reduction (NR) or acoustic shock protection (ASP) at a global level, use the **media service** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**media service**
**no media service**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Media service is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| 15.2(3)T | This command was modified. Support for the Cisco Unified Border Element (Cisco UBE) was added. |

## Usage Guidelines

Use the **media service** command to apply a media class for NR or ASP at a global level. You can configure a media service after creating a media profile and applying the profile to a media class.

## Examples

The following example shows how to apply a media class for NR or ASP at a global level:

```
Device> enable
Device# configure terminal
Device(config)# media service
Device(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| **media class** | Creates a media class to configure noise reduction parameters. |

# meetme-conference

To define a feature code for a Feature Access Code (FAC) to initiate an SCCP Meet-Me Conference, use the **meetme-conference**command in STC application feature access-code configuration mode. To return the feature code to its default, use the **no** form of this command.

**meetme-conference** *keypad-character*
**no meetme-conference**

## Syntax Description

| | |
|---|---|
| *keypad-character* | Character string that can be dialed on a telephone keypad (0-9, *, #). Default: 5.<br>The string can be any of the following:<br>• A single character (0-9, *, #)<br>• Two digits (00-99)<br>• Two to four characters (0-9, *, #) and the leading or ending character must be an asterisk (*) or number sign (#) |

## Command Default

The default value of the feature code is 5.

## Command Modes

STC application feature access-code configuration (config-stcapp-fac)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)YA | This command was introduced. |
| 12.4(22)T | This command was integrated into Cisco IOS Release 12.4(22)T. |

## Usage Guidelines

This command changes the value of the feature code for SCCP Meet-Me Conference from the default (5) to the specified value.

If the length of the *keypad-character* argument is at least two characters and the leading or ending character of the string is an asterisk (*) or a number sign (#), phone users are not required to dial a prefix to access this feature. Typically, phone users dial a special feature access code (FAC) consisting of a prefix plus a feature code, for example **2. If the feature code is 55#, the phone user dials only 55#, without the FAC prefix, to access the corresponding feature.

If you attempt to configure this command with a value that is already configured for another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

If you attempt to configure this command with a value that precludes or is precluded by another FAC, speed-dial code, or the Redial FSD, you receive a message. If you configure a feature code to a value that precludes or is precluded by another code, the system always executes the call feature with the shortest code and ignores the longer code. For example, #1 will always preclude #12 and #123. You must configure a new value for the precluded code in order to enable phone user access to that feature.

To display a list of all FACs, use the **show stcapp feature codes** command.

## Examples

The following example shows how to change the value of the feature code for SCCP Meet-Me Conference from the default (5). This configuration also changes the value of the prefix for all FACs from the default (**) to ##. With this configuration, a phone user must press ##9 on the phone keypad to cancel all-call forwarding.

```
Router(config)# stcapp feature access-code
Router(config-stcapp-fac)# prefix ##
Router(config-stcapp-fac)# meetme-conference 9
Router(config-stcapp-fac)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **prefix** (stcapp-fac) | Defines the prefix for feature access codes (FACs). |
| **show stcapp feature codes** | Displays all feature access codes (FACs). |
| **stcapp feature access-code** | Enables feature access codes (FACs) and enters STC application feature access-code configuration mode for changing values of the prefix and features codes from the default. |

# member (dial peer cor list)

To add a member to a dial peer class of restrictions (COR) list, use the **member** command in dial peer COR list configuration mode. To remove a member from a list, use the **no** form of this command.

**member** *class-name*
**no member** *class-name*

## Syntax Description

| | |
|---|---|
| *class-name* | Class name previously defined in dial peer COR custom configuration mode by using of the **name** command. |

## Command Default

No default behavior or values.

## Command Modes

Dial peer COR list configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |

## Examples

The following example adds three members to the COR list named list3:

```
dial-peer cor list list3
 member 900_call
 member 800_call
 member catchall
```

## Related Commands

| Command | Description |
|---|---|
| **dial-peer cor list** | Defines a COR list name. |

# memory-limit (trace)

To define the memory limit for storing VoIP Trace information, use the **memory-limit** command in trace configuration mode. To reset to the default memory limit, use the **no** form of this command.

**memory-limit** { **platform** | **memory** }
**no memory-limit** { **platform** | **memory** }

## Syntax Description

| | |
|---|---|
| **memory-limit** | Defines the memory limit for storing VoIP Trace information. |
| **memory** | Defines a custom memory limit for VoIP Trace. Range is 10–1000 MB. |
| **platform** | Configures 10% of available platform memory at the time of configuration of the command as memory limit for VoIP Trace. |

## Command Default

A limit equivalent to 10% of available platform memory is enabled by default. (**memory-limit platform**)

## Command Modes

Trace configuration mode (conf-serv-trace)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.2<br>Cisco IOS XE Bengaluru 17.4.1a | This command was introduced on Cisco Unified Border Element. |

## Usage Guidelines

Configure **memory-limit** to define a custom memory limit for VoIP Trace information storage within the range of 10 MB to 1000 MB. If **platform** is configured, 10% of the total memory available to the IOS processor at the time of configuring is allocated to the storage of VoIP Trace information.

```
router(conf-voi-serv)#trace
router(conf-serv-trace)#?
memory-limit  Set limit on the usage of resources
router(conf-serv-trace)#memory-limit 10
```

Configuration of custom memory-limit more than the available platform memory is not allowed. Configuration fails with an error message:

```
router(config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#memory-limit 800
Error: Setting memory-limit more than available platform memory (732 MB) is not allowed.
```

Configuration of memory-limit more than the 10% of the available platform memory affects the system performance. Configuration is successful with a warning message:

```
router(config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#memory-limit 100
Warning: Setting memory limit more than 10% of available platform memory (73 MB) will affect
 system performance.
```

Reducing the memory-limit from an existing limit **resets** the VoIP Trace data. Take copy of the **show voip trace statistics detail** and **show voip trace all** output data before reducing the memory-limit.

A confirmation message is displayed when you reduce the memory-limit from an existing limit:

```
Reducing the memory-limit clears all VoIP Trace statistics and data.
If you wish to copy this data first, enter ‘no’ to cancel,
otherwise enter ‘yes’ to proceed.
```

Increasing the memory-limit does not impact the VoIP Trace data.

**Note** If the memory-limit is exhausted by active calls, incoming calls are not traced.

## Examples

The following is a sample of CLI command **memory-limit** configured under trace configuration sub-mode:

```
router(conf-voi-serv)#trace
router(conf-serv-trace)#?
Voip Trace submode commands:
default       Set a command to its defaults
exit          Exit from voice service voip trace mode
no            Negate a command or set its defaults
shutdown      Shut Voip Trace debugging
memory-limit  Set limit based on memory used
router(conf-serv-trace)#memory-limit ?
<10-1000>     Specify maximum memory limit in MB
  platform    Use 10 percent of available memory
CSR(conf-serv-trace)#memory-limit 10
```

## Related Commands

| Command | Description |
|---|---|
| **trace** | Enables the VoIP Trace serviceability framework in CUBE. |
| **shutdown (trace)** | Disables the VoIP Trace serviceability framework in CUBE. |
| **show voip trace** | Displays the VoIP Trace information for SIP legs on a call that is received on CUBE. |

# message-exchange max-failures

To configure the maximum number of failed message that is exchanged between the application and the provider before the provider stops sending messages to the application, use the **message-exchange max-failures** command. To reset the maximum to the default number, use the **no** form of this command.

**message-exchange max-failures** *number*
**no message-exchange max-failures** *number*

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of messages allowed before the service provider stops sending messages to the application. Range is from 1 to 3. Default is 1. |

## Command Default

The default is 1.

## Command Modes

uc wsapi mode configuration mode

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

Use this command to set the maximum number of messages that can fail before the system determines that the application is unreachable and the service provider stops sending messages to the application.

## Examples

The following example sets the maximum number of failed messages to 2.

```
Router(config)# uc wsapi
Router(config-uc-wsapi)# message-exchange max-failures 2
```

## Related Commands

| Command | Description |
|---|---|
| **probing interval** | Sets the time interval between probing messages. |
| **probing max-failure** | Sets the number of messages that the system will send without receiving a reply before the system unregisters the application. |

# method

To set a specific accounting method list, use the **method** command in gateway accounting AAA configuration mode.

**method** *acctMethListName*

## Syntax Description

| | |
|---|---|
| *acctMethListName* | Name of the accounting method list. |

## Command Default

H.323 is the default accounting method list.

## Command Modes

Gateway accounting AAA configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced on the following platforms: Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850. |

## Usage Guidelines

- For information on setting AAA network security for your network, including setting method lists, refer to the *Authentication, Authorization, and Accounting Cisco IOS Security Configuration Guide* , Release 12.2.
- The **method** command sets the accounting method globally (not for a dial peer). To initially define the AAA method list name for accounting, use the **aaa accounting** command.
- The method list name used is the same name used to define the method list name under the **aaa accounting** command.

## Examples

The following example uses the method list named "klz_aaa6" that was previously defined using the AAA commands.

```
aaa new-model
!
aaa group server radius sg6
server 1.6.30.70 auth-port 1708 acct-port 1709
!
aaa authentication login klz_aaa6 group sg6
! klz_aaa6 is defined as the method list name.
aaa authorization exec klz_aaa6 group sg6
aaa accounting connection klz_aaa6 start-stop group sg6
!
gw-accounting aaa
method klz_aaa6
! The same method list named klz_aaa6 is used.
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables accounting of requested services for billing or security purposes. |

| Command | Description |
|---|---|
| **gw-accounting aaa** | Enables VoIP gateway accounting. |

# mgcp

To allocate resources for the Media Gateway Control Protocol (MGCP) and start the MGCP daemon, use the **mgcp**command in global configuration mode. To terminate all calls, release all allocated resources, and stop the MGCP daemon, use the **no** form of this command.

**mgcp** [*port*]
**no mgcp**

## Syntax Description

| | |
|---|---|
| *port* | (Optional) User Datagram Protocol (UDP) port for the MGCP gateway. Range is from 1025 to 65535. The default is UDP port 2427. |

## Command Default

UDP port 2427

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the Cisco AS5300. |
| 12.1(3)T | This command was implemented on the following platforms: Cisco 3660, Cisco uBR924, and Cisco 2600 series. |
| 12.1(5)XM | This command was added to Cisco MC3810. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.2(11)T | This command was implemented on the Cisco AS5850. |

## Usage Guidelines

Once you start the MGCP daemon using the **mgcp**command, you can suspend it (for example, for maintenance) by using the **mgcp block-newcalls** command. When you are ready to resume normal MGCP operations, use the **no mgcp block-newcalls** command. Use the **no mgcp** command only if you intend to terminate all MGCP applications and protocols.

W hen the MGCP daemon is not active, all MGCP messages are ignored.

If you want to change the UDP port while MGCP is running, you must stop the MGCP daemon using the **no mgcp** command, and then restart it with the new port number using the **mgcp** *port* command.

## Examples

The following example initiates the MGCP daemon:

```
Router(config)# mgcp
```

The following example enables the MGCP daemon on port 4204:

