mode (ATM/T1/E1 controller) through mwi-server

mode (ATM T1 E1 controller)

To set the DSL controller into ATM mode and create an ATM interface or to set the T1 or E1 controller into T1 or E1 mode and create a logical T1/E1 controller, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no** form of this command.

Cisco 1800, Cisco 2800, Cisco 3700, Cisco 3800 Series
mode atm
no mode atm

Cisco 1700 Series, Cisco 2600XM
mode {**atm** | **t1** | **e1**}
no mode {**atm** | **t1** | **e1**}

Cisco IAD2430
mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDBC) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only; it is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco IAD2430 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis: • Cisco 2600 series--0. • Cisco 3660--0 or 1.
cas	(Cisco 2600 series WIC slots only) Channel-associated signaling (CAS) mode. The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (that is, it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1. On the Cisco IAD2430 series IAD, CAS mode is not supported.

t1	Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

The controller mode is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to the merged SGCP/MGCP software.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for the Cisco IAD2420.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The keyword **aim** and the argument *aim-slot* were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	This command was integrated into Cisco IOS Release 12.3(4)XD on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

When a DSL controller is configured in ATM mode, the mode must be configured identically on both the CO and CPE sides. Both sides must be set to ATM mode.

Note If using the **no mode atm** command to leave ATM mode, the router must be rebooted immediately to clear the mode.

When configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CPE and CO sides.

Examples

ATM Mode Example

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode atm
```

T1 Mode Example

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Configures a list of time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect.

mode (T1 E1 controller)

To set the T1 or E1 controller into asynchronous transfer mode (ATM) and create an ATM interface, to set the T1 or E1 controller into T1 or E1 mode and create a logical T1 or E1 controller, or to set the T1 or E1 controller into channel-associated signaling (CAS) mode, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no**form of this command.

mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDB3) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. On the Cisco MC3810, ATM mode is supported only on controller 0 (T1 or E1 0). **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only and is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco MC3810 and the Cisco IAD2420 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis. For the Cisco 2600 series, the AIM slot number is 0; for the Cisco 3660, the AIM slot number is 0 or 1.
cas	(CAS mode on Cisco 2600 series WIC slots only) The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1.
t1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

No controller mode is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
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	Support was extended to the Cisco 2600 series and Cisco 3660. The **aim**keyword and the *aim-slot* argument were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	Support was extended on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(7)T	The support that was added in Cisco IOS Release 12.3(4)XD was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

This command has the following platform-specific usage guidelines:

- Cisco 2600 series, Cisco 3660 routers, or Cisco 3700 series that use an AIM for ATM processing must use the **mode atm aim***aim-slot* command.
- Cisco 2600 series routers that use an AIM for DSP processing and specify DS0 groups must use the **mode cas** command if they are using WIC slots for voice. This command does not apply if network modules are being used.
- Cisco 3660 routers or Cisco 3700 series that use an AIM only for DSP resources should not use this command.
- On Cisco 2600 series routers that use WIC slots for voice, the **mode atm** command without the **aim** keyword specifies software ATM segmentation and reassembly. When the **aim** keyword is used with the **mode atm** command, the AIM performs ATM segmentation and reassembly.
- Cisco MC3810 routers cannot use the **aim** keyword.
- Cisco MC3810 routers with digital voice modules (DVMs) use some DS0s exclusively for different signaling modes. The DS0 channels have the following limitations when mixing different applications (such as voice and data) on the same network trunk:
  - On E1 controllers, DS0 16 is used exclusively for either CAS or common channel signaling (CCS), depending on which mode is configured.
  - On T1 controllers, DS0 24 is used exclusively for CCS.

- Cisco MC3810--When no mode is selected, channel groups and clear channels (data mode) can be created using the **channel group** and **tdm-group** commands, respectively.
- Cisco MC3810 is not supported in the AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series feature.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in ATM mode, the mode must be set to the same mode on both the CO and CPE sides. Both sides must be set to ATM mode.
    - If the **no mode atm** command is used to leave ATM mode, the router must be rebooted immediately to clear the mode.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CO and CPE sides.

Examples

The following example configures ATM mode on controller T1 0. This step is required for Voice over ATM.

```
Router(config)# controller
 T1 0
Router(config-controller)# mode atm
```

The following example configures ATM mode on controller T1 1/ 0 on a Cisco 2600 series router using an AIM in slot 0 for ATM segmentation and reassembly:

```
Router(config)# controller
 t1 1/0
Router(config-controller)# mode atm aim 0
```

The following example configures CAS mode on controller T1 1 on a Cisco 2600 series router:

```
Router(config)# controller
 T1 1
Router(config-controller)# mode cas
```

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl 3/0
Router(config-controller)# mode atm
```

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Defines the time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

mode border-element

To enable the set of commands used in the border-element configuration, use the **mode border-element** command in voice service voip configuration mode. To disable the set of commands used in border-element configuration, use the **no** form of this command.

mode border-element license [**capacity** *sessions* | **periodicity** {**mins** *value* | **hours** *value* | **days** *value*}]
no mode border-element

Syntax Description

license capacity	(Optional) Configures the license capacity for the Cisco Unified Border Element (UBE).
sessions	(Optional) Number of licenses enabled for the border-element configuration. The range is from 0 through 999999.
periodicity	(Optional) Configures periodicity interval for license entitlement requests for Cisco Unified Border Element (UBE). Default is 7 days.
mins	(Optional) Number of minutes for which the license periodicity configuration is applicable. The range is from 1 through 59.
hours	(Optional) Number of hours for which the license periodicity configuration is applicable. The range is from 1 through 23.
days	(Optional) Number of days for which the license periodicity configuration is applicable. The range is from 1 through 30.

Command Modes

voice service voip configuration (conf-voi-serv)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1r	• Introduced support for YANG models. • The **capacity** keyword and *sessions* argument were deprecated. • The **periodocity** keyword and corresponding arguments were introduced.
15.2(1)T	The command was modified. The **license capacity** keyword and the *sessions* argument were added.
15.0(1)M	This command was introduced.

Usage Guidelines

Effective from Cisco IOS XE Amsterdam 17.2.1r, the **capacity** keyword and *sessions* argument are deprecated. However, the keyword and argument are available in the Command Line Interface (CLI). If you try to configure license capacity using CLI, the following error message is displayed:

```
Error: CUBE SIP trunk licensing is now based on dynamic session counting. Static
 license capacity configuration has been deprecated.
```

If you have configured license capacity in your current release, then while upgrading to Cisco IOS XE Amsterdam 17.2.1r or later releases, license capacity count is ignored and only **mode border-element** command is configured.

For releases before Cisco IOS XE Amsterdam 17.2.1r, the Cisco UBE status display is enabled only if the license capacity has been configured with **mode border-element** command. Without the license capacity configuration, the **show cube status** command does not display any output. This dependency is removed from Cisco IOS XE Amsterdam 17.2.1r and later releases.