```
Router(config)# mgcp
4204
```

## Related Commands

| Command | Description |
|---|---|
| **application** | Enables debugging on MGCP. |
| **debug mgcp** | Enables debugging on MGCP. |
| **mgcp block -newcalls** | Gracefully terminates all MGCP activity. |
| **mgcp ip -tos** | Enables or disables the IP ToS for MGCP connections. |
| **mgcp request retries** | Specifies the number of times to retry sending the **mgcp** command. |
| **show mgcp** | Displays the MGCP parameter settings. |

# mgcp behavior

To configure a gateway to alter the Media Gateway Control Protocol (MGCP) behavior, use the **mgcp behavior**command in global configuration mode. To resume using the standard protocol version behavior that is specified in the configuration, use the **no** form of this command.

**mgcp behavior** *category version*
**no mgcp behavior** *category version*

## Syntax Description

| | |
|---|---|
| *category* | MGCP behavior category. For valid values, see the first table below. |
| *version* | MGCP version for the behavior category. For valid values, see the second table below. |

## Command Default

The gateway follows the rules and guidelines that are specified by the configured MGCP protocol version.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T1 | This command was introduced. |
| 12.3(4)T | This command was modified. The **signals v0.1** keyword was added. |
| 12.3(8)T | This command was modified. The **dlcx-clear-signals** keyword was added. |
| 12.3(11)T | This command was modified. The **ack-init-rsip disable** and **init-rsip-per-insvc legacy**keywords were added. |
| 12.3(14)T | This command was modified. The **q-mode-enduring legacy** keyword was added. |
| 12.3(16) | This command was modified. The **mdcx-sdp ack-with-sdp**keyword was added. |
| 12.4(4)T | This command was modified. The **rsip-range** keyword was added. |
| 12.4(24)T | This command was modified. The default behavor of the mode parameter in the SDP was given higher preference to the mode present in the M: line of the MGCP message. The **digit-collect-stuck play-reorder**, **fxs-gs emulate-ls-disconnect**, **mode-attrb-in-sdp disable, private-localhost**, **and transient-state-response enable**keywords were added. |
| 15.1(1)T | This command was modified. The **dynamically-change-codec-pt disable** keyword was added**.** |
| 15.1(3)T | This command was modified. The **negotiate-nse enable** keyword was added. |

## Usage Guidelines

The table below describes the MGCP behavior category keywords.

*Table 1: MGCP Behavior Category Keywords*

| Keywords | Description |
|---|---|
| **ack-init-rsip disable** | Forces the gateway to accept commands from the call agent before its initial ReStart In Progress (RSIP) messages are acknowledged; that is, 405 error codes do not occur. The gateway also behaves in this way if it is configured for MGCP Version 1.0 and earlier versions.<br>By default, or when the **no** form of this command is issued, if the gateway is configured for MGCP Version RFC 3435-1.0 or later versions, it responds to call agent commands with a 405 error code until its initial RSIPs are acknowledged by the call agent. |
| **digit-collect-stuck play-reorder** | Forces the gateway to play a reorder tone to the user when 60 seconds have passed and when MGCP is in the process of collecting the digits.<br>By default, or when the **no** form of this command is issued, if the MGCP application does not get a connection or gets disconnected within a specific time when the endpoint is in the off-hook state, then the endpoint may be busy in the digit collection state. |
| **dlcx-clear-signals all** | Forces the gateway to turn off or clear all signals when it receives a Delete Connection (DLCX) message from the call agent even if there is no S: line in the message.<br>By default, and as specified by RFC 3435, the gateway maintains current endpoint signals if a DLCX has no S: line. The MGCP gateway clears signals only when the call agent explicitly turns off each signal or sends an empty S: line to clear all signals. |
| **dynamically-change-codec-pt disable** | Forces the gateway not to change the codec payload type when it is dynamically changed in the incoming Session Description Protocol (SDP).<br>By default, or when **no** form of this command is issued, MGCP dynamically changes the payload, if the incoming SDP has a different codec. |
| **fxs-gs emulate-ls-disconnect** | Forces the gateway not to disconnect the call even when the gateway receives a DLCX for a ground-start enabled endpoint. The gateway plays the busy tone as the call does not get disconnected.<br>By default, or when **no** form of thiscommand is issued, MGCP disconnects the call when it receives a DLCX. |

| Keywords | Description |
|---|---|
| **init-rsip-per-insvc legacy** | Forces the gateway to always use the restart method of Restart for its initial RSIP messages, regardless of the service state of the endpoints. Wildcard demotion may occur as needed, based on configuration.<br>By default, or when the **no** form of this command is issued, if the MGCP gateway is running Version RFC 3435-1.0, the default restart method for initial RSIPs depends on the service state of the endpoint. For in-service endpoints, the restart method is Restart. For out-of-service endpoints, the restart method is Forced.<br>Additionally, regardless of the protocol version, the gateway always attempts to use a wildcard RSIP * message to minimize the number of messages that are sent to the call agent. The gateway sends the fully wildcarded RSIP * message as long as the following requirements are met:<br>• MGCP is configured for a single profile (or the default profile) only.<br>• A single DS0 group is configured for each DS1.<br>• The single DS0 group includes all the possible DS0s.<br>• All endpoints are in the same service state (when the MGCP call agent is configured for Version RFC 3435-1.0 and the **no** form of this command is issued).<br>If any one of these requirements is not met, the initial RSIP * message is demoted and sent as multiple RSIP messages to the call agent. When demoting, the gateway continues to attempt to minimize the number of RSIP messages. |
| **mdcx-sdp ack-with-sdp** | Forces the gateway to generate a SDP in response to a modify connection (MDCX) message that contains an SDP. The response contains the SDP only if the MDCX is responded to with a positive (200) acknowledgment.<br>By default, or when the **no** form of this command is issued, the positive acknowledgment reply generates an SDP only if any of the parameters have changed from the previous SDP that was generated by the gateway. With this command, even if all the parameters are the same as the previous SDP, the SDP is still generated. This enables operation with a SIP gateway that expects an SDP response to every CRCX or MDCX message. |
| **mode-attrb-in-sdp disable** | Forces the gateway to take connection mode M in Create Connection (CRCX).<br>By default, or when **no** form of this command is issued, preference is given to the connection mode present in SDP. This is only when the mode is present in SDP. |
| **negotiate-nse enable** | Makes MGCP gateway aware of the remote side's Named Signaling Event (NSE) capabilities by examining the remote SDP for NSE capabilities.<br>By default, or when the **no** form of thiscommand is issued, NSE is disabled on the gateway.<br>Cisco Unified Call Manager (UCM) does not support modem or fax passthrough. This feature should not be enabled when Cisco UCM is the call agent. |

| Keywords | Description |
|---|---|
| **private-localhost** | Requires the outgoing messages from the gateway, like Notify (NTFY), RSIP, DLCX, have the private-localhost appended to the endpoint ID.<br>By default, or when the **no** form of this command is issued, the outgoing messages from the gateway have the global router name appended to the endpoint ID.<br>This is applicable for MGCP 0.1 and MGCP 1.0 versions. |
| **q-mode-enduring legacy** | Allows the gateway to keep the current quarantine mode when a request notification (RQNT) does not contain a Q: line. Operation reverts to legacy behavior, which is the following:<br>**Note** Only the first bulleted item results in modified behavior.<br>• No Q: line--Makes no changes to the quarantine mode (whatever mode was set in the previous command persists).<br>• Empty Q: line--Resets the quarantine mode to the default.<br>• Valid Q: line--Sets the quarantine mode per command.<br>• Invalid Q: line--Generates an error.<br>**Note** The quarantine mode is set with the **mgcp quarantine mode** command, and the default is discarded. This is the configuration mode used if the quarantine mode is not specified in the RQNT or embedded request for events.<br>By default, or when the **no** form of this command is issued, MGCP behaves according to both MGCP Version 0.1 and MGCP Version 1.0 specifications--that is, the MGCP gateway resets the quarantine mode to the default in the running configuration if no Q: line is present. |
| **rsip-range** | Determines whether the gateway can generate RSIP messages with endpoint ranges for versions other than Trunking Gateway Control Protocol (TGCP). By default, endpoint ranges are generated in RSIP messages for TGCP only. The following *category* and *version* values can be configured:<br>• **rsip-range all** --Allows the gateway to generate endpoint ranges in RSIP messages for all MGCP versions.<br>• **rsip-range none** --Prevents the gateway from generating endpoint ranges for all MGCP versions, including TGCP.<br>• **rsip-range tgcp-only** --Allows the gateway to generate endpoint ranges in RSIP messages only if the configured protocol is TGCP. This is the default value.<br>TGCP specifications require support for endpoint ranges in RSIP messages. Not all call agents may support this functionality however. In such cases, selecting **none** allows the gateway to interoperate with these call agents. Conversely, if a non-TGCP call agent supports endpoint ranges, selecting **all** allows the gateway to take advantage of this functionality. |

| Keywords | Description |
|---|---|
| **transient-state-response enable** | Forces the gateway to send 400 responses for an MGCP message even if the endpoint is in a transient state.<br>By default, or when **no** form of thiscommand is issued, the gateway does not respond to MGCP messages even if the endpoint is in a transient or disconnecting state. |

The table below describes the MGCP behavior version keywords.

*Table 2: MGCP Behavior Version Keywords*

| Keywords | Description |
|---|---|
| **auep v0.1** | Forces the gateway to reply to an Audit Endpoint (AUEP) command according to the MGCP Version 0.1 specification. This behavior applies specifically to the case in which the endpoint being audited is out of service. If this command is used, an AUEP command on an out-of-service endpoint returns error code of 501.<br>By default, or when the **no** form of this command is issued, MGCP Version 1.0 behavior occurs--that is, response code 200 is sent for all valid endpoints, regardless of their service state, and requested audit information follows. In either case, the configured MGCP version is ignored. |
| **signals v0.1** | Forces the gateway to handle call signaling tones such as ringback, network congestion, reorder, busy, and off-hook warning tones according to the MGCP Version 0.1 specification. The MGCP Version 0.1 specification treats some call signaling tones as on-off tones, which terminate only after a specific MGCP message has been received to stop the signal.<br>By default, or when the **no** form of this command is issued, RFC 3660 is followed, which treats the call signaling tones as timeout tones that terminate when the appropriate timeout expires. In either case, the configured MGCP version is ignored. |

## Examples

The following example shows how the gateway sends MGCP 0.1 responses to AUEP commands:

```
Router(config)# mgcp behavior auep v0.1
```

The following example shows how the gateway provides MGCP 0.1 treatment of call signaling tones:

```
Router(config)# mgcp behavior signals v0.1
```

The following example shows how to disable the requirement that the RSIP be acknowledged before a call agent command is accepted:

```
Router(config)# mgcp behavior ack-init-rsip disable
```

The following example show how to configure the gateway to not demote initial RSIPs based on the service state of the endpoints:

```
Router(config)# mgcp behavior init-rsip-per-insvc legacy
```

The following example shows how to configure the gateway to turn off all signals on receipt of a DLCX:

```
Router(config)# mgcp behavior dlcx-clear-signals all
```

The following examples show how to set quarantine mode to legacy:

```
Router(config)# mgcp behavior q-mode-enduring legacy
```

The following example shows how to force the gateway to generate an SDP in the response to an MDCX with SDP:

```
Router(config)# mgcp behavior mdcx-sdp ack-with-sdp
```

The following example shows how to force the gateway to generate endpoint ranges for all MGCP versions:

```
Router(config)# mgcp behavior rsip-range all
```

The following example shows how to force the gateway not to change the codec payload type when it is dynamically changed in the incoming SDP for all MGCP versions:

```
Router(config)# mgcp behavior dynamically-change-codec-pt disable
```

The following example shows how to force the gateway not to disconnect when it receives DLCX:

```
Router(config)# mgcp behavior fxs-gs emulate-ls-disconnect
```

The following example shows how forces the gateway to send responses for MGCP messages even if the endpoint is in a transient state:

```
Router(config)# mgcp behavior transient-state-response enable
```

The following example shows how to force the gateway to take connection mode M in CRCX:

```
Router(config)# mgcp behavior mode-attrb-in-sdp disable
```

The following example shows how to force the outgoing messages to have the configured private-localhost appended to the endpoint ID for MGCP 0.1 and MGCP 1.0 versions:

```
Router(config)# mgcp behavior private-localhost cisco.com
```

The following example shows how to force the gateway to play a reorder tone when MGCP is still stuck trying to collect digits:

```
Router(config)# mgcp behavior digit-collect-stuck play-reorder
```

The following example shows how to allow the gateway to be aware of NSE capabilities:

```
Router(config)# mccp behavior negotiate-nse enable
```

Use the following commands to display the MGCP behavior and versions settings:

```
Router# show running-config | include behavior
mgcp behavior auep v0.1
mgcp behavior signals v0.1
mgcp behavior ack-init-rsip disable
mgcp behavior init-rsip-per-insvc legacy
mgcp behavior q_mode-enduring legacy
mgcp behavior dlcx-clear-signals all
mgcp behavior mdcx-sdp ack-with-sdp
mgcp behavior rsip-range all
mgcp behaviour dynamically-change-codec-pt disable
mgcp behavior fxs-gs emulate-ls-disconnect
mgcp behavior transient-state-response enable
mgcp behavior mode-attrb-in-sdp-disable
mgcp behavior private-localhost cisco.com
mgcp behavior digit-collect-stuck- play-reorder
mgcp behavior negotiate-nse enable
Router# show running-config | include call-agent
mgcp call-agent ca123.example.net 4040 service-type mgcp version rfc3435-1.0
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Allocates resources for MGCP and starts the MGCP daemon. |
| **mgcp call-agent** | Specifies the address and protocol for the MGCP call agent. |
| **mgcp quarantine mode** | Configures the mode for MGCP quarantined events. |
| **show mgcp** | Displays values for MGCP parameters. |
| **show running-config** | Displays the contents of the currently running configuration file. |

# mgcp behavior comedia-check-media-src

To force IP address and port detection from the first RTP packet received for the entire Media Gateway Control Protocol (MGCP) gateway and enable the callback function selected by MGCP, use the **mgcp behavior comedia-check-media-src** command in global configuration mode.

**mgcp behavior comedia-check-media-src** {**enable** | **disable**}

## Syntax Description

| | |
|---|---|
| **enable** | Forces ip address and port detection. |
| **disable** | Disables ip address and port detection. |

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Use the **mgcp behavior comedia-check-media-src** command to force IP address and port detection from the first rtp packet received for the entire MGCP gateway. This command also enables the callback function selected by MGCP, and with the configuration of the **mgcp behavior comedia-role** command contributes to the determination of whether to populate the SDP direction attribute.

## Examples

The following example shows IP address and port detection being enabled for the entire MGCP gateway:

```
Router(config)# mgcp behavior comedia-check-media-src enable
```

## Related Commands

| Field | Description |
|---|---|
| **mgcp** | Allocates resources for the MGCP and starts the daemon. |
| **mgcp behavior comedia-role** | Specifies the location of the configured MGCP gateway. |
| **mgcp behavior comedia-sdp-force** | Forces the SDP to place the direction attribute in the SDP using the command as a reference. |
| **show mgcp connection** | Displays information for active MGCP-controlled connections. |

# mgcp behavior comedia-role

To specify the location of the configured Media Gateway Control Protocol (MGCP) gateway, use the **mgcp behavior comedia-role** command in global configuration mode.