You can configure the license entitlement interval in minutes, hours, or days. The default value of the license entitlement interval is 7 days.

We recommend you to configure interval in days. Configuring interval in minutes or hours increases the frequency of entitlement requests and thereby increases the processing load on Cisco Smart Software Manager (CSSM). License periodicity configuration of minutes or hours is recommended to be used only with Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) mode.

The following warning is displayed when you try to configure the interval in minutes or hours:

```
Warning: Periodicity interval of mins/hours would result in frequent licensing
requests and should be used with satellite mode of license manager, continue?
[confirm]
```

For **mode border-element** or **no mode border-element** command to take effect, you must save the running-config file and reload the router after you enter the command. The CLI displays the following notification after the command is entered:

```
You need to save and reload the router for this configuration change to be
effective.
```

If you do not reload the router, the **mode border-element** or **no mode border-element** command does not take effect, and the availability of the commands used in the border-element configuration is not affected.

Note The **show running-config** command displays the **mode border-element** or **no mode border-element** command in its output, even if a reload has not been done and either command is not in effect.

Examples

The following example shows how to configure the license capacity in releases before Cisco IOS XE Amsterdam 17.2.1r with the **mode border-element** command for enabling the Cisco UBE status display:

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element license capacity 100
```

The following example shows how to configure license periodicity for releases Cisco IOS XE Amsterdam 17.2.1r and later.

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element license periodicity days 15
```

The following alert message is displayed if you configure periodicity in minutes or hours:

```
Router(config)# voice service voip
Router(conf-voi-serv)# mode border-element license periodicity mins 30
```

```
Warning: Periodicity interval of mins/hours would result in frequent licensing requests and
 should be used with satellite mode of license manager, continue? [confirm]
```

Related Commands

Command	Description
codec (voice port)	Specifies voice compression.
codec complexity	Specifies the call density and codec complexity based on the codec used.
media	Enables media packets to pass directly between the endpoints without the intervention of the IP-to-IP gateway and enables the incoming and outgoing IP-IP call gain/loss feature for audio call scoring on either the incoming dial peer or the outgoing dial peer.
show cube status	Displays the Cisco UBE status, the software version, the license capacity, the image version, and the platform name of the router.
show dial peer voice	Displays the codec setting for dial peers.
show running-config	Displays the contents of the currently running configuration file on the router.

mode ccs

To configure the T1/E1 controller to support common channel signaling (CCS) cross-connect or CCS frame forwarding, use the mode ccs command in global configuration mode. To disable support for CCS cross-connect or CCS frame forwarding on the controller, use the no form of this command.

mode ccs {**cross-connect** | **frame-forwarding**}
no mode ccs {**cross-connect** | **frame-forwarding**}

Syntax Description

cross -connect	Enables CCS cross-connect on the controller.
frame -forwarding	Enables CCS frame forwarding on the controller.

Command Default

No CCS mode is configured

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced on the Cisco MC3810.
12.1(2)XH	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

On Cisco 2600 series routers and Cisco 2600XM series routers with the AIM-ATM, AIM-VOICE-30 or AIM-ATM-VOICE-30 module installed, the channel group configuration must be removed before the **no mode ccs frame-forwarding** command is entered. This restriction does not apply to the Cisco 3600 series routers or the Cisco 3700 series routers.

Examples

To enable CCS cross-connect on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs cross-connect
```

To enable CCS frame forwarding on controller T1 1, enter the following commands:

```
controller T1 1
 mode ccs frame-forwarding
```

Related Commands

Command	Description
ccs connect	Configures a CCS connection on an interface configured to support CCS frame forwarding.

modem passthrough (dial peer)

To enable modem pass-through over VoIP for a specific dial peer, use the **modem passthrough** command in dial peer configuration mode. To disable modem pass-through for a specific dial peer, use the **no**form of this command.

modem passthrough {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**]}
no modem passthrough

Syntax Description

system	Defaults to the global configuration.
nse	Specifies that named signaling events (NSEs) are used to communicate codec switchover between gateways.
payload -type *number*	(Optional) NSE payload type. Range varies by platform, but is from 96 to 119 on most platforms. For details, refer to command-line interface (CLI) help. Default is 100.
codec	Codec selections for upspeeding.
g711ulaw	Codec G.711 u-law 64000 bits per second for T1.
g711alaw	Codec G.711 a-law 64000 bits per second for E1.
redundancy	(Optional) Enables a single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss.

Command Default

payload -type *number*:100

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use this command to enable fax pass-through over VoIP individually for a single dial peer. Use the same values for all options on originating and terminating gateways.

Fax pass-through occurs when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and configuration and loading the pass-through parameters for the duration of the fax session. The switchover of codec is known as upspeeding, and it changes the bandwidth needed for the call to the equivalent of G.711.

The **system** keyword overrides the configuration for the dial peer and directs that the values from the global configuration are to be used for this dial peer. When the **system** keyword is used, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**.

The **modem passthrough (voice service)** command can be used to set pass-through options globally on all dial peers at one time. If the **modem passthrough (voice service)**command is used to set pass-through options for all dial peers and the **modem passthrough (dial peer)**command is used on a specific dial peer, the dial peer configuration takes precedence over the global configuration for that dial peer.

Examples

The following example configures fax pass-through over VoIP for a specific dial peer:

```
dial-peer voice 25 voip
 modem passthrough nse codec g711ulaw redundancy
```

Related Commands

Command	Description
dial -peer voice	Enters dial-peer configuration mode.
modem passthrough (voice service)	Enables fax or modem pass-through over VoIP globally for all dial peers.

modem passthrough (voice-service)

To enable fax or modem pass-through over VoIP globally for all dial peers, use the **modem passthrough**command in voice-service configuration mode. To disable fax or modem pass-through, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, Cisco 3700 Series, Cisco AS5300
modem passthrough nse [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*]]
no modem passthrough

Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco AS5350XM, Cisco AS5400XM, Cisco VGD 1T3
modem passthrough {**nse** | **protocol**} [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*] [**sample-duration** [{**10** | **20**}]]]
no modem passthrough

Syntax Description

nse	Specifies the named signaling events (NSEs) used to communicate codec switchover between gateways.
payload -type *number*	(Optional) Specifies NSE payload type. The range varies for this keyword, but is from 96 to 119 on most platforms. For details, see the command-line interface (CLI) help. Default value is 100.
codec	Configures codec selections for upspeed.
g711ulaw	Configures Codec G.711 mu-law, 64000 bits per second for T1.
g711alaw	Configures Codec G.711 A-law, 64000 bits per second for E1.
redundancy	(Optional) Specifies the single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss.
maximum-sessions *sessions*	(Optional) Specifies the maximum number of simultaneous pass-through sessions. Ranges and defaults vary by platform. For details, see the CLI help.
protocol	Configures the Session Initiation Protocol (SIP)/H.323 protocol used for signal modem pass-through.
sample -duration	(Optional) Specifies the Time, in milliseconds, of the largest Real-time Transport Protocol (RTP) packet when packet redundancy is active. Keywords vary by platform, but are either **10** or **20**. Default is **10**.

Command Default

The command is disabled, so no fax or modem pass-through occurs.

Command Modes

Voice-service configuration (conf-voi-serv)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.

Release	Modification
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **sample-duration** keyword was added.
12.4(24)T	This command was implemented on the following platforms: Cisco AS5350XM, Cisco AS5400XM, and Cisco VGD 1T3. The **protocol** keyword was added.

Usage Guidelines

Use this command to enable fax or modem pass-through over VoIP globally for all dial peers. Use the same values for all options on originating and terminating gateways.

In Cisco IOS Release 12.4(24)T, the **modem passthrough protocol** command is supported only on SIP signaling.

Note The **modem passthrough protocol** and **fax protocol** commands cannot be configured at the same time. If you enter either one of these commands when the other is already configured, the command-line interface returns an error message. The error message serves as a confirmation notice because the **modem passthrough protocol** command is internally treated the same as the **fax protocol passthrough** command by the Cisco IOS software. For example, no other mode of fax protocol (for example, fax protocol T.38) can operate if the **modem passthrough protocol** command is configured.

Note Cisco does not support the following protocols for the **modem pass through protocol codec g711alaw** command for inter-operating third-party vendors using voice modems:

- ITU-T V.152
- A set standard for modem passthrough
- Protocol based modem passthrough up-speeds based on the sdp attribute "a=silenceSupp:off -"

Note Even though the **modem passthrough protocol** and **fax protocol passthrough** commands are treated the same internally, be aware that if you change the configuration from the **modem passthrough protocol** command to the **modem passthrough ns e** command, the configured **fax protocol passthrough** command is not automatically reset to the default. If default settings are required for the **fax protocol** command, you have to specifically configure the **fax protocol** command.

Fax pass-through occurs when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and configuration and loading the pass-through parameters for the duration of the fax session. The switchover of codec is known as upspeeding, and it changes the bandwidth needed for the call to the equivalent of G.711.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem pass-through with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You can associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that the incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Device(config)# dial-peer voice
 tag
 voip
Device(config-dial-peer)# incoming called-number
```

The **modem passthrough (dial peer)** command can be used to set pass-through options on individual dial peers. If the **modem passthrough (voice-service)**command is used to set pass-through options for all dial peers and the **modem passthrough (dial peer)** command is used on a specific dial peer, the dial-peer configuration takes precedence over the global configuration for that specific dial peer.

Examples

The following example shows how to configure modem pass-through for NSE payload type 101 using the G.711 mu-law codec:

```
voice service voip
 modem passthrough nse payload-type 101 codec g711ulaw redundancy maximum-sessions 1
```

Related Commands

Command	Description
fax protocol (voice-service)	Specifies the global default fax protocol to be used for all VoIP dial peers.
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem passthrough (dial peer)	Enables fax or modem pass-through over VoIP for a specific dial peer.
voice service voip	Enters voice-service configuration mode and specifies the voice encapsulation type.

modem relay (dial peer)

To configure modem relay over VoIP for a specific dial peer, use the **modem relay** command in dial peer configuration mode. To disable modem relay over VoIP for a specific dial peer, use the **no**form of this command.

modem relay {**nse** [**payload-type** *number*] **codec** {**g711alaw** | **g711ulaw**} [**redundancy**] | **system**} **gw-controlled**
no modem relay {**nse** | **system**}

Syntax Description

nse	Named signaling event (NSE).
payload -type *number*	(Optional) NSE payload type. Range is from 98 to 119. Default is 100.
codec	Sets the upspeed voice compression selection for speech or audio signals. The upspeed method is used to dynamically change the codec type and speed to meet network conditions. A faster codec speed may be required to support both voice and data calls and a slower speed for only voice traffic.
g711ulaw	Codec G.711 mu-law 64,000 bits per second (bps) for T1.
g711alaw	Codec G.711 a-law 64,000 bps for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic. Sends redundant packets for modem traffic during pass-through.
system	This default setting uses the global configuration parameters set with the **modem relay** command in voice-service configuration mode for VoIP.
gw -controlled	Specfies the gateway-configured method for establishing modem relay parameters.

Command Default

Cisco modem relay is disabled. Payload type: 100

Command Modes

Dial peer 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(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

This command applies to VoIP dial peers. Use this command to configure modem relay over VoIP for a specific dial peer.

Use the same codec typefor the originating and terminating gateway, as follows:

- T1 requires the G.711 mu-law codec.

- E1 requires the G.711 a-law codec.

The **system** keyword overrides the configuration for the dial peer, and the values from the **modem-relay** command in voice-service configuration mode for VoIP are used.

When using the **voice service voip** and **modem relay nse** commands on a terminating gateway to globally set up modem relay with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example shows Cisco modem relay configured for a specific dial peer using the G.711 mu-law codec and enabling redundancy and gateway-controlled negotiation parameters:

```
Router(config-dial-peer)# modem relay nse codec g711ulaw redundancy gw-controlled
```

Related Commands

Command	Description
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem passsthrough (voice service)	Enables fax or modem pass-through over VoIP globally for all dial peers.
modem relay (voice-service)	Enables fax or modem pass-through over VoIP globally for all dial peers.
voice service voip	Enters voice-service configuration mode and specifies the voice encapsulation type.

modem relay (voice-service)

To configure modem relay over VoIP for all connections, use the **modem relay**command in voice-service configuration mode. To disable modem relay over VoIP for all connections, use the **no** form of this command.

modem relay nse [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *value*]] **gw-controlled**
no modem relay nse

Syntax Description

nse	Named signaling event (NSE).
payload -type *number*	(Optional) NSE payload type. Range is from 98 to 119. Default is 100.
codec	Sets the upspeed voice compression selection for speech or audio signals. The upspeed method is used to dynamically change the codec type and speed to meet network conditions. A faster codec speed may be required to support both voice and data calls and a slower speed for only voice traffic.
g711ulaw	Codec G.711m u-law 64,000 bits per second (bps) for T1.
g711alaw	Codec G.711 a-law 64,000 bps for E1.
redundancy	(Optional) Packet redundancy (RFC 2198) for modem traffic. Sends redundant packets for modem traffic during pass-through.
maximum -sessions *value*	(Optional) Maximum redundant, simultaneous modem-relay pass-through sessions. Range is from 1 to 10000. Default is 16. Recommended value for the Cisco AS5300 is 26.
gw-controlled	Specfies the gateway-configured method for establishing modem relay parameters.

Command Default

Cisco modem relay is disabled. Payload type: 100.