**mgcp behavior comedia-role** {**active** | **passive** | **none**}

## Syntax Description

| | |
|---|---|
| **active** | Specifies MGCP gateways located inside NAT. |
| **passive** | Specifies MGCP gateways located outside of NAT. |
| **none** | Specifies gateway behavior be as in releases prior to Cisco IOS Release 12.4(11)T. |

## Command Default

**none**

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

This command will specify the location of the configured MGCP gateway and its role in solving the NAT media traversal. A comedia role of **active** is configured for MGCP gateways inside NAT. For gateways located outside of NAT a comedia role of **passive** is configured. Configuring the **none** keyword specifies gateway behavior before the **mgcp behavior comedia-role**command was introduced.

The **mgcp behavior comedia-role**and **mgcp behavior comedia-check-media-src** commands are used to determine when to populate the sdp direction attribute.

## Examples

The following example shows the location of the MGCP gateway configured for MGCP gateways inside NAT:

```
Router(config)# mgcp behavior comedia-role active
```

## Related Commands

| Field | Description |
|---|---|
| **mgcp behavior comedia-check-media-src** | Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway. |
| **mgcp behavior comedia-sdp-force** | Forces the SDP to place the direction attribute in the SDP using the command as a reference. |
| **mgcp** | Allocates resources for the MGCP and starts the daemon. |
| show mgcp | Displays the entire mgcp configuration. |
| **show mgcp connection** | Displays information for active MGCP-controlled connections. |

# mgcp behavior comedia-sdp-force

To force MGCP to place the direction attribute in the Session Description Protocol (SDP), use the **mgcp behavior comedia-sdp-force**command in global configuration mode.

**mgcp behavior comedia-sdp-force** {**enable** | **disable**}

## Syntax Description

| | |
|---|---|
| **enable** | Forces MGCP to place the direction attribute in the SDP. |
| **disable** | Allows the **mgcp behavior comedia-role**, and **mgcp behavior comedia-check-media-src** commands and the remote descriptor to determine if the direction attribute is added to the SDP. |

## Command Default

Disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

This command will force the MGCP to always place the direction attribute in the SDP using the **mgcp behavior comedia-sdp-force** command as a reference. When the **mgcp behavior comedia-sdp-force** command is configured with the **disable** keyword, the **mgcp behavior comedia-role** and **mgcp behavior comedia-check-media-src** commands and the remote descriptor determine if the direction is added to the SDP. If the role is not configured, this command has no effect.

## Examples

The following example configuration forces the direction attribute to be placed in the SDP:

```
Router(config)# mgcp behavior comedia-sdp-force enable
```

## Related Commands

| Field | Description |
|---|---|
| **mgcp** | Allocates resources for the MGCP and starts the daemon. |
| **mgcp behavior comedia-check-media-src** | Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway. |
| **mgcp behavior comedia-role** | Specifies the location of the configured MGCP gateway. |
| **show mgcp connection** | Displays information for active MGCP-controlled connections. |

# mgcp behavior g729-variants static-pt

To change the default from dynamic to static Real-time Transport Protocol (RTP) payload type on G.729 voice codecs, use the **mgcp behavior g729-variants static-pt** command in global configuration mode. To return the default to dynamic, use the **no** form of this command.

**mgcp behavior g729-variants static-pt**
**no mgcp behavior g729-variants static-pt**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is enabled by default, so the RTP payload type on G.729 voice codecs is static.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |
| 12.4(22)T2 12.4(24)T1 | This command was modified to be enabled by default. |

## Usage Guidelines

Prior to Cisco IOS Releases 12.4(22)T2 and 12.4(24)T1, the negotiated value (dynamic) payload type was not set in RTP packets. If you upgraded the Cisco IOS software on your network voice gateways (with existing Cisco Unified Communications Manager) and calls were going between Skinny Client Control Protocol (SCCP) phones controlled by Cisco Unified Communications Manager and public switched telephone network (PSTN) phones connected to a Cisco gateway, a condition of "no audio" could occur. The **mgcp behavior g729-variants static-pt**commandchanges the default from dynamic to static RTP payload type on G.729 voice codecs and eliminates the "no audio" condition.

## Examples

The following example shows how to set the RTP payload type to static for G.729 voice codecs:

```
Router(config)# mgcp behavior g729-variants static-pt
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp codec** | Selects the default codec type and its optional packetization period value. |
| **mgcp rtp payload-type** | Specifies use of the correct RTP payload type for backward compatibility in MGCP networks. |

# mgcp bind

To configure the source address for signaling and media packets to the IP address of a specific interface, use the **mgcp bind**command in global configuration mode. To disable binding, use the **no** form of this command.

**mgcp bind** {**control** | **media**} **source-interface** *interface-id*
**no mgcp bind** {**control** | **media**}

## Syntax Description

| | |
|---|---|
| **control** | Binds only Media Gateway Control Protocol (MGCP) control packets. |
| media | Binds only media packets. |
| **source -interface** | Specifies an interface as the source address of MGCP or Session Initiation Protocol (SIP) packets.<br>**Note** The MGCP Gateway Support for the mgcp bind Command feature does not support SIP. |
| interface-id | Specifies the interface for source address of MGCP packets. The following are valid source addresses:<br>• **Async** --Async interface<br>• **BVI** --Bridge-Group Virtual Interface<br>• **CTunnel** --CTunnel interface<br>• **Dialer** --Dialer interface<br>• **FastEthernet** --Fast Ethernet IEEE 802.3<br>• **Lex** --Lex interface<br>• **Loopback** --Loopback interface<br>• **MFR** --Multilink Frame Relay bundle interface<br>• **Multilink** --Multilink-group interface<br>• **Null** --Null interface<br>• **Serial** --Serial<br>• **Tunnel** --Tunnel interface<br>• **Vif** --PGM Multicast Host interface<br>• **Virtual -Template**--Virtual Template interface<br>• **Virtual -TokenRin**g--Virtual Token Ring |

## Command Default

Binding is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced for MGCP on the Cisco 2400 series, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco IAD2421, Cisco MC3810, and Cisco VG200. |

## Usage Guidelines

If the **mgcp bind** command is not enabled, the IP layer still provides the best local address.

A warning message is displayed if any of the following situations occur:

- When there are active MGCP calls on the gateway, the mgcp bind command is rejected for both control and media.
- If the bind interface is not up, the command is accepted but does not take effect until the interface comes up.
- If the IP address is not assigned on the bind interface, the mgcp bind command is accepted but takes effect only after a valid IP address is assigned. During this time, if MGCP calls are up, the mgcp bind command is rejected.
- When the bound interface goes down, either because of a manual shutdown on the interface or because of operational failure, the bind activity is disabled on that interface.
- When bind is not configured on the media gateway controller (MGC), the IP address used for sourcing MGCP control and media is the best available IP address.

## Examples

The following example shows how the configuration of bind interfaces is shown when show running-config information is viewed:

```
.
.
.
mgcp bind control source-interface FastEthernet0
mgcp bind media source-interface FastEthernet0
.
.
.
```

## Related Commands

| Command | Description |
|---|---|
| show mgcp | Displays values for MGCP parameters. |

# mgcp block-newcalls

To block new calls while maintaining existing calls, use the **mgcp block-newcalls** command in global configuration mode. To resume media gateway control protocol (MGCP) operation, use the **no** form of this command.

**mgcp block-newcalls**
**no mgcp block-newcalls**

## Syntax Description

This command has no arguments or keywords.

## Command Default

New call are not blocked.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the Cisco AS5300. |
| 12.1(3)T | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924. |
| 12.2(11)T | This command was implemented on the Cisco AS5850. |

## Usage Guidelines

This command is valid only if the **mgcp** command is enabled.

Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until participants terminate them or you use the **no mgcp** command. When the last active call is terminated, the MGCP daemon is terminated and all resources that are allocated to it are released. The **no mgcp block-newcalls** command returns the router to normal MGCP operations.

## Examples

The following example prevents the gateway from receiving new calls:

```
Router(config)# mgcp block-newcalls
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Allocates resources for the MGCP and starts the daemon. |

# mgcp call-agent

To configure the address and protocol of the call agent for Media Gateway Control Protocol (MGCP) endpoints on a media gateway, use the **mgcp call-agent** command in global configuration mode. To reset to the default, use the **no** form of this command.

**mgcp call-agent** {*host-nameip-address*} [*port*] [**service-type** *type* [**version** *protocol-version*]]
**no mgcp call-agent**

## Syntax Description

| | |
|---|---|
| *host -name* | Fully qualified domain name (including host portion) for the call agent; for example, ca123.example.net. |
| *ip -address* | IP address for the call agent. |
| *port* | (Optional) User Datagram Protocol (UDP) port over which the gateway sends messages to the call agent. Range is from 1025 to 65535. |
| **service -type** *type* | (Optional) Type of Gateway control service protocol. It can be one of the following values:<br>• **mgcp** --Media Gateway Control Protocol<br>• **ncs** --Network Communication Server<br>• **sgcp** --Simple Gateway Control Protocol<br>• **tgcp** --Trunking Gateway Control Protocol |
| **version** *protocol -version* | (Optional) Version of gateway control service protocol. It can be one of the following values:<br>• For service-type mgcp: 0.1, 1.0, rfc3435-1.0<br>• 0.1--Version 0.1 of MGCP (Internet Draft)<br>• 1.0--Version 1.0 of MGCP (RFC2705 Version 1.0)<br>• rfc3435-1.0--Version 1.0 of MGCP (RFC3435 Version 1.0)<br>**Note** This configuration value is used to allow the router to tailor the MGCP application behavior to be compatible based on the RFC2705 or RFC3435 definitions.<br>• For service-type ncs: 1.0<br>• For service-type sgcp: 1.1, 1.5<br>• For service-type tgcp: 1.0 |

## Command Default

Call-agent UDP port: 2727 for MGCP 1.0, NCS 1.0, and TGCP 1.0 Call-agent UDP port: 2427 for MGCP 0.1 and SGCP Call-agent UDP port: 2427 for Cisco CallManager Service type and version: mgcp 0.1 Service type for Cisco CallManager: mgcp

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the Cisco AS5300. |
| 12.1(3)T | The service-type type keyword and argument were added. |
| 12.1(5)XM | The **version***protocol-version* keyword and argument were added. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.2(2)XA | New service types (ncs and tgcp) and appropriate versions were added. Version 1.0 was added for the mgcp service type. This command was implemented on Cisco 2600 series and Cisco 3600 series routers. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(2)XN | This command was implemented to provide enhanced MGCP voice gateway interoperability on Cisco CallManager Version 3.1 for the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco VG200. |
| 12.2(11)T | This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the Cisco IAD2420 series and Cisco AS5850. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400. |
| 12.3(8)T 1 | This command was modified by adding the RFC3435-1.0 option to the command. |

## Usage Guidelines

Global call-agent configuration (with this command) and call-agent configuration for an MGCP profile (with the **mgcp profile call-agent** command) are mutually exclusive; the first to be configured on an endpoint blocks configuration of the other on the same endpoint.

Identifying call agents by Domain Name System (DNS) name rather than by IP address in the **mgcp call-agent**and **mgcp profile call-agent** commands provides call-agent redundancy, because a DNS name can have more than one IP address associated with it. If a call agent is identified by DNS name and a message from the gateway fails to reach the call agent, the **max1 lookup** and **max2 lookup** commands enable a search from the DNS lookup table for a backup call agent at a different IP address.

The *port* argument configures the call-agent port number (the UDP port over which the gateway sends messages to the call agent). The reverse (the gateway port number, or the UDP port over which the gateway receives messages from the call agent) is configured by specifying a port number in the **mgcp** command.

When the service type is set to mgcp, the call agent processes the restart in progress (RSIP) error messages sent by the gateway if the mgcp sgcp restart notify command is enabled. When the service type is set to sgcp, the call agent ignores the RSIP messages.

Use this command on any platform and media gateway.

The **mgcp**service type supports the RSIP error messages sent by the gateway if the **mgcp sgcp restart notify** command is enabled.

## Examples

The following examples illustrate several formats for specifying the call agent (use any one of these formats):

```
Router(config)# mgcp call-agent 209.165.200.225 service-type mgcp version 1.0
Router(config)# mgcp call-agent 10.0.0.1 2427 service-type mgcp version rfc3435-1.0
Router(config)# mgcp call-agent igloo.northpole.net service-type ncs
Router(config)# mgcp call-agent igloo.northpole.net 2009 service-type sgcp version 1.5
Router(config)# mgcp call-agent 209.165.200.225 5530 service-type tgcp
```

## Related Commands

| Command | Description |
|---|---|
| **call -agent** | Specifies a call-agent address and protocol for an MGCP profile. |
| **debug mgcp events** | Displays debug messages for MGCP events. |
| **max1 lookup** | Enables DNS lookup of the MGCP call agent address when the suspicion threshold is reached. |
| **max2 lookup** | Enables DNS lookup of the MGCP call agent address when the disconnect threshold is reached. |
| **mgcp** | Starts and allocates resources for the MGCP daemon. |
| **mgcp profile** | Initiates MGCP profile mode to create and configure an MGCP profile associated with one or more endpoints, or to configure the default profile. |
| **mgcp sgcp restart notify** | Starts RSIP message processing in the MGCP application.mgcp |
| sgcp restart notify | Enables the MGCP application to process SGCP-type RSIP messages. |

# mgcp codec

To select the codec type and its optional packetization period value, use the **mgcp codec** command in global configuration mode. To set the codec to its default value of G711 u-law, use the **no** form of this command.

**mgcp codec** *type* [**packetization-period** *value*]
**no mgcp codec**

## Syntax Description

| | |
|---|---|
| *type* | Type of codec supported. Valid codecs include the following: G711alaw, G711ulaw, G723ar53, G723ar63, G723r53, G723r63, G729ar8, G729br8, and G729r8. |
| **packetization -period***value* | (Optional) Packetization period. This value is useful when the preferred compression algorithm and packetization period parameter is not provided by the media gateway controller. The range depends on the type of codec selected:<br>• Range for **G729** is 10 to 220 in increments of 10.<br>• Range for **G711** is 10 to 20 in increments of 10.<br>• Range for **G723**is 30 to 330 in increments of 10. |

## Command Default

**G711 u -law codec**

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the Cisco AS5300. |
| 12.1(3)T | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924. |
| 12.1(5)XM | This command was implemented on the Cisco MC3810. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. |
| 12.2(11)T | This command was implemented on the Cisco AS5850. |

## Examples

The following example specifies the codec type:

```
Router(config)# mgcp codec g711alaw
```

The following example sets the codec type and packetization period:

```
Router(config)# mgcp codec g729r8 packetization-period 150
```

### Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |

# mgcp codec gsmamr-nb

To specify the Global System for Mobile Adaptive Multi-Rate Narrow Band (GSMAMR-NB) codec for an MGCP dial peer, use the **mgcp codec gsmamr-nb**command in dial peer voice configuration mode. To disable the GSMAMR-NB codec, use the **no** form of this command.

**mgcp codec gsmamr-nb** [**packetization-period 20**] [**encap rfc3267**] [**frame-format** {**bandwidth-efficient** | **octet-aligned** [{**crc** | **no-crc**}]}] [**modes** *modes-value*]
**no mgcp codec gsmamr-nb**

## Syntax Description

| | |
|---|---|
| **packetization-period 20** | (Optional) Sets the packetization period at 20 ms. |
| **encap rfc3267** | (Optional) Sets the encapsulation value to comply with RFC 3267. |
| **frame-format** | **(Optional) Specifies a frame format. Supported values are octet-aligned and bandwidth-efficient. The default is octet-aligned.** |
| **crc \| no-crc** | **(Optional) CRC is applicable only for octet-aligned frame format. If you enter bandwidth-efficient frame format, the crc \| no-crc options are not available because they are inapplicable.** |
| **modes** | (Optional) The eight speech-encoding modes (bit rates between 4.75 and 12.2 kbps) available in the GSMAMR-NB codec. |
| *modes-value* | (Optional) Valid values are from 0 to 7. You can specify modes as a range (for example, 0-2), or individual modes separated by commas (for example, 2,4,6), or a combination of the two (for example, 0-2,4,6-7). |

## Command Default

Packetization period is **20** ms. Encapsulation is **rfc3267**. Frame format is **octet-aligned**. CRC is **no-crc**. Modes value is **0-7**.

## Command Modes

Dial peer voice configuration (config-dial-peer)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)XW | This command was introduced. |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

## Usage Guidelines

Use the **mgcp codec gsmamr-nb** command to configure the GSMAMR-NB codec and its parameters on the Cisco AS5350XM and Cisco AS5400XM platforms.

## Examples

The following example shows how to set the codec to **gsmamr-nb** and set the parameters:

```
Router(config-dial-peer)# mgcp codec gsmamr-nb packetization-period 20 encap rfc3267
frame-format octet-aligned crc
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |

# mgcp codec ilbc

To specify the internet Low Bandwidth Codec (iLBC) for an MGCP dial peer, use the **mgcp codec ilbc**command in dial peer voice configuration mode. To disable the iLBC, use the **no** form of this command.

**mgcp codec ilbc mode** *frame_size* [**packetization-period** *value*]
**no mgcp codec ilbc**

## Syntax Description

| | |
|---|---|
| **mode** *frame_size* | Specifies the iLBC operating frame mode that is encapsulated in each packet in milliseconds (ms). Valid entries are the following:<br>• 20--20, 40, 60, 80, 100 or 120 ms frames for 15.2 kbps bit rate. Default is 20.<br>• 30--30, 60, 90, or 120 ms frames for 13.33 kbps bit rate. Default is 30. |
| **packetization -period***value* | (Optional) Packetization period. This value is useful when the preferred compression algorithm and packetization period parameter are not provided by the media gateway controller. The range is 20 to120 in increments of 10. |

## Command Default

20ms frames for a 15.2 kbps bit rate.

## Command Modes

Dial peer voice configuration (config-dial-peer)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)XW | This command was introduced. |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

## Usage Guidelines

The iLBC is only supported on Cisco AS5350XM and Cisco AS5400XM Universal Gateways with Voice Feature Cards (VFCs) and IP-to-IP gateways with no transcoding and conferencing.

## Examples

The following example shows how to set the MGCP codec to **ilbc** and set the parameters:

```
Router(config-dial-peer)# mgcp codec ilbc mode 20 packetization-period 60
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |

# mgcp crypto rfc-preferred

To enable support for the media-level Session Description Protocol (SDP) a=crypto attribute on Cisco IOS Media Gateway Control Protocol (MGCP) gateways, use the **mgcp crypto rfc-preferred** command in global configuration mode. To disable support for the a=crypto attribute, use the **no** form of this command.

**mgcp crypto rfc-preferred**
**no mgcp crypto rfc-preferred**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Support for the a=crypto attribute is not enabled on Cisco IOS MGCP gateways.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)XA | This command was introduced. |

## Usage Guidelines

Cryptographic parameters for Secure RTP (SRTP) media sessions are signalled and negotiated using the crypto attribute in the SDP. Some versions of the crytpo attribute syntax set the crypto attribute name to the X-crypto keyword (a=X-crypto). RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams, defines the crypto attribute syntax, where the attribute name is set to the crypto keyword (a=crypto). You use the **mgcp crypto rfc-preferred** command to enable support for the a=crypto attribute on Cisco MGCP gateways.

When support for a=crypto is enabled, the system can choose to use the a=crypto or a=X-crypto notation, depending on the SDP received. By default, if a remote SDP is not present, all SDPs generated by the gateway use the a=crypto notation.

If the command is disabled, the gateway can understand both a=crypto or a=X-crypto in any SDP it receives. However, all SDPs generated by the gateway use the a=X-crypto notation.

You must configure the command based on the notation used by the call agent. For example, the Cisco public switched telephone network (PSTN) gateway (PGW) uses the a=crypto notation and Cisco Unified Call Manager uses the a=X-crypto notation.

## Examples

The following example enables support for the SDP a=crypto attribute on the Cisco IOS MGCP gateway:

```
Router(config)# mgcp crypto rfc-preferred
```

The following is sample output from the **show mgcp** command when support for the SDP a=crypto attribute is enabled on the Cisco IOS MGCP gateway:

```
Router(config)# show mgcp
MGCP rsip-range is enabled for TGCP only.
MGCP Comedia role is NONE
MGCP Comedia check media source is DISABLED
MGCP Comedia SDP force is DISABLED
MGCP Guaranteed scheduler time is DISABLED
MGCP Disconnect delay error recovery DISABLED
MGCP support for a:crypto RFC notation is ENABLED
MGCP DNS stale threshold is 30 seconds
```

## Related Commands

| Command | Description |
|---|---|
| **debug mgcp** | Enables debug traces for MGCP errors, events, media, packets, parser, and CAC. |
| max1 retries | Sets the MGCP suspicion threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for retransmission). |
| max2 retries | Set the MGCP disconnect threshold value (the number of attempts to retransmit messages to a call agent address before performing a new lookup for further retransmission). |
| mgcp | Allocates resources for the MGCP and starts the MGCP daemon. |
| **mgcp block -newcalls** | Blocks new calls while maintaining existing calls. |
| **mgcp ip -tos** | Enables or disables the IP ToS for MGCP connections. |
| mgcp profile | Creates and configures an MGCP profile to be associated with one or more MGCP endpoints or configures the default MGCP profile. |
| **show mgcp** | Displays values for MGCP parameters. |

# mgcp dns stale threshold

To configure the Media Gateway Control Protocol (MGCP) Domain Name System (DNS) stale threshold, use the **mgcp dns stale threshold** command in global configuration mode. To disable the stale threshold configuration, use the **no** form of this command.

**mgcp dns stale threshold** *seconds*
**no mgcp dns stale threshold**

## Syntax Description

| | |
|---|---|
| *seconds* | The threshold time in seconds, that MGCP DNS values are considered stale. The range is from 0 to 600. The default is 300. |

## Command Default

The MGCP DNS threshold value is set to 300 seconds.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(24)T | This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T. |

## Examples

The following example shows how to set the threshold stale time to 44 seconds:

```
Router(config)# mgcp dns stale threshold 44
```

## Related Commands

| Command | Description |
|---|---|
| **show mgcp** | Displays MGCP parameter details. |

# mgcp debug-header

To enable the display of Media Gateway Control Protocol (MGCP) module-dependent information in the debug header, use the **mgcp debug-header** command in global configuration mode. To disable the MGCP module-dependent information, use the **no** form of this command.

**mgcp debug-header**
**no mgcp debug-header**

## Syntax Description

This command has no arguments or keywords.

## Command Default

MGCP module-dependent information in the debug header is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

This command determines whether MGCP module-dependent information is displayed in the standard header for debug output.

## Examples

The following example enables MGCP module-dependent information in debug headers:

```
Router(config)# mgcp debug-header
```

## Related Commands

| Command | Description |
|---|---|
| **debug mgcp all** | Enables all debug traces for MGCP. |
| **debug mgcp endpoint** | Enables debug traces for a specific MGCP endpoint. |
| **mgcp** | Starts the MGCP daemon. |
| **show debugging** | Displays the types of debugging that are enabled. |
| **show mgcp** | Displays the MGCP parameter settings. |
| **voice call debug** | Specifies the format of the debug header. |

# mgcp default-package

To configure the default package capability type for the media gateway, use the **mgcp default-package** command in global configuration mode. This command does not have a **no** form. To change the default package, use the **mgcp default-package** command with a different, actively supported package.

**Residential Gateways**
**mgcp default-package** {**dt-package** | **dtmf-package** | **fxr-package** | **gm-package** | **hs-package** | **line-package** | **ms-package** | **rtp-package**}

**Business Gateways**
**mgcp default-package** {**atm-package** | **dt-package** | **dtmf-package** | **fxr-package** | **gm-package** | **hs-package** | **line-package** | **ms-package** | **rtp-package** | **trunk-package**}

**Trunking Gateways**
**mgcp default-package** {**as-package** | **atm-package** | **dt-package** | **dtmf-package** | **gm-package** | **hs-package** | **md-package** | **mo-package** | **ms-package** | **nas-package** | **rtp-package** | **script-package** | **trunk-package**}

## Syntax Description

| | |
|---|---|
| **as -package** | Announcement server package. |
| **atm -package** | ATM package. |
| **dtmf -package** | DTMF package. |
| **dt -package** | DTMF trunk package (for Channel Associated Signaling (CAS) endpoints). |
| **fxr-package** | FXR package for fax transmissions. |
| **gm -package** | Generic media package. |
| **hs -package** | Handset package. |
| **line -package** | Line package. |
| **md-package** | MD package for Feature Group D (FGD) Exchange Access North American (EANA) signaling. |
| **mo -package** | MF operator services package (for CAS endpoints). |
| **ms -package** | MF wink/immediate start package (for CAS endpoints). |
| **nas -package** | Network access server package. |
| **rtp -package** | RTP package. |
| **script -package** | Script package. |
| **trunk -package** | Trunk package. |

## Command Default

For residential gateways: **line-package** For trunking gateways: **trunk-package**

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the Cisco AS5300. |
| 12.1(3)T | The **line-package** keyword and a distinction between residential and trunking gateways were added. |
| 12.1(5)XM | This command was implemented on the Cisco MC3810 and Cisco 3600 series. The **atm-package**, **hs-package**, **ms-package**, **dt-package**, and **mo-package** keywords were added. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |
| 12.3(1) | The **fxr-package** keyword was added. |
| 12.4(4)T | The **md-package** keyword was added. |

## Usage Guidelines

This command is helpful when the Media Gateway Controller does not provide the package capability to be used for the specific connection.

Before selecting a package as the default, use the **show mgcp** command to ensure that the package is actively supported. If the package you want does not appear in the display, use the **mgcp package-capability** command to add the package to the supported list.

**Note** The CAS packages (**dt-package**, **md-package**, **mo-package**, and **ms-package**) are available only as default package options. They do not appear as options in the **mgcp package-capability** command. This is because the non-CAS packages are configured on a per-gateway basis, whereas the CAS packages are defined on a per-trunk basis. Each trunk is defined using the **ds0-group** command.

If only one package is actively supported, it becomes the default package.

When the FXR package is the default, the call agent omits the "fxr/" prefix on two types of requests in CRCX, MDCX, DLCX, and RQNT messages: requests to detect events ("R:<pkg>/<evt>") and requests to generate events ("S:<pkg>/<evt>"). For example, to ask for T.38 detection, the call agent sends "R:t38" in an RQNT message rather than "R:fxr/t38." Note that the "fxr/fx:" parameter to the Local Connection Options is not affected by selection of FXR as the default package and always needs the "fxr/" prefix.