Command Modes

Voice-service 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(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

Use this command to configure modem relay over VoIP. The default behavior for this command is **no modem relay**. Configuration of modem relay for VoIP dial peers via the **modem relay**dial-peer configuration command overrides this voice-service command for the specific VoIP dial peer on which the dial-peer command is configured.

Use the same payload-type number for both the originating and terminating gateways.

Use the same codec typefor the originating and terminating gateway, as follows:

- T1 requires the G.711 mu-law codec.
- E1 requires the G.711 a-law codec.

The **maximum-sessions** keyword is an optional parameter for the **modem relay** command. This parameter determines the maximum number of redundant, simultaneous modem relay sessions. The recommended *value* for the **maximum-sessions** keyword is 16. The value can be set from 1 to 10000. The **maximum-sessions** keyword applies only if the **redundancy** keyword is used.

When using the **voice service voip** and **modem relay nse** commands on a terminating gateway to globally set up modem relay with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls will match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice
 tag
 voip
Router(config-dial-peer)# incoming called-number .
```

Examples

The following example shows Cisco modem relay enabled with NSE payload type 101 using the G.711 mu-law codec, enabling redundancy and gateway-controlled negotiation parameters:

```
Router(conf-voi-serv)# modem relay nse payload-type 101 codec g711ulaw redundancy
maximum-sessions 1 gw-controlled
```

Related Commands

Command	Description
incoming called-number	Defines an incoming called number to match a specific dial peer.
modem relay (dial-peer)	Configures modem relay on a specific VoIP dial peer.

modem relay gateway-xid

To enable in-band negotiation of compression parameters between two VoIP gateways, use the **modem relay gateway-xid** command in dial-peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

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

Syntax Description

compress	(Optional) Direction in which data flow is compressed. For normal dialup, compression should be enabled on both directions. 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. • **backward** --Enables compression only in the backward direction. • **both** --Enables compression in both directions. For normal dialup, this is the preferred setting. This is the default. • **forward** --Enables compression only in the forward direction. • no--Disables compression in both directions. **Note** The compress, dictionary, and string-length arguments can be entered in any order.
dictionary *value*	(Optional) V.42 *bis* parameter that specifies characteristics of the compression algorithm. Range is from 512 to 2048. Default is 1024. **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. **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

Dial-peer configuration
Voice-service 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.

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 remaining parameters specify the negotiation posture of this gateway in the subsequent inband negotiation step (assuming inband negotiation was 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:

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

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 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 latency

To optimize the Modem Relay Transport Protocol and the estimated one-way delay across the IP network, use the **modem relay latency** command in dial-peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay latency *value*
no modem relay 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

Dial-peer configuration
Voice-service 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.

```
Router(config-dial-peer)# modem relay latency 100
```

Related Commands

Command	Description
mgcp modem relay voip latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network using MGCP.
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 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 modem relay sprt retries command in dial-peer or voice-service configuration mode. To disable this function, use the **no** form of this command.

modem relay sprt retries *value*
no modem relay 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

Dial-peer configuration
Voice-service 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.

```
modem relay sprt retries 15
```

Related Commands

Command	Description
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.
modem relay latency	Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network.

modem relay sprt v14

To configure V.14 modem-relay parameters for packets sent by the Simple Packet Relay Transport (SPRT) protocol, use the **modem relay sprt v14**command in voice service configuration mode. To disable this function, use the **no** form of this command.

modem relay sprt v14 [{**receive playback hold-time** *milliseconds* | **transmit hold-time** *milliseconds* | **transmit maximum hold-count** *characters*}]
no modem relay sprt v14

Syntax Description

receive playback hold-time *milliseconds*	(Optional) 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*	(Optional) 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*	(Optional) 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

Voice service configuration

Command History

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

Usage Guidelines

SPRT packets are used to reliably transport modem signals between gateways. Use the **modem relay sprt v14** command under the **voice service voip** command to configure parameters for SPRT packet transport. The maximum size of the receive buffers is set at 500 characters, a nonprovisionable limit. Use the **modem relay sprt v14 receive playback hold-time**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 **modem relay sprt v14 transmit hold-time** *milliseconds and the* **modem relay 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.

Use the **stcapp register capability** *voice-port* **modem-relay** command to specify modem relay as the transport method for a specific device.

Examples

The following example shows the receive playback hold time, transmit hold time, and transmit hold count parameters:

```
Router(conf-voi-serv)
# modem relay sprt v14 receive playback hold-time 200
Router(conf-voi-serv)
# modem relay sprt v14 transmit hold-time 25
Router(conf-voi-serv)
# modem relay 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.
stcapp register capability	Configures the modem transport method for a specified device registered with Cisco CallManager.
voice service voip	Enters voice service configuration mode for VoIP encapsulation.

modem relay sse

To enable V.150.1 modem-relay secure calls and configure state signaling events (SSE) parameters, use the **modem relay sse** command in voice service configuration mode. To disable this function, use the **no** form of this command.

modem relay sse [**redundancy**] [**interval** *milliseconds*] [**packet** *number*] [**retries** *value*] [**t1** *milliseconds*][**v150mer]**
no modem relay sse

Syntax Description

redundancy	(Optional) Specifies 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 to 50 ms. Default is 20 ms.
packet *number*	(Optional) Specifies the SSE packet retransmission count before disconnecting. Range is one to five packets. Default is three packets.
retries *value*	(Optional) Specifies the number of SSE packet retries, repeated every **t1** interval, before disconnecting. Range is zero to five retries. Default is five 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 to 3000 ms. Default is 1000 ms.
v150mer	Configures the V150.1 MER modem relay support for SIP trunks.

Command Default

Modem relay mode of operation, using the SSE protocol, is enabled by default using default parameter values.

Command Modes

Voice service configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.5(3)M	This command was modified. The **v150mer** keyword was added.

Usage Guidelines

Use the **modem relay sse** command under the **voice service voip** command to configure SSE parameters used to negotiate the transition from voice mode to V.150.1 modem-relay mode on the digital signal processor (DSP). Secure voice and data calls through the SCCP Telephony Control Application (STCAPP) gateway connect 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 that use payload 118, are used to coordinate transitions between secure and non-secure media states.

Use the **stcapp register capability** command to specify modem transport method for secure calls.

Use the **modem relay sprt v14 receive playback hold-time** command to configure V.14 receive parameters for Simple Packet Relay Transport (SPRT) protocol packets in V.150.1 modem relay mode.

Use the **modem relay sprt v14 transmit hold-time** and **modem relay sprt v14 transmit maximum hold-count** commands to configure SPRT transmit parameters in V.150.1 modem relay mode.

Use the **mgcp modem relay voip mode sse** command to enable secure V.150.1 modem relay calls on trunk-side or non-STCAPP-enabled gateways. Use the **mgcp modem relay voip mode nse** command to enable non-secure modem-relay mode; by default, NSE modem-relay mode is disabled.