## Examples

The following example sets the default package:

```
Router(config)# mgcp default-package as-package
! The announcement server package type will be the new default package type.
```

## Related Commands

| Command | Description |
|---|---|
| **ds0-group** | Specifies the DS0 time slots that make up a logical voice port |

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |
| **mgcp package -capability** | Includes a specific MGCP package that is supported by the gateway. |
| **show mgcp** | Displays values for MGCP parameters. |

# mgcp disconnect-delay

To configure the MGCP disconnect delay error recovery mechanism, use the **mgcp disconnect-delay** command in global configuration mode. To disable error recovery, use the **no** form of this command.

**mgcp disconnect-delay** [**timeout** *seconds*]
**no mgcp disconnect-delay**

## Syntax Description

| | |
|---|---|
| **timeout** | (Optional) User defined timeout before the error recovery procedure is initiated. |
| *seconds* | Length of timeout, in seconds before the error recovery procedure is initiated. The range is from 2 to 15. There is no default. |

## Command Default

Disconnect delay error recovery is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T8, 12.4(20)T2 | This command was introduced. |
| 12.4(22)T1 | This command was integrated into Cisco IOS Release 12.4(22)T1. |

## Usage Guidelines

When the FXS telephony endpoint disconnect request exceeds the configured timeout value for completion, the call agent continues to send MGCP messages, which cause the FXS endpoint to eventually block or unregister the gateway. To avoid this situation, configure the gateway with the **mgcp disconnect-delay**command so that the MGCP application initiates the disconnect delay error recovery procedure when the disconnect request takes too long to complete.

When the **mgcp disconnect-delay timeout** command is configured without the optional **timeout**keyword the disconnect delay error recovery mechanism is set to 7 seconds.

## Examples

The following example shows the disconnect delay error recovery mechanism set to the default timeout of 7 seconds:

```
Router(config)# mgcp disconnect-delay
```

The following example shows the disconnect delay error recovery mechanism set with a user-defined 15 seconds:

```
Router(config)# mgcp disconnect-delay timeout 15
```

# mgcp dtmf-relay

To ensure accurate forwarding of digits on compressed codecs, use the **mgcp dtmf-relay** command in global configuration mode. To disable this process for uncompressed codecs, use the **no** form of this command.

**Voice over IP (VoIP)**
**mgcp dtmf-relay voip codec** {**all** | **low-bit-rate**} **mode** {**cisco** | **disabled** | **nse** | **out-of-band** | **nte-gw** | **nte-ca**}
**no mgcp dtmf-relay voip**

**Voice over AAL2 (VoAAL2)**
**mgcp dtmf-relay voaal2 codec** [{**all** | **low-bit-rate**}]
**no mgcp dtmf-relay voaal2**

## Syntax Description

| | |
|---|---|
| **voip** | Specifies VoIP calls. |
| **voaal2** | Specifies voice over AAL2 (VoAAL2) calls (using Annex K type 3 packets). |
| **codec** | Specifies the MGCP DTMF relay codec configuration. |
| **all** | Specifies that dual-tone multifrequency (DTMF) relay is to be used with all voice codecs. |
| **low -bit-rate** | Specifies that the DTMF relay is to be used with only low-bit-rate voice codecs, such as G.729. |
| **mode** | Sets MGCP DTMF relay mode. |
| **cisco** | Specifies that Real-time Transport Protocol (RTP) digit events are encoded using a proprietary format similar to Frame Relay as described in the FRF.11 specification. The events are transmitted in the same RTP stream as nondigit voice samples, using payload type 121. |
| **disabled** | Sets MGCP DTMF relay mode to be disabled. This keyword is available only for the **all** keyword. |
| **nse** | Specifies that named signaling event (NSE) RTP digit events are encoded using the format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples, using the payload type that is configured using the **mgcp tse payload** command. |
| **out -of-band** | Specifies that Media Gateway Control Protocol (MGCP) digit events are sent using Notify (NTFY) messages to the call agent, which plays them on the remote gateway using Request Notification (RQNT) messages with **S:** (signal playout request). |
| **nte-gw** | Specifies that RTP digit events are encoded using the named telephony event (NTE) format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples. The payload type is negotiated by the gateways before use. The configured value for payload type is presented as the preferred choice at the beginning of the negotiation. |
| **nte-ca** | Behaves similar to the **nte-gw** keyword except that the call agent's local connection options **a:** line is used to enable or disable DTMF relay. |

## Command Default

For the Cisco 7200 series router, the command is disabled. For all other platforms, noncompressed codecs are disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.1(5)XM | This command was integrated into Cisco IOS Release 12.1(5)XM and implemented on the Cisco MC3810. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. The voaal2 keyword was added. |
| 12.2(2)XB | This command was modified. The **nte-gw** and **nte-ca** keywords were added to this command. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(2)XN | This command was integrated into Cisco IOS Release 12.2(2)XN and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco Voice Gateway 200 (Cisco VG200). |
| 12.2(11)T | This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 2.0. This command was implemented on the following platforms: Cisco AS5300, Cisco AS5400, Cisco AS5850, and Cisco IAD2420. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T and implemented on the Cisco 1751 and Cisco 1760. |
| 15.0(1)M | This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **disabled** keyword was added. |

## Usage Guidelines

Use this command to access an announcement server or a voice-mail server that cannot decode RTP packets containing DTMF digits. When the **mgcp dtmf-relay** command is active, the DTMF digits are removed from the voice stream and carried so that the server can decode the digits.

Only VoIP supports the **mode** keyword for forwarding digits on codecs.

## Examples

The following example shows how to remove the DTMF tone from the voice stream and send FRF.11 with a special payload for the DTMF digits:

```
Router(config)# mgcp dtmf-relay codec mode cisco
```

The following example shows how to configure a low-bit-rate codec using VoIP in NSE mode:

```
Router(config)# mgcp dtmf-relay voip codec low-bit-rate mode nse
```

The following example shows how to configurev a codec for VoAAL2:

```
Router(config)# mgcp dtmf-relay voaal2 codec all
```

The following example shows how to configure a low-bit-rate codec using VoIP in NSE mode:

```
Router(config)# mgcp dtmf-relay voip codec low-bit-rate mode nse
```

The following example shows how to set the DTMF relay codec and mode to gateway:

```
Router(config)# mgcp dtmf-relay codec mode nte-gw
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |

# mgcp endpoint offset

To enable incrementing of the POTS or DS0 portion of an endpoint name when using the Network-based Call Signaling (NCS) 1.0 profile of Media Gateway Control Protocol (MGCP), use the **mgcp endpoint offset** command in global configuration mode. To reset to the default, use the **no** form of this command.

**mgcp endpoint offset**
**no mgcp endpoint offset**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XA | This command was introduced. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |

## Usage Guidelines

This command is used with NCS 1.0 to increment the POTS or DS0 portion of an endpoint name by 1 to minimize potential interoperability problems with call agents (media gateway controllers).

NCS 1.0 mandates that the port number of an endpoint be based on 1, and port numbering on some gateway platforms is based on 0.

When this command is configured, it offsets all endpoint names on the gateway. For example, an endpoint with a port number of aaln/0 is offset to aaln/1, and a DS0 group number of 0/0:0 is offset to 0/0:1.

## Examples

The following example enables incrementing the port number portion of an endpoint name:

```
Router(config)# mgcp endpoint offset
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts and allocates resources for the MGCP daemon. |

# mgcp explicit hookstate

To enable detection of explicit hookstates, use the **mgcp explicit hookstate** command in global configuration mode. To disable hookstate detection, use the **no** form of this command.

**mgcp explicit hookstate**
**no mgcp explicit hookstate**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Hookstate detection is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)XM | This command was introduced. |
| 12.2(2)T | This command was implemented on the Cisco 7200 series. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |

## Usage Guidelines

Explicit hookstate detection is enabled by default. In this state, the gateway returns a "401 endpoint already off hook" or "402 endpoint already on hook" NACK (Not Acknowledged) response to R:hu or R:hd event requests.

If you turn hookstate detection off with the **no**form of the **mgcp explicit hookstate** command, the hookstate is not checked when the gateway receives R:hu or R:hd event requests. The gateway acknowledges (ACK) these event requests.

## Examples

The following example enables hookstate detection:

```
Router(config)# mgcp explicit hookstate
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |

# mgcp fax rate

To establish the maximum fax rate for Media Gateway Control Protocol (MGCP) T.38 sessions, use the **mgcp fax rate** command in global configuration mode. To reset MGCP endpoints to their default fax rate, use the **no** form of this command.

**mgcp fax rate** {**2400** | **4800** | **7200** | **9600** | **12000** | **14400** | **voice**}
**no mgcp fax rate**

## Syntax Description

| | |
|---|---|
| **2400** | Maximum fax transmission speed of 2400 bits per second (bps). |
| **4800** | Maximum fax transmission speed of 4800 bps. |
| **7200** | Maximum fax transmission speed of 7200 bps. |
| **9600** | Maximum fax transmission speed of 9600 bps. |
| **12000** | Maximum fax transmission speed of 12,000 bps. |
| **14400** | Maximum fax transmission speed of 14,400 bps. |
| **voice** | Highest possible transmission speed allowed by the voice codec. This is the default. |

## Command Default

MGCP fax rate is set to the highest possible transmission speed allowed by the voice codec (**mgcp fax rate voice**).

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |

## Usage Guidelines

Use this command to specify the maximum fax transmission rate for all MGCP endpoints in the gateway.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher transmission speed values (14,400 bps) provide a faster transmission speed but use a significantly large portion of the available bandwidth. A lower transmission speed value (2400 bps, for example) provides a slower transmission speed but uses a smaller portion of the available bandwidth.

**Note** MGCP fax rate does not support call admission and control or bandwidth allocation.

When the MGCP fax rate is set to the highest possible transmission speed allowed by the voice codec (**mgcp fax rate voice**), all MGCP endpoints limit T.38 fax calls to this speed. For example, if the voice codec is G.711, fax transmission may occur up to 14,400 bps because 14,400 bps is less than the 64-kbps voice rate. If the voice codec is G.729 (8 kbps), the fax transmission speed is limited to the nearest fax rate of 7200 bps.

**Tip** If the fax rate transmission speed is set higher than the codec rate in the same dial peer, the data sent over the network for fax transmission will be greater than the bandwidth reserved for Resource Reservation Protocol (RSVP). The **mgcp fax rate** command sets a maximum fax rate for T.30 negotiation (DIS/DCS). Fax machines can negotiate a lower rate, but not a higher rate.

Only values other than the default value appear in the saved gateway configuration.

## Examples

The following example configures a maximum fax rate transmission speed of 9600 bps for MGCP T.38 fax relay sessions:

```
Router(config)# mgcp fax rate 9600
```

The following example configures the maximum fax rate transmission speed to 12,000 bps for MGCP T.38 fax relay sessions:

```
Router(config)# mgcp fax rate 12000
```

## Related Commands

| Command | Description |
|---|---|
| **show call active fax** | Displays the maximum fax rate for the current T.38 fax session. |
| **show mgcp** | Displays the current configuration for the MGCP fax rate. |

# mgcp fax-relay

To allow for the suppression of tones from the fax machine side so that Super Group 3 (SG3) fax machines can negotiate down to G3 speeds for Media Gateway Control Protocol (MGCP) fax relay, use the **mgcp fax-relay**commandinglobal configuration mode. To disable this function, use the **no** form of this command.

**mgcp fax-relay** {**ans-disable** | **sg3-to-g3**}
**no mgcp fax-relay** {**ans-disable** | **sg3-to-g3**}

## Syntax Description

| | |
|---|---|
| **ans-disable** | Suppresses ANS tones from originating SG3 fax machines so that these machines can operate at G3 speeds using fax relay. |
| **sg3-to-g3** | Allows SG3 machines to negotiate down to G3 speeds using fax relay. |

## Command Default

If this command is not enabled, modem upspeed can occur when ANS tones are detected and SG3-to-SG3 fax relay communication is not supported and probably will fail.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced as the **mgcp fax-relay sg3-to-g3** command. |
| 12.4(6)T | This feature was implemented on the Cisco 1700 series and Cisco 2800 series. |
| 12.4(20)T1 | The **ans-disable** keyword was added. |
| 12.4(24)T | This command was integrated into Cisco IOS Release 12.4(24)T. |

## Usage Guidelines

When the **mgcp fax-relay ans-disable** command is entered, modem upspeed does not occur when an ANS tone is detected. When the **ans-disable** keyword is entered, the modem-related sessions will fail because the ANS tones are squelched at the digital signal processor (DSP) level by the TI C5510 DSP.

When the **mgcp fax-relay sg3-to-g3** command is entered, the DSP fax-relay firmware suppresses the V.8 CM tone and the fax machines negotiate down to G3 speeds for the fax stream.

## Examples

The following global configuration output shows V.8 fax CM message suppression being enabled on the voice dial peer for MGCP signaling types:

```
Router(config)# mgcp fax-relay sg3-to-g3
```

## Related Commands

| Command | Description |
|---|---|
| **fax-relay** (voice-service) | Allows ANS tones to be disabled for SG3 machines to operate at G3 speeds using fax relay and to enable the fax stream between two SG3 fax machines to negotiate down to G3 speeds on a VoIP dial peer. |

| Command | Description |
|---|---|
| **mgcp fax t38** | Specifies MGCP fax T.38 parameters. |

# mgcp fax t38

To configure MGCP fax T.38 parameters, use the **mgcp fax t38**command in global configuration mode. return a parameter to its default, use the **no** form of this command.

**mgcp fax t38** {**ecm** | **gateway force** | **hs_redundancy** *factor* | **inhibit** | **ls_redundancy** *factor* | **nsf** *hexcode*}
**no mgcp fax t38** {**ecm** | **gateway force** | **hs_redundancy** | **inhibit** | **ls_redundancy** | **nsf**}

## Syntax Description

| | |
|---|---|
| **ecm** | Enables error correction mode (ECM) for the gateway. By default, ECM is not enabled. |
| **gateway force** | Forces gateway-controlled T.38 fax relay using Cisco-proprietary named signaling events (NSEs) even if the capability to use T.38 and NSEs cannot be negotiated by the MGCP call agent at call setup time. The default is that force is not enabled. |
| **hs_redundancy** *factor* | Sends redundant T.38 fax packets. Refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. For the **hs_redundancy** parameter, the *factor* range is from 0 through 2. The default is 0 (no redundancy).<br>**Note** Setting the **hs_redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call. |
| **inhibit** | Disables use of T.38 for the gateway. By default, T.38 is enabled.<br>**Note** If the MGCP gateway uses the auto-configuration function, the **mgcp fax t38 inhibit**command is automatically configured on the gateway each time a new configuration is downloaded. Beginning with Cisco IOS Software Release 12.4T, the auto-configuration of this command is removed. For MGCP gateways using auto-cofiguration and running Cisco IOS version 12.4T or later, you must manually configure the **mgcp fax t38 inhibit**command to use T.38 fax relay. |
| **ls_redundancy** *factor* | Sends redundant T.38 fax packets. The **ls_redundancy** parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the **ls_redundancy** parameter, the *factor* range is from 0 through 2. Default is 0 (no redundancy). |
| **nsf** *hexcode* | Overrides the nonstandard facilities (NSF) code with the code provided using the *hexcode* argument. The *word* argument is a two-digit hexadecimal country code and a four-digit hexadecimal manufacturer code. By default, the NSF code is not overridden. |

## Command Default

**ecm** --disabled**gateway force**--disabled**hs_redundancy**--0**inhibit**--disabled (T.38 is enabled. See note in above table.)**ls_redundancy**--0**nsf**--not overridden

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XB | This command was introduced. |

| Release | Modification |
|---|---|
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release. |
| 12.2(11)T | This command was applicable to the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 in this release. |
| 12.2(11)T2 | This command was modified. The **gateway force** keyword pair was introduced. |
| 12.2(15)T | This command was implemented on the Cisco 1751 and Cisco 1760. |
| 12.4T | This command was modified. The **mgcp fax t38 inhibit**command was no longer configured by default for MGCP gateways that use the auto-configuration function. |

## Usage Guidelines

Nonstandard facilities (NSF) are capabilities a particular fax manufacturer has built into a fax machine to distinguish products from each other.

To disable T.38 fax relay, use the **mgcp fax t38 inhibit** command.

Some MGCP call agents do not properly pass those portions of Session Description Protocol (SDP) messages that advertise T.38 and NSE capabilities. As a result, gateways that are controlled by these call agents are unable to use NSEs to signal T.38 fax relay to other gateways that use NSEs. The **mgcp fax t38 gateway force** command provides a way to ensure gateway-controlled T.38 fax relay and use of NSEs between an MGCP gateway and another gateway. The other gateway can be an H.323, Session Initiation Protocol (SIP), or MGCP gateway. Both gateways must be configured to use NSEs to signal T.38 fax relay mode switchover. On H.323 and SIP gateways, use the **fax protocol t38 nse force**command to specify the use of NSEs for T.38 fax relay. On MGCP gateways, use the **mgcp fax t38 gateway force** command.

## Examples

The following example configures the gateway to use NSEs for gateway-controlled T.38 fax relay signaling:

```
Router(config)# mgcp fax t38 gateway force
```

The following example shows that MGCP T.38 fax relay and ECM are enabled, NSF override is disabled, and low- and high-speed redundancy are set to the default value of 0:

```
Router(config)# mgcp fax t38 ecm

Router(config)# exit

Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 172.18.195.147 2436 Initial protocol service is MGCP 0.1
MGCP block-newcalls DISABLED
MGCP send RSIP for SGCP is DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: CA, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough mode: NSE, codec: g711ulaw
MGCP TSE payload: 119
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer disabled
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: DISABLED
MGCP piggyback msg ENABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp DISABLED
MGCP undotted-notation DISABLED
MGCP codec type g729r8, MGCP packetization period 10
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lmw 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP RTP precedence 5, MGCP signaling precedence: 3
MGCP default package: dt-package
MGCP supported packages: gm-package dtmf-package trunk-package line-package
                         hs-package rtp-package as-package atm-package ms-package
                         dt-package mo-package res-package mt-package
                         dt-package mo-package res-package mt-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0
MGCP T.38 Fax High Speed Redundancy: 0
```

The following example shows that NSF is overridden:

```
MGCP T.38 Fax NSF Override is ENABLED: AC04D3
```

## Related Commands

| Command | Description |
|---|---|
| **fax protocol** | Specifies fax protocol parameters on H.323 and SIP gateways. |

# mgcp ip qos dscp

To configure Differentiated Services Code Point (DSCP) for Media Gateway Control Protocol (MGCP) packets, use the **mgcp ip qos dscp** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**mgcp ip qos dscp** {*dscp-valueaf-numbercs-number* | **default** | **ef**} {**media** | **signaling**}
**no mgcp ip qos dscp** {*dscp-valueaf-numbercs-number* | **default** | **ef**} {**media** | **signaling**}

## Syntax Description

| | |
|---|---|
| *dscp-value* | DSCP value. The range is from 0 to 63. |
| *af-number* | Assured forwarding bit pattern. The assure forwarding bit patterns are as follows:<br>• **af11**<br>• **af12**<br>• **af13**<br>• **af21**<br>• **af22**<br>• **af23**<br>• **af31**<br>• **af32**<br>• **af33**<br>• **af41**<br>• **af42**<br>• **af43**<br>For more information, use the question mark (?) online help function. |
| *cs-number* | Class selector code point. The class selector code points are as follows:<br>• **cs1**<br>• **cs2**<br>• **cs3**<br>• **cs4**<br>• **cs5**<br>• **cs6**<br>• **cs7**<br>For more information, use the question mark (?) online help function. |

| | |
|---|---|
| **default** | Sets the DSCP to the default bit pattern. For more information, use the question mark (?) online help function. |
| **ef** | Sets the DSCP to the expedited forwarding bit pattern. For more information, use the question mark (?) online help function. |
| **media** | Applies DSCP to media payload packets. |
| **signaling** | Applies DSCP to signaling packets. |

## Command Default

DSCP is applied to media payload packets and signaling packets.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

The **mgcp ip qos dscp** command is used to set the DSCP for the quality of service. This command provides voice and signaling traffic priorities.

## Examples

The following example shows how to configure DSCP for MGCP packets:

```
Router# configure terminal
Router(config)# mgcp ip qos dscp af31 signaling
```

## Related Commands

| Command | Description |
|---|---|
| **show mgcp** | Displays values for MGCP parameters. |

# mgcp ip-tos

To enable or disable the IP type of service (ToS) for media gateway control protocol (MGCP) connections, use the **mgcp ip-tos** command in global configuration mode. To restore the default, use the **no** form of this command.

**mgcp ip-tos** {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*}
**no mgcp ip-tos** {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*}

## Syntax Description

| | |
|---|---|
| **high -reliability** | High-reliability ToS. |
| **high -throughput** | High-throughput ToS. |
| **low -cost** | Low-cost ToS. |
| **low -delay** | Low-delay ToS. |
| **rtp precedence** *value* | Value of the Real-Time Transport Protocol (RTP) IP precedence bit. Range is from 0 to 7. The default is 3.<br>**Note** In Cisco IOS Release 12.1(3)T, this parameter was **precedence** *value*. |
| **signaling precedence** *value* | IP precedence value for MGCP User Datagram Protocol (UDP) and Real-Time Transport Protocol Control Protocol (RTCP) signaling packets. Range is from 0 to 7. The default is 3. |

## Command Default

Services are disabled. RTP precedence: 3 Signaling precedence: 3

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the Cisco AS5300. |
| 12.1(3)T | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924. |
| 12.1(5)XM | This command was implemented on the Cisco MC3810. The **precedence**parameter was changed to **rtp precedence** and the **signaling precedence** parameter was added. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |

## Usage Guidelines

Only one of the keywords in the group **high-reliability**, **high-throughput**, **low-cost**, and **low-delay** can be enabled at any given time. Enabling one keyword disables any other that was active. Enabling one of these keywords has no effect on the **precedence** value.

The **no** form of the **mgcp ip-tos** command disables the first four keywords and sets **the precedence value**back to 3.

When you configure a new value for **precedence**, the old value is erased.

## Examples

The following example activates the **low-delay** keyword and disables the previous three keywords:

```
Router(config)# mgcp ip-tos high-rel
Router(config)# mgcp ip-tos high-throughput
Router(config)# mgcp ip-tos low-cost
Router(config)# mgcp ip-tos low-delay
Router(config)# mgcp ip-tos rtp precedence 4
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |

# mgcp lawful-intercept

To enable the lawful-intercept feature for the Media Gateway Control Protocol (MGCP), use the **mgcp lawful-intercept**command in global configuration mode. To disable the feature in mgcp, use the **no** form of this command.

**mgcp lawful-intercept**
**no mgcp lawful-intercept**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Lawful Intercept feature is enabled in mgcp.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Usage Guidelines

The Lawful Intercept feature is the process law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications as authorized by judicial or administrative order. By default the **lawful-intercept** feature is enabled in mgcp. The **no mgcp lawful-intercept** command is used to disable the lawful-intercept feature in mgcp.

## Examples

The following example shows the electronic surveillance being disabled:

```
Router(config)# no mgcp lawful-intercept
```

## Related Commands

| Command | Description |
|---|---|
| **debug mgcp** | Enables debugging on MGCP. |
| **show mgcp** | Displays the MGCP parameter settings. |

# mgcp max-waiting-delay

To specify the media gateway control protocol (MGCP) maximum waiting delay (MWD), use the **mgcp max-waiting-delay** command in global configuration mode. To reset to the default, use the **no** form of this command.

**mgcp max-waiting-delay** *milliseconds*
**no mgcp max-waiting-delay**

## Syntax Description

| | |
|---|---|
| *milliseconds* | Time, in milliseconds, to wait after restart. Range is from 0 to 600000 (600 seconds). The default is 3000 (3 seconds). |

## Command Default

3000 ms

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced on the Cisco AS5300. |
| 12.1(3)T | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924. |
| 12.2(11)T | This command was implemented on the Cisco AS5850. |

## Usage Guidelines

Use this command to send out an Restart in Progress (RSIP) message to the call agent with the restart method. This command helps prevent traffic bottlenecks caused by MGCP gateways all trying to connect at the same time after a restart.

## Examples

The following example sets the MGCP maximum waiting delay to 600 ms:

```
Router(config)# mgcp max-waiting-delay 600
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |
| **mgcp restart -delay** | Configures the graceful teardown method sent in the RSIP message. |

# mgcp modem passthrough codec

To select the codec that enables the gateway to send and receive modem and fax data in VoIP and VoATM adaptation layer 2 (VoAAL2) configurations, use the **mgcp modem passthrough codec**command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

**mgcp modem passthrough** {**voip** | **voaal2**} **codec** {**g711alaw** | **g711ulaw**}
**no mgcp modem passthrough** {**voip** | **voaal2**}

## Syntax Description

| | |
|---|---|
| **voip** | VoIP voice protocol. |
| **voaal2** | VoAAL2 voice protocol. |
| **g711alaw** | G.711 a-law codec for changing speeds during modem and fax switchover. |
| **g711ulaw** | G.711 u-law codec for changing speeds during modem and fax switchover. |

## Command Default

**The g711 u-law** codec for both VOIP and VOAAL2

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.1(5)XM | This command was implemented on the Cisco MC3810. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |

## Usage Guidelines

Use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. Selecting a codec dynamically changes the codec type and speed to meet network conditions.

## Examples

The following example enables a gateway to send and receive VoAAL2 modem or fax data using the G711 a-law codec:

```
Router(config)# mgcp modem passthrough voaal2 codec g711alaw
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |
| **mgcp modem passthrough mode** | Sets the method for changing speeds for modem and fax transmissions on the gateway. |
| **mgcp quarantine persistent -events disable** | Enables redundancy for VoIP modem and fax transmissions. |

| Command | Description |
|---|---|
| **mgcp tse payload** | Enables the TSE payload for modem and fax operation. |

# mgcp modem passthrough mode

To set the method for changing speeds that enables the gateway to send and receive modem and fax data in VoIP and VoATM adaptation layer 2 (VoAAL2) configurations, use the **mgcp modem passthrough mode**command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

**mgcp modem passthrough** {**voip** | **voaal2**} **mode** {**cisco** | **nse**}
**no mgcp modem passthrough** {**voip** | **voaal2**}

## Syntax Description

| | |
|---|---|
| **voip** | VoIP. |
| **voaal2** | Voice over AAL2 calls using Annex K type 3 packets. |
| **cisco** | Cisco-proprietary method for changing modem speeds, based on the protocol. |
| **nse** | Named signaling event (NSE)-based method for changing modem speeds. For VoAAL2 configurations, AAL2 Annex K (type 3) is used. |

## Command Default

**NSE-based method**

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.1(5)XM | This command was implemented on the Cisco MC3810. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series router. |
| 12.2(11)T | This command was implemented on the Cisco AS5300 and Cisco AS5850. |

## Usage Guidelines

Use this command for fax pass-through because the answer tone can come from either modem or fax transmissions.

Upspeed is the method used to change the codec type and speed dynamically to meet network conditions.

If you use the **nse** keyword, you must also use the **mgcp tse payload** command.

If you use the default **nse** keyword and the **voip** or **voaal2** keyword, the **show run** command does *not* display the **mgcp modem passthrough mode** command in the configuration output, although the command is displayed for the **cisco**keyword. The **show mgcp** command displays settings for both the **nse** and **cisco** keywords.

## Examples

The following example enables a gateway to send and receive VoIP modem or fax data using the NSE modem-speed-changing method:

```
Router(config)# mgcp modem passthrough voip mode nse
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |
| **mgcp modem passthrough codec** | Selects the codec to use for modem and fax transmissions on the gateway. |
| **mgcp quarantine persistent -events disable** | Enables redundancy for VoIP modem and fax transmissions. |
| **mgcp tse payload** | Enables the TSE payload for modem and fax operation. |

# mgcp modem passthrough voip redundancy

To enable redundancy on a gateway that sends and receives modem and fax data in VoIP configurations, use the **mgcp modem passthrough voip redundancy**command in global configuration mode. To disable redundancy, use the **no** form of this command.

**mgcp modem passthrough voip redundancy** [**sample-duration** [{**10** | **20**}]] [**maximum-sessions** *number*]
**no mgcp modem passthrough voip redundancy** [**sample-duration** [{**10** | **20**}]] [**maximum-sessions** *number*]

## Syntax Description

| | |
|---|---|
| **sample-duration** | (Optional) Specifies the time length of the largest Real-time Transport Protocol (RTP) packet when packet redundancy is active, in milliseconds (ms). |
| **10** \| **20** | (Optional) Specifies the redundancy sample duration in milliseconds (ms). The default sample duration is 10. |
| **maximum-sessions** | (Optional) Specifies the maximum number of redundant sessions that can run simultaneously on each subsystem. |
| *number* | Number of maximum modem passthrough sessions on each module. The range is from 1 to 30. |

## Command Default

The default redundancy sample duration is 10 milliseconds (ms).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(5)XM | This command was introduced. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. |
| 12.2(11)T | This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5300 and Cisco AS5850. |
| 15.0(1)M | This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The *number*argument and the following keywords were added:<br>• **sample-duration**<br>• **10** \| **20**<br>• **maximum-sessions** |

## Usage Guidelines

Use the **modem passthrough voip redundancy**command for fax pass-through because the answer tone can come from either modem or fax transmissions. This command enables a single repetition of packets (using

RFC 2198) to improve reliability by protecting against packet loss. When redundancy is on, all calls on the gateway are affected.

Upspeed is the method used to dynamically change the codec type and speed to meet network conditions.

## Examples

The following example shows how to enable redundancy for VoIP modem and fax transmissions on a gateway:

```
Router(config)# mgcp modem passthrough voip redundancy sample-duration 20
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |
| **mgcp modem passthrough codec** | Selects the codec for modem and fax transmissions. |
| **mgcp modem passthrough mode** | Sets the method for changing speeds for modem and fax transmissions on the gateway. |
| **mgcp tse payload** | Enables the TSE payload for modem and fax operation. |

# mgcp modem passthru

To enable the gateway to send and receive modem and fax data, use the **mgcp modem passthru** command in global configuration mode. To disable support for modem and fax data, use the **no** form of this command.

**mgcp modem passthru** {**cisco** | **ca**}
**no mgcp modem passthru**

## Syntax Description

| | |
|---|---|
| **cisco** | When the gateway detects a modem/fax tone, it switches the codec to G.711 to allow the analog data to pass through. |
| **ca** | When the gateway detects a modem/fax tone, it alerts the call agent to switch the codec to G.711 to allow the analog data to pass through. |

## Command Default

**ca**

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was added to MGCP. |
| 12.2(11)T | This command was implemented on the Cisco AS5850. |

## Usage Guidelines

When the **cisco** keyword is activated and the gateway detects a modem/fax tone, the gateway switches the codec to G.711 then sends the analog data to a remote gateway. The remote gateway also switches the codec on its side of the call to G.711 to allow the analog data to pass through.

When the **ca**keyword is activated and the gateway detects a modem/fax tone, the gateway alerts the call agent to switch the codec to G.711 to allow the analog data to pass through. The call agent must send an MDCX signal to the G.711 codec for successful data pass-through.

## Examples

The following example configures a gateway to send and receive modem or fax data:

```
Router(config)# mgcp modem passthru cisco
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp** | Starts the MGCP daemon. |

# mgcp modem relay voip gateway-xid

To enable in-band negotiation of compression parameters between two VoIP gateways using Media Gateway Control Protocol (MGCP), use the **mgcp modem relay voip gateway-xid** command in global configuration mode. To disable this function, use the **no** form of this command.

**mgcp modem relay voip gateway-xid** [**compress** {**backward** | **both** | **forward** | **no**}] [**dictionary** *value*] [**string-length** *value*]
**no mgcp modem relay voip gateway-xid**

## Syntax Description

| | |
|---|---|
| **compress** | (Optional) Direction in which data flow is compressed. For normal dialup, compression should be enabled in both directions.<br>You may want to disable compression in one or more directions. This is normally done during testing and perhaps for gaming applications, but not for normal dialup when compression is enabled in both directions.<br>• **backward** --Enables compression only in the backward direction.<br>• **both** --Enables compression in both directions. For normal dialup, this is the preferred setting. This is the default.<br>• **forward** --Enables compression only in the forward direction.<br>• no--Disables compression in both directions. |
| **dictionary** *value* | (Optional) V.42*bis* parameter that specifies characteristics of the compression algorithm. Range is from 512 to 2048. Default is 1024.<br>**Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup. |
| **string -length***value* | (Optional) V.42*bis* parameter that specifies characteristics of the compression algorithm. Range is from 16 to 32. Default is 32.<br>**Note** Your modem may support values higher than this range. A value acceptable to both sides is negotiated during modem call setup. |

## Command Default

Command: enabled Compress: both Dictionary: 1024 String length: 32

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300. |

## Usage Guidelines

This command enables XID negotiation for modem relay. By default it is enabled.

This command affects only VoIP calls and not Voice over ATM adaption layer 2 (VoAAL2) calls. This is because MGCP supports VoAAL2 calls for voice and fax/modem, but not for modem relay.

If this command is enabled on both VoIP gateways of a network, the gateways determine whether they need to engage in in-band negotiation of various compression parameters. The remaining keywords in this command specify the negotiation posture of this gateway in the subsequent in-band negotiation (assuming that in-band negotiation is agreed on by the two gateways).

The **compress**, **dictionary**, and **string-length** keywords are digital-signal-processor (DSP)-specific and related to xid negotiation. If this command is disabled, they are all irrelevant. The application (MGCP or H.323) just passes these configured values to the DSPs, and it is the DSP that requires them.

## Examples

The following example enables in-band negotiation of compression parameters on the VoIP gateway, with compression in both directions, dictionary size of 1024, and string length of 32 for the compression algorithm:

```
mgcp modem relay voip gateway-xid compress both dictionary 1024 string-length 32
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp modem relay voip mode** | Enables modem relay mode support in a gateway for MGCP VoIP calls. |
| **mgcp modem relay voip sprt retries** | Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting. |
| **modem relay gateway-xid** | Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP. |
| **mgcp tse payload** | Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP. |

# mgcp modem relay voip latency

To optimize the Modem Relay Transport Protocol and the estimated one-way delay across the IP network using Media Gateway Control Protocol (MGCP), use the **mgcp modem relay voip latency** command in global configuration mode. To disable this function, use the **no** form of this command.

**mgcp modem relay voip latency** *value*
**no mgcp modem relay voip latency**

## Syntax Description

| | |
|---|---|
| *value* | Estimated one-way delay across the IP network, in milliseconds. Range is from 100 to 1000. Default is 200. |

## Command Default

200 ms

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300. |

## Usage Guidelines

Use this command to adjust the retransmission timer of the Simple Packet Relay Transport (SPRT) protocol, if required, by setting the value to the estimated one-way delay (in milliseconds) across the IP network. Changing this value may affect the throughput or delay characteristics of the modem relay call. The default value of 200 does not need to be changed for most networks.

## Examples

The following example sets the estimated one-way delay across the IP network to 100 ms.

```
mgcp modem relay voip latency 100
```

## Related Commands

| Command | Description |
|---|---|
| mgcp modem relay voip mode | Enables modem relay mode support in a gateway for MGCP VoIP calls. |
| mgcp modem relay voip sprt retries | Sets the maximum number of times that the SPRT protocol tries to send a packet before disconnecting. |
| mgcp tse payload | Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP. |
| modem relay gateway-xid | Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP. |
| modem relay latency | Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network. |

# mgcp modem relay voip mode

To enable named signaling event (NSE) based modem relay mode for VoIP calls on a Media Gateway Control Protocol (MGCP) gateway, use the **mgcp modem relay voip mode** command in global configuration mode. To disable this function, use the **no** form of this command.

**mgcp modem relay voip mode** [**nse**] **codec** [{**g711alaw** | **g711ulaw**}] [**redundancy**] **gw-controlled**
**no mgcp modem relay voip mode**

## Syntax Description

| | |
|---|---|
| **nse** | (Optional) Instructs the gateway to use NSE mode for upspeeding. |
| **codec** | (Optional) Specifies a codec to use for upspeeding:<br>• **g711alaw** --G.711 a-law 64,000 bits per second (bps) for E1.<br>• **g711ulaw** --G.711 mu-law 64,000 bps for T1. This is the default. |
| **redundancy** | (Optional) Specifies packet redundancy for modem traffic during modem pass-through. By default, redundancy is disabled. |
| **gw-controlled** | Specifies the gateway-configured method for establishing modem relay parameters. |

## Command Default

Modem relay in NSE mode is disabled. All modem calls go through as pass-through calls, which are less reliable and use more bandwidth than modem relay calls, provided that pass-through is enabled. The G.711 mu-law codec is used for upspeeding. Redundancy is disabled and no duplicate data packets are sent while the gateway is in modem/fax pass-through mode.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300. |
| 12.4(2)T | Usage guidelines were added for the **nse** keyword. |
| 12.4(4)T | The **gw-controlled** keyword was added. |
| 12.4(6)T | This feature was implemented on the Cisco 1700 series and Cisco 2800 series. |

## Usage Guidelines

The **mgcp modem relay voip mode**command enables non secure modem relay mode for MGCP VoIP calls. By default, NSE modem relay mode is disabled. This command configures upspeeding, which is needed because modem pass-through is an intermediate step while the gateway switches from handling voice calls to handling modem relay calls.

The **mgcp modem relay voip mode nse** command is not supported on the TI C2510 digital signal processor (DSP), formerly known as the TI C5510 DSP; only the TI C549 DSP supports negotiation of NSE parameters. If Cisco CallManager is used as the call agent, the **mgcp modem relay voip mode nse** command is not supported.

Redundancy causes the gateway to generate duplicate (redundant) data packets for fax/modem pass-through calls as per RFC 2198. For these calls to be more reliable, redundant packets transmission is needed to make up for excessive loss of packets in VoIP networks. Even if one of the gateways is configured with redundancy, calls go through. Gateways can handle asymmetric (one-way) redundancy.

To enable secure voice and data calls between Secure Telephone Equipment (STE) and IP-STE endpoints using the state signaling events (SSE) protocol, use the **mgcp modem relay voip mode sse** command. Before configuring SSE parameters, you must use the **mgcp package-capability mdste** command to enable modem relay capabilities and SSE protocol support.

The **gw-controlled** keyword specifies that modem transport parameters are configured directly on the gateway instead of being negotiated by the call agent.