Examples

The following example shows SSE parameters configured to support secure calls between IP-STE and STE endpoints:

```
Router(config-voi-serv)
# modem relay sse redundancy interval 20
Router(config-voi-serv)
# modem relay sse redundancy packet 4
Router(config-voi-serv)
# modem relay sse retries 5
Router(config-voi-serv)
# modem relay sse t1 1000
Router(config-voi-serv)
# modem relay sse v150mer
```

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-STE and STE.
modem relay sprt v14 receive playback hold-time	Configures SPRT parameters.
modem relay sprt v14 transmit hold-time	Configures SPRT transmit parameters.
modem relay sprt v14 transmit maximum hold-count	Configures SPRT transmit parameters.
modem relay sprt v14 transmit maximum hold-count	Configures SPRT transmit parameters.
stcapp register capability	Configures the modem transport method for a specified device registered with Cisco CallManager.
voice service voip	Enters voice service configuration mode for VoIP encapsulation.

monitor call application event-log

To display the event log for an active application instance in real-time, use the **monitor call application event-log**command in privileged EXEC mode.

monitor call application event-log [{**app-tag** *application-name* {**last** | **next**} | **session-id** *session-id* [{**stop**}] | **stop**}]

Syntax Description

app-tag *application-name*	Displays event log for the specified application.
last	Displays event log for the most recent active instance.
next	Displays event log for the next active instance.
session-id *session-id*	Displays event log for specific application instance.
stop	(Optional) Stops the monitoring session.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command enables dynamic event logging so that you can view events as they happen for active application instances. You can view the most recent active instance or the next new instance of a specified application, or the specified active application instance, or it stops the display. To display event logs with this command, you must enable either the **call application event-log** command or the**call application voice event-log** command.

Examples

The following example displays the event log for the next active session of the application named sample_app:

```
Router# monitor call application event-log app-tag generic last

5:1057278146:172:INFO: Prompt playing finished successfully.
5:1057278151:173:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278151:174:INFO: Script received event = "noinput"
5:1057278151:175:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278158:177:INFO: Prompt playing finished successfully.
5:1057278163:178:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278163:179:INFO: Script received event = "noinput"
5:1057278163:180:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278170:182:INFO: Prompt playing finished successfully.
5:1057278175:183:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278175:184:INFO: Script received event = "noinput"
5:1057278175:185:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
5:1057278181:187:INFO: Prompt playing finished successfully.
5:1057278186:188:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057278186:189:INFO: Script received event = "noinput"
5:1057278186:190:INFO: Playing prompt #1: tftp://172.19.139.145/audio/ch_welcome.au
```

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application voice event-log	Enables event logging for a specific voice application.

monitor call leg event-log

To display the event log for an active call leg in real-time, use the **monitor call leg event-log**command in privileged EXEC mode.

monitor call leg event-log {**leg-id** *leg-id* [**stop**] | **next** | **stop**}

Syntax Description

leg-id *leg-id*	Displays the event log for the identified call leg.
next	Displays the event log for the next active call leg.
stop	(Optional) Stops the monitoring session.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command enables dynamic event logging so that you can view events as they happen for active voice call legs. You can view the event log for the next new call leg, or the specified active call leg, or it stops the display. To display event logs with this command, you must enable the **call leg event-log** command.

Examples

The following is sample output from the **monitor call leg event-log next** command showing the event log for the next active call leg after a PSTN incoming call was made to the gateway:

```
Router# monitor call leg event-log next
2B:1058571679:992:INFO: Call setup indication received, called = 4085550198,  calling =
52927, echo canceller = enable, direct inward dialing
2B:1058571679:993:INFO: Dialpeer = 1
2B:1058571679:998:INFO: Digit collection
2B:1058571679:999:INFO: Call connected using codec None
2B:1058571688:1007:INFO: Call disconnected (cause = normal call clearing (16))
2B:1058571688:1008:INFO: Call released
```

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.

monitor event-trace voip ccsip

To configure event tracing for Voice over IP (VoIP) Session Initiation Protocol (SIP) events, use the **monitor event-trace voip ccsip** command in global configuration mode. To disable event tracing, use the **no** form of this command.

monitor event-trace voip ccsip *trace-type*
size *number*
no monitor event-trace voip ccsip *trace-type*

Syntax Description

trace-type	The type of trace.
size *number*	(Optional) The number of events of the specific types that are stored for a specific instance. The range is from 1 to 1000000. The default value depends on the trace-type setting.

Command Default

Event tracing is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **monitor event-trace voip ccsip** command to enable or disable event tracing. The table below shows the valid values for *trace-type* argument.

Trace Type	Description
api	Use this keyword to configure event tracing for the VoIP CCSIP subsystem API events. These events are interactions between the SIP subsystem and other subsystems.
fsm	Use this keyword to configure event tracing for VoIP CCSIP Finite State Machine (FSM) and CNFSM events. These messages provide information on the status of various state transitions.
global	Use this keyword to configure event tracing for VoIP CCSIP global events. Global events are all events that occur outside of a call context.
misc	Use this keyword to configure event tracing for VoIP CCSIP miscellaneous events. These messages provide information about invoked features.

Trace Type	Description
msg	Use this keyword to configure event tracing for VoIP CCSIP message events. These messages provide information about the SIP messages that are sent and received by the Cisco Unified Border Element (Cisco UBE).

Use the **size** keyword to set the number of events of the specific types that are stored for this instance. If the number of events increases beyond this size earlier events are overwritten. If you do not set a value for size, the system uses the default value for the specified trace-type, as follows:

- **api**—50
- **fsm**—100
- **global**—100
- **misc**—50
- **msg**—50

Note The amount of data collected from the trace depends on the trace buffer size configured using the **monitor event-trace voip ccsip** command for each instance of a trace.