## Examples

The following example enables MGCP modem relay and specifies the following: NSE mode for upspeeding, G.711 mu-law codec, packet redundancy, and gateway-controlled for modem traffic during modem pass-through:

```
Router(config)# mgcp modem relay voip mode nse codec g711ulaw redundancy gw-controlled
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp modem relay voip gateway-xid** | Optimizes the modem relay transport protocol and the estimated one-way delay across the IP network. |
| **mgcp modem relay voip mode sse** | Enables SSE-based modem relay. |
| **mgcp package-capability mdste** | Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE. |
| **mgcp tse payload** | Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP. |

# mgcp modem relay voip mode sse

To enable State Signaling Event (SSE) based modem relay mode and to configure SSE parameters on the MGCP gateway, use the **mgcp modem relay voip mode sse** command in global configuration mode. To disable this function, use the **no** form of this command.

**mgcp modem relay voip mode sse** [**redundancy** [{**interval** *number* | **packet** *number*}]] [**retries** *value*] [**t1** *time*]
**no mgcp modem relay voip mode sse**

## Syntax Description

| | |
|---|---|
| **redundancy** | (Optional) Packet redundancy for modem traffic during modem pass-through. By default redundancy is disabled. |
| **interval** *milliseconds* | (Optional) Specifies the timer in milliseconds (ms) for redundant transmission of SSEs. Range is 5 - 50 ms. Default is 20 ms. |
| **packet** *number* | (Optional) Specifies the SSE packet retransmission count before disconnecting. Range is 1- 5 packets. Default is 3 packets. |
| **retries** *value* | (Optional) Specifies the number of SSE packet retries, repeated every **t1** interval, before disconnecting. Range is 0 - 5 retries. Default is 5 retries. |
| **t1** *milliseconds* | (Optional) Specifies the repeat interval, in milliseconds, for initial audio SSEs used for resetting the SSE protocol state machine (clearing the call) following error recovery. Range is 500 - 3000 ms. Default is 1000 ms. |

## Command Default

SSE mode is enabled by default, using default parameter values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(2)T | This command was introduced |

## Usage Guidelines

Use the **mgcp modem relay voip mode sse**command to configure state signaling events (SSE) parameters for secure MGCP voice and data calls between Secure Telephone Equipment (STE) and IP STE endpoints using the SSE protocol, a subset of the V.150.1 standard for modem relay. SSEs, which are Real-Time Transport Protocol (RTP) encoded event messages, are used to coordinate transitions between the different media states, secure and nonsecure. Before configuring SSE parameters, you must use the **mgcp package-capability mdste**command to enable modem relay capabilities and SSE protocol support.

## Examples

The following examples configure SSE parameters for redundancy interval redindancy packet count, number of retries and the **t1**timer interval:

```
Router(config)# mgcp modem relay voip mode sse redundancy interval 20
Router(config)# mgcp modem relay voip mode sse redundancy packet 4
Router(config)# mgcp modem relay voip mode sse retries 5
Router(config)# mgcp modem relay voip mode sse t1 1000
```

## Related Commands

| Command | Description |
|---|---|
| **mgcp package-capability mdste** | Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP Secure Telephone Equipment (IP-STE) and STE. |

# mgcp modem relay voip sprt retries

To set the maximum number of times that the Simple Packet Relay Transport (SPRT) protocol tries to send a packet before disconnecting, use the mgcp modem relay voip sprt retries command in global configuration mode. To disable this function, use the **no** form of this command.

**mgcp modem relay voip sprt retries** *value*
**no mgcp modem relay voip sprt retries**

## Syntax Description

| | |
|---|---|
| *value* | Maximum number of times that the SPRT protocol tries to send a packet before disconnecting. Range is from 6 to 30. The default is 12. |

## Command Default

12 times

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300. |

## Examples

The following example sets 15 as the maximum number of times that the SPRT protocol tries to send a packet before disconnecting:

```
mgcp modem relay voip sprt retries 15
```

## Related Commands

| Command | Description |
|---|---|
| mgcp modem relay voip gateway-xid | Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network. |
| mgcp modem relay voip mode | Enables modem relay mode support in a gateway for MGCP VoIP calls. |
| mgcp tse payload | Enables TSEs for communications between gateways, which are required for modem relay over VoIP using MGCP. |
| modem relay gateway-xid | Enables in-band negotiation of compression parameters between two VoIP gateways that use MBCP. |

# mgcp modem relay voip sprt v14

To configure V.14 modem relay parameters for packets sent by the Simple Packet Relay Transport (SPRT) protocol, use the **mgcp modem relay voip sprt v14** command in global configuration mode. To disable this function, use the **no** form of this command.

**mgcp modem relay voip sprt v14** [{**receive playback hold-time** *milliseconds* | **transmit hold-time** *milliseconds* | **transmit maximum hold-count** *characters*}]
**no mgcp modem relay voip sprt v14**

## Syntax Description

| | |
|---|---|
| **receive playback hold-time** *milliseconds* | Configures the time in milliseconds (ms) to hold incoming data in the V.14 receive queue. Range is 20 to 250 ms. Default is 50 ms. |
| **transmit hold-time** *milliseconds* | Configures the time to wait, in ms, after the first character is ready before sending the SPRT packet. Range is 10 to 30 ms. Default is 20 ms. |
| **transmit maximum hold-count** *characters* | Configures the number of V.14 characters to be received on the ISDN public switched telephone network (PSTN) interface that will trigger sending the SPRT packet. Range is 8 to 128. Default is 16. |

## Command Default

V.14 modem relay parameters are enabled by default, using default parameter values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(2)T | This command was introduced. |

## Usage Guidelines

The maximum size of receive buffers is set at 500 characters, a nonprovisionable limit. Use the **mgcp modem relay voip sprt v14 receive playback hold-time** *milliseconds*command to configure the minimum holding time before characters can be removed from the receive queue. Characters received on the PSTN or ISDN interface may be collected for a configurable collection period before being sent out on SPRT channel 3, potentially resulting in variable size SPRT packets. To configure V.14 transmit parameters for SPRT packets, use the **mgcp modem relay voip sprt v14 transmit hold-time** *milliseconds and*the **mgcp modem relay voip sprt v14 transmit maximum hold-count** *characters*commands.

Parameter changes do not take effect during existing calls; they affect new calls only.

SPRT transport channel 1 is not supported.

## Examples

The following example sets 200 ms as the receive playback hold time, 25 ms as the transmit hold time, and 10 characters as the transmit hold count parameters:

```
Router(config)# mgcp modem relay voip sprt v14 receive playback hold-time 200
Router(config)# mgcp modem relay voip sprt v14 transmit hold-time 25
Router(config)# mgcp modem relay voip sprt v14 transmit maximum hold-count 10
```

### Related Commands

| Command | Description |
|---|---|
| **debug voip ccapi inout** | Traces the execution path through the call control API. |
| **debug vtsp all** | Displays all VTSP debugging except statistics, tone, and event. |
| **mgcp package-capability mdste-package** | Enables MGCP gateway support for processing events and signals for modem connections over a secure communication path between IP-STE and STE. |
| **mgcp modem relay voip mode sse** | Enables MGCP gateway SSE based modem relay mode support for VoIP calls. |

# mgcp package-capability

To specify the MGCP package capability type for a media gateway, use the **mgcp package-capability**command in global configuration mode. To remove a specific MGCP package capability from the list of capabilities, use the **no** form of this command.

**mgcp package-capability** *package*
**no mgcp package-capability** *package*

## Syntax Description

| | |
|---|---|
| *package* | One of the following package capabilities (available choices vary according to platform and release version; check the CLI help for a list):<br>• **as -package**--Announcement server package.<br>• **atm -package**--ATM package. MGCP for VoATM using ATM adaptation layer 2 (AAL2) permanent virtual circuit (PVC) and a subset of ATM extensions specified by Cisco is supported. Switched virtual circuit (SVC)-based VoAAL2 is not supported.<br>• **dt -package**--Dual Tone(DT) package. Events and signals for immediate-start and basic dual tone multifrequency (DTMF) and dial-pulse trunks.<br>• **dtmf -package**--DTMF package. Events and signals for DTMF relay.<br>• **fxr -package**--Fax Transmission (FXR) package for fax transmissions.<br>• **fm -package**--Media Format (FM) Parameter Package. This package provides support for the media format parameter Local Connection Option (LCO) and is used for easy DTMF over MGCP-to-SIP configuration.<br>• **gm -package**--Generic media package. Events and signals for several types of endpoints, such as trunking gateways, access gateways, or residential gateways.<br>• **hs -package**--Handset package. An extension of the line package, to be used when the gateway can emulate a handset.<br>• **it -package**--PacketCable Trunking Gateway Control Protocol (TGCP) ISDN User Part (ISUP) trunk package.<br>• **lcs -package**--MGCP Line Control Signaling (LCS) package.<br>• **line -package**--Line package. Events and signals for residential lines. This is the default for residential gateways.<br>• **md -package**--MD package. Provides support for Feature Group D (FGD) Exchange Access North American (EANA) protocol signaling.<br>• **mdste -package--**Modem relay Secure Telephone Equipment (STE) package. Events and signals for modem connections enabling a secure communication path between IP-STE and STE.<br>• **mf -package**--Multifrequency (MF) tone package. Events and signals for MF relay.<br>• **mo -package**--Multifrequency Operations (MO) package. Events and signals for Operator Service Signaling protocol for FGD. |

| | |
|---|---|
| | • **ms -package**--MS package. Events and signals for MF single-stage dialing trunks, including wink-start and immediate-start PBX Direct Inward Dialing (DID) and Direct Outward Dialing (DOD), basic R1, and FGD Terminating Protocol.<br>• **nas -package**--Network Access Server (NAS) Package. Accepts NAS requests from the call agent.<br>**Note** For Cisco IOS Release 12.4(4)T and later releases, the **nas-package** is not enabled by default.<br>• **script -package**--Script package. Events and signals for script loading.<br>• **srtp -package**--Secure RTP (SRTP) package. Enables the MGCP gateway to process SRTP packages. The default is disabled.<br>• **tone-package --Tone package. Disabled by default. Enables the MGCP gateway to play secure call tone during midcall.**<br>• **trunk -package**--Trunk package. Events and signals for trunk lines. This is the default for trunking gateways. |

### Command Default

The **line-package** is configured by default for residential gateways and the **trunk package** is configured by default for trunk gateways.

### Command Modes

Global configuration (config)

### Command History

| Release | Modification |
|---|---|
| 12.0(7)XR2 | This command was introduced on the Cisco AS5300. |
| 12.1(1)T | This command was integrated into Cisco IOS Release 12.1(1)T. |
| 12.1(3)T | This command was implemented on the following platforms: Cisco uBR924, Cisco 2600 series, and Cisco 3660. The **line-package**, **rtp-package**, and **script-package** keywords were added and a distinction was made between residential and trunking gateways. |
| 12.1(5)XM | This command was implemented on the Cisco 3600 series and Cisco MC3810. The **atm-package**, **dt-package, hs-package**, **mo-package, and ms-package** keywords were added. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series. |
| 12.2(2)XB | This command was modified. The **nat-package and res-package** keywords were added. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(11)T | This command was implemented on the following platforms: Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850. |
| 12.3(1) | This command was modified. The **fxr-package** keyword was added. |
| 12.3(8)T | This command was modified. The **lcs-package** keyword was added. |

| Release | Modification |
|---|---|
| 12.3(8)XY | This command was modified. The **pre-package** keyword was added. |
| 12.3(11)T | This command was modified. The **srtp-package** keyword was added. |
| 12.4(2)T | This command was modified. The **mdste-package** keyword was added. |
| 12.4(4)T | This command was modified. The **md-package** keyword was added. The **nas-package** keyword was not enabled by default. |
| 15.1(4)M | This command was modified. The **tone-package** keyword was added. |

## Usage Guidelines

Events specified in the MGCP messages from the call agent must belong to one of the supported packages. Otherwise, connection requests are refused by the gateway.

By default, certain packages are configured as supported on each platform type. Using the **mgcp-package capability** command, you can configure additional package capability only for packages that are supported by your call agent. You can also disable support for a package with the **no** form of this command. Enter each package you want to add as a separate command.

**Note** Beginning in Cisco IOS Release12.4(4)T the **nas-package** keyword is not enabled by default.

The **md-package** keyword is enabled automatically when a T1 interface is configured to use FGD EANA signaling with the **ds0-group** command.

Use the **show mgcp** command to display the packages that are supported on the gateway.

Use this command before specifying a default package with the **mgcp default-package** command. Specify at least one default package.

Packages that are available to be configured with this command vary by platform and type of gateway. Use the CLI help to ascertain the packages available on your gateway. This example shows the CLI help output for a Cisco 3660:

```
Router# mgcp package-capability ?
as-package     Select the Announcement Server Package
atm-package    Select the ATM Package
dtmf-package   Select the DTMF Package
fm-package      Select the FM Package
gm-package     Select the Generic Media Package
hs-package     Select the Handset Package
line-package   Select the Line Package
mf-package     Select the MF Package
res-package    Select the RES Package
rtp-package    Select the RTP Package
trunk-package  Select the Trunk Package
tone-package     Select the Tone Package
```

**Note** The Channel Associated Signaling (CAS) packages configured using the **dt-package**, **md-package**, **mo-package**, and **ms-package** keywords are available only as default packages using the **mgcp default-package** command. They do not appear as keywords in the **mgcp package-capability** command because all the other packages are configured on a per-gateway basis, whereas the CAS packages are defined on a per-trunk basis. The per-trunk specification is made when the trunk is configured using the **ds0-group** command.

When the **lcs-package** keyword is used on the Cisco Integrated Access Device (IAD), the named telephony events (NTEs) associated with the line control signaling (LCS) package are enabled automatically. NTEs are used by a media gateway to transport telephony tones and trunk events across a packet network. See RFC 2833.

**Note** Using NTE in the LCS package requires a successful MGCP/Session Definition Protocol (SDP) negotiation during call setup. The call agent must use the Line Connection Option’s FMTP parameter keyword, **telephone-event**, to indicate which LCS NTEs will be used. If the IAD has been configured to use the LCS package, the IAD will answer with an SDP containing the requested LCS NTE events.

## Examples

The following example enables the modem relay STE package, trunk package, DTMF package, script package, and tone package on the gateway, and then names the trunk package as the default package for the gateway:

```
Router(config)# mgcp package-capability mdste-package
Router(config)# mgcp package-capability trunk-package
Router(config)# mgcp package-capability dtmf-package
Router(config)# mgcp package-capability script-package
Router(config)# mgcp package-capability tone-package
Router(config)# mgcp default-package trunk-package
```

## Related Commands

| Command | Description |
|---|---|
| **ds0-group** | Specifies the DS0 time slots that make up a logical voice port |
| **mgcp** | Starts the MGCP daemon. |
| **mgcp default-package** | Configures the default package capability type for the media gateway. |
| **show mgcp** | Displays the supported MGCP packages. |