Example

The following example shows how to enable event tracing for different event types in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device# configure terminal
Device(config)# monitor event-trace voip ccsip api size 50
Device(config)# monitor event-trace voip ccsip fsm size 100
Device(config)# monitor event-trace voip ccsip global size 100
Device(config)# monitor event-trace voip ccsip misc size 50
Device(config)# monitor event-trace voip ccsip msg size 50
```

monitor event-trace voip ccsip (EXEC)

To monitor and control the event trace function for Voice Over IP (VoIP) Call-Control Session Initiation Protocol (CCSIP), use the **monitor event-trace voip ccsip** command is privileged EXEC mode.

monitor event-trace voip ccsip {**all** | **api** | **fsm** | **global** | **history** | **misc** | **msg**} {**clear** | **disable** | **dump** [**filter** {**call-id** | **called-num** | **calling-num** | **sip-call-id**} *filter-value*] [**pretty**] | **enable**}

Syntax Description

all	Event tracing for API, Finite State Machine (FSM) and Communicating Nested FSM (CNFSM), miscellaneous and message VoIP CCSIP events.
api	Event tracing for VoIP CCSIP API events.
fsm	Event tracing for VoIP CCSIP FSM and CNFSM events.
global	Event tracing for VoIP CCSIP global events.
history	Specifies that event traces are not deleted until the maximum limit is reached. When the maximum limit is reached, the oldest history trace is deleted to capture event-trace for new call.
misc	Event tracing for VoIP CCSIP miscellaneous events.
msg	Event tracing for VoIP CCSIP message events.
clear	Clears all captured VoIP CCSIP event traces.
disable	Turns off VoIP CCSIP event tracing.
dump	Writes the event trace results to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command. The traces are saved in binary format.
filter	(Optional) Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command.
call-id *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified call ID.
called-num *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified called number.
calling-num *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified calling number.

sip-call-id *filter-value*	Filters the traces written to the file configured with the global configuration **monitor event-trace voip ccsip dump-file** command based on the specified SIP call ID.
pretty	(Optional) Dumps the event trace message in ASCII format.
enable	Turns on VoIP CCSIP event tracing, if it has been configured in global configuration mode.

Command Default

Event tracing is disabled, except for history.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **monitor event-trace voip ccsip** command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace voip ccsip** command in global configuration mode.

Note The amount of data collected from the trace depends on the trace buffer size configured using the **monitor event-trace voip ccsip dump-file** command in global configuration mode for each instance of a trace.

Use the **show monitor event-trace voip ccsip** command to display traces. Use the **monitor event-trace voip ccsip dump filter** command to save trace message information for specific events.

By default, trace information is saved in binary format. If you want to save traces in ASCII format, possibly for additional application processing, use the **monitor event-trace voip ccsip dump pretty** command.

To write the event traces that are in the buffer to a file (secondary storage), enter the **monitor event-trace voip ccsip** *trace-type* **dump** command. To configure the file where you want to save trace information, use the **monitor event-trace voip ccsip dump-file** command in global configuration mode. By default, the event traces are saved in a binary format.

Example

The following example shows the command for writing traces for an event in ASCII format:

```
Device# monitor event-trace voip ccsip all dump pretty
```

The following shows how to stop event tracing, clear the current contents of memory, and re-enable the trace function for the VoIP CCSIP component. The **all** keyword indicates that these instructions apply to API, FSM, CNFSM, miscellaneous and message events. This example assumes that the tracing function is configured and enabled on the networking device:

```
Device# monitor event-trace voip ccsip all disable
Device# monitor event-trace voip ccsip all clear
Device# monitor event-trace voip ccsip all enable
```

monitor event-trace voip ccsip api

To configure event tracing for Voice over IP (VoIP) application programming interface (API) events, use the **monitor event-trace voip ccsip api** command in global configuration mode. To disable API event tracing, use the **no** form of the command.

monitor event-trace voip ccsip api [**size** *number*]
no monitor event-trace voip ccsip api [**size** *number*]

Syntax Description

size *number*	(Optional) The number of API events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 50.

Command Default

API event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

This command configures event tracing for the VoIP CCSIP subsystem API events. These events are interactions between the Session Initiation Protocol (SIP) subsystem and other subsystems.

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for API events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip api size 50
```

monitor event-trace voip ccsip dump

To specify the options to automatically dump or store event tracing messages for Voice over IP (VoIP) Session Initiation Protocol (SIP) events, use the **monitor event-trace voip ccsip dump** command in global configuration mode. To stop event tracing messages being written to the dump file, use the **no** form of this command.

monitor event-trace voip ccsip dump {**all** | **marked** | **none**}
no monitor event-trace voip ccsip dump

Syntax Description

all	Specifies that all event trace messages are written to the specified location upon completion of the call or call-leg.
marked	Cisco Unified Border Element (Cisco UBE) has identified specific internal errors, and the traces are dumped only if any of these errors occur.
none	Specifies that event trace messages are not to be automatically written to the specified location.

Command Default

Event trace messages are not automatically dumped.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to specify an automatic policy based on which VoIP CCSIP event tracing messages are written to the dump file.

Note Use the **monitor event-trace voip ccsip dump-file** command to set the dump location. Without a valid dump-file configuration, neither manual dumps nor automatic dumps will function.

Example

The following examples show how to specify that only marked event trace messages are written to the dump file:

```
Device(config)# monitor event-trace voip ccsip
dump-file slot0:ccsip-dump-file
```

```
Device(config)# monitor event-trace voip ccsip dump-file
ftp://username:password@server_ip//path/ccsip-dump-file
Device(config)# monitor event-trace voip ccsip dump-file
tftp://server_ip//path/ccsip-dump-file
```

monitor event-trace voip ccsip dump-file

To specify the file where event trace messages are written from memory on the networking device, use the **monitor event-trace voip ccsip dump-file** command in global configuration mode.

monitor event-trace voip ccsip dump-file *file-name*
no monitor event-trace voip ccsip dump-file

Syntax Description

file-name	The name of the file where event trace messages are written.

Command Default

Dump file is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to specify the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.

To make the filename unique for different calls a unique identifier is added after a file-name for each dump. If there is a filename length restriction on the storage device you must ensure that the length of the filename you specify plus the unique identifier string does not exceed the allowable filename length.

Note Without a valid dump-file configuration, neither manual dumps nor automatic dumps will function.

Example

The following example shows how to set the trace messages file to ccsip-dump-file in slot0 (flash memory) and to remote servers:

```
Device(config)# monitor event-trace voip ccsip dump-file slot0:ccsip-dump-file
Or
Device(config)# monitor event-trace voip ccsip dump-file
ftp://username:password@server_ip//path/ccsip-dump-file
Or
Device(config)# monitor event-trace voip ccsip dump-file
tftp://server_ip//path/ccsip-dump-file.txt
```

monitor event-trace voip ccsip fsm

To configure event tracing for Voice over IP (VoIP) CCSIP Finite State Machine (FSM) and communicating nested FSM (CNFSM) events, use the **monitor event-trace voip ccsip fsm** command in global configuration mode. To disable FSM and CNFSM event tracing, use the **no** form of the command.

monitor event-trace voip ccsip fsm [**size** *number*]
no monitor event-trace voip ccsip fsm [**size** *number*]

Syntax Description

size *number*	(Optional) The number of FSM events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 100.

Command Default

FSM event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Event messages for VoIP CCSIP FSM and CNFSM events provide information on the status of various state transitions.

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for FSM and CNFSM events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip fsm size 100
```

monitor event-trace voip ccsip global

To configure event tracing for Voice over IP (VoIP) global events, use the **monitor event-trace voip ccsip global** command in global configuration mode. To disable global event tracing, use the **no** form of the command.

monitor event-trace voip ccsip global [**size** *number*]
no monitor event-trace voip ccsip global [**size** *number*]

Syntax Description

size *number*	(Optional) The number of global events that are stored. The range is from 1 to 1000000. The default value is 100.

Command Default

Global event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Global events are all events that occur outside of a call context.

Use the **size** keyword to set the number of events that are stored. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for global events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip global size 100
```

monitor event-trace voip ccsip limit

To limit the resources used by the event tracing mechanism, use the **monitor event-trace voip ccsip limit** command in global configuration mode. To remove any resource limits, use the **no** form of this command.

monitor event-trace voip ccsip limit {**connections** *max-connections* | **memory** *size*}
no monitor event-trace voip ccsip limit

Syntax Description

connections *max-connections*	Specifies the maximum number of calls that can be traced. The range is from 1 to 1000. The default is 1000 simultaneous call-legs.
memory *size*	Specifies the maximum memory that can be used by the event tracing mechanism. The range is from 1 to 1000 MB.

Command Default

The maximum number of call-legs that can be traced is 1000.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to control the amount of resources used by the event tracing mechanism. The limits can be applied based on the maximum call-leg allowed or the maximum memory that can be used by the event tracing mechanism. The event tracing mechanism will operate within the set limits. If the limit is reached, the system will first try to reuse memory reclaimed from the history. If this is not possible, then subsequent event traces are not captured.

Note If the **no** form of this command is configured, it can impact the resources available for calls, and can also impact the call density on the device.

Example

The following examples shows how to configure a maximum connections limit of 500 connections:

```
Device(config)# monitor event-trace voip ccsip limit connections 500
```

monitor event-trace voip ccsip misc

To configure event tracing for Voice over IP (VoIP) CCSIP miscellaneous events, use the **monitor event-trace voip ccsip misc** command in global configuration mode. To disable miscellaneous-event tracing, use the **no** form of the command.

monitor event-trace voip ccsip misc [**size** *number*]
no monitor event-trace voip ccsip misc [**size** *number*]

Syntax Description

size *number*	(Optional) The number of miscellaneous events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 50.

Command Default

Miscellaneous event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

Miscellaneous event messages provide information about invoked features.

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for miscellaneous events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip misc size 50
```

monitor event-trace voip ccsip msg

Use this keyword to configure event tracing for VoIP CCSIP message events. These messages provide information about theSession Initiation Protocol (SIP) messages that are sent and received by the Cisco Unified Border Element (Cisco UBE).

To configure event tracing for Voice over IP (VoIP) CCSIP message events, use the **monitor event-trace voip ccsip msg** command in global configuration mode. To disable message-event tracing, use the **no** form of the command.

monitor event-trace voip ccsip msg [**size** *number*]
no monitor event-trace voip ccsip msg [**size** *number*]

Syntax Description

size *number*	(Optional) The number of message events that are stored for a specific connection (call leg). The range is from 1 to 1000000. The default value is 50.

Command Default

Message event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into Cisco IOS Release 15.3(3)S.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

VoIP CCSIP message events provide information about the SIP messages that are sent and received by the Cisco Unified Border Element (Cisco UBE).

Use the **size** keyword to set the number of events that are stored for this instance. If the number of events increases beyond this size, earlier events are overwritten. If you do not set a value for size, the system uses the default value.

Example

The following example shows how to enable event tracing for message events in the VoIP CCSIP subsystem component in Cisco IOS software:

```
Device(config)# monitor event-trace voip ccsip msg size 50
```

monitor event-trace voip ccsip stacktrace

To enable stack traces at trace points, and to specify the depth of the stack trace stored, use the **monitor event-trace voip ccsip stacktrace** command in global configuration mode. To stop stack traces at trace points, use the **no** form of this command.

monitor event-trace voip ccsip stacktrace *number*
no monitor event-trace voip ccsip stacktrace

Syntax Description

number	The depth of the stack trace stored. Valid values are from 1 to 12.

Command Default

Stack trace at trace points is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to enable stack trace at tracepoint and to configure the stack trace depth.

Example

The following example shows how to enable stack traces at trace points and to specify a stack trace depth of 9:

```
Device(config)# monitor event-trace voip ccsip stacktrace 9
```

monitor probe icmp-ping

To enable dial-peer status changes based on the results of probes from Internet Control Message Protocol (ICMP) pings, use the **monitor probe icmp-ping** command in dial-peer configuration mode. To disable this capability, use the **no** form of this command.

monitor probe [{**icmp-ping** | **rtr**}] [*ip-address*]
no monitor probe [{**icmp-ping** | **rtr**}] [*ip-address*]

Syntax Description

icmp-ping	(Optional) Specifies ICMP ping as the method for monitoring the destination target and updating the status of the dial peer.
rtr	(Optional) Specifies that the Response Time Reporter (RTR) probe is the method for monitoring the destination target and updating the status of the dial peer.
ip -address	(Optional) The destination IP address of a target interface for the probe signal.

Command Default

If this command is not entered, no ICMP or RTR probes are sent.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced in a release earlier than Cisco IOS Release 12.2(11)T.

Usage Guidelines

The principal use of this command is to specify ICMP ping as the probe method, even though the option for selecting RTR is also available.

In order for the **monitor probe icmp-ping** command to work properly, the **call fallback icmp-ping** command or the **call fallback active** command must be configured. One of these two commands must be in effect before the **monitor probe icmp-ping** command can be used.

If the **call fallback icmp-ping** command is not entered, the **call fallback active** command in global configuration is used for measurements. If the **call fallback icmp-ping** command is entered, these values override the global configuration.

Examples

The following example shows how to configure a probe to use ICMP pings to monitor the connection to IP address 10.1.1.1:

```
dial-peer voice tag voip
 call fallback icmp-ping
 monitor probe icmp-ping 10.1.1.1
```

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion and specifies the type of probe for pings to IP destinations.

Command	Description
call fallback icmp-ping	Specifies ICMP ping as the method for network traffic probe entries to IP destinations and configures parameters for the ping packets.
show voice busyout	Displays information about the voice busyout state.
voice class busyout	Creates a voice class for local voice busyout functions.

mrcp client accept-charset-compliance

To set the format of the Media Resource Control Protocol (MRCP) client as per RFC 2616, use the **mrcp client accept-charset-compliance** command in global configuration mode.

mrcp client accept-charset-compliance

Syntax Description

This command has no arguments or keywords.

Command Default

The default character set is **Accept-charset: charset: utf-8**.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

In a Cisco Voice Portal (CVP), the VXML gateway communicates with Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers using MRCP. Communication between the gateway and the ASR servers fails when the character set negotiation is incorrect.

The current character set, **Accept-Charset: charset: utf-8**, results in MRCP error on the VXML gateway. To resolve the MRCP error, use the command **mrcp client accept-charset-compliance** on the VXML gateway in global configuration mode. This command resets the character set as **Accept-charset: utf-8**, which is as per RFC 2616.

Examples

The following example sets the character set as per RFC 2616.

```
Router (config)# mrcp client accept-charset-compliance
```

mrcp client codec

To set the codec for communication between MRCP (Media Resource Control Protocol) client and the media processing resources such as Automatic Speech-Recognition (ASR) engines and Text-To-Speech (TTS) engines, use the **mrcp client codec** command in global configuration mode. To set the MRCP codec to the default g711ulaw, use the **no** form of this command.

mrcp client codec g711alaw
no mrcp client codec g711alaw

Syntax Description

g711alaw	Sets the audio codec for the MRCP client.

Command Default

Audio codec g711ulaw

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Audio codecs determine VoIP call quality.The default MRCP client codec is g711ulaw. Use this command to set the audio codec g711alaw for the MRCP client.

Examples

The following example sets the audio codec g711alaw for the MRCP client.

```
Router (config)# mrcp client codec g711alaw
```

mrcp client rtpsettup enable

To enable the sending of an IP address in the Real Time Streaming Protocol (RTSP) SETUP message, use the **mrcp client rtpsettup enable** command in global configuration mode. To disable sending of the IP address, use the **no** form of this command.

mrcp client rtpsettup enable
no mrcp client rtpsettup enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

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.

Examples

The following example shows how to enable the sending of IP address in the RTSP SETUP message:

```
Router# configure terminal
Router(config)# mrcp client rtpsetup enable
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mrcp client session history duration

To set the maximum number of seconds for which history records for Media Resource Control Protocol (MRCP) sessions are stored on the gateway, use the **mrcp client session history duration**command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client session history duration *seconds*
no mrcp client session history duration

Syntax Description

seconds	Maximum time, in seconds, for which MRCP history records are stored. Range is from 0 to 99999999. The default is 3600 (1 hour). If 0 is configured, no MRCP records are stored on the gateway.

Command Default

3600 seconds (1 hour)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command affects the number of records that are displayed when the **show mrcp client session history** command is used.

Active MRCP sessions are not affected by this command.

Examples

The following example sets the maximum amount of time for which MRCP history records are stored to 2 hours (7200 seconds):

```
Router(config)# mrcp client session history duration 7200
```

Related Commands

Command	Description
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.

mrcp client session history records

To set the maximum number of records of Media Resource Control Protocol (MRCP) client history that the gateway can store, use the **mrcp client session history records** command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client session history records *number*
no mrcp client session history records

Syntax Description

number	Maximum number of MRCP history records to save. The maximum value is platform-specific. The default is 50. If 0 is configured, no MRCP records are stored on the gateway.

Command Default

50 records

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command affects the number of records that are displayed when the **show mrcp client session history** command is used.

Active MRCP sessions are not affected by this command.

Examples

The following example sets the maximum number of MRCP records to 30:

```
Router(config)# mrcp client history records 30
```

Related Commands

Command	Description
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.

mrcp client session nooffailures

To configure the maximum number of consecutive failures before disconnecting calls, use the **mrcp client session nooffailures** command in global configuration mode. To disable the number of consecutive failures before disconnecting calls, use the **no** form of this command.

mrcp client session nooffailures *number*
no mrcp client session nooffailures

Syntax Description

number	Maximum number of consecutive failures before disconnecting calls. The range is from 1 to 50. The default is 20.

Command Default

The maximum number is set to 20.

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.

Examples

The following example shows how to configure the maximum number of consecutive failures before disconnecting calls:

```
Router# configure terminal
Router(config)# mrcp client session nooffailures 20
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mrcp client statistics enable

To enable Media Resource Control Protocol (MRCP) client statistics to be displayed, use the **mrcp client statistics enable**command in global configuration mode. To disable display, use the **no** form of this command.

mrcp client statistics enable
no mrcp client statistics enable

Syntax Description

This command has no arguments or keywords.

Command Default

MRCP client statistics are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command enables MRCP client statistics to be displayed when the **show mrcp client statistics hostname** command is used. If this command is not enabled, client statistics cannot be displayed for any host when the **show mrcp client statistics hostname** command is used.

Examples

The following example enables MRCP statistics to be displayed:

```
Router(config)# mrcp client statistics enable
```

Related Commands

Command	Description
show mrcp client statistics hostname	Displays statistics about MRCP sessions for a specific MRCP host.

mrcp client timeout connect

To set the number of seconds allowed for the router to establish a TCP connection to a Media Resource Control Protocol (MRCP) server, use the **mrcp client timeout connect**command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client timeout connect *seconds*
no mrcp client timeout connect

Syntax Description

seconds	Amount of time, in seconds, the router waits to connect to the server before timing out. Range is 1 to 20.

Command Default

3 seconds

Command Modes

Global configuration (global)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command determines when the router abandons its attempt to connect to an MRCP server and declares a timeout error, if a connection cannot be established after the specified number of seconds.

Examples

The following example sets the connection timeout to 10 seconds:

```
Router(config)# mrcp client timeout connect 10
```

mrcp client timeout message

To set the number of seconds that the router waits for a response from a Media Resource Control Protocol (MRCP) server, use the **mrcp client timeout message**command in global configuration mode. To reset to the default, use the **no** form of this command.

mrcp client timeout message *seconds*
no mrcp client timeout message

Syntax Description

seconds	Amount of time, in seconds, the router waits for a response from the server after making a request. Range is 1 to 20.

Command Default

3 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(15)T	This command was modified to support MRCP version 2 (MRCP v2).

Usage Guidelines

This command sets the amount of time the router waits for the MRCP server to respond to a request before declaring a timeout error.

Examples

The following example sets the request timeout to 10 seconds:

```
Router(config)# mrcp client timeout message 10
```

mta receive aliases

To specify a hostname accepted as a Simple Mail Transfer Protocol (SMTP) alias for off-ramp faxing, use the **mta receive aliases**command in global configuration mode. To disable the alias, use the **no** form of this command.

mta receive aliases *string*
no mta receive aliases *string*

Syntax Description

string	Hostname or IP address to be used as an alias for the SMTP server. If you specify an IP address to be used as an alias, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx]. Default is the domain name of the gateway.

Command Default

Enabled with an empty string

Command Modes

Global 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.
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

This command creates an accept or reject alias list. The first alias is used by the mailer to identify itself in SMTP banners and when generating its own RFC 822 Received: header.

Note This command does not automatically include reception for a domain IP address; the address must be explicitly added. To explicitly add a domain IP address, use the following format: **mta receive aliases** [*ip-address*] . Use the IP address of the Ethernet or the FastEthernet interface of the off-ramp gateway.

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

Examples

The following example specifies the host name "seattle-fax-offramp.example.com" as the alias for the SMTP server:

```
mta receive aliases seattle-fax-offramp.example.com
```

The following example specifies IP address 172.16.0.0 as the alias for the SMTP server:

```
mta receive aliases [172.16.0.0]
```

Related Commands

Command	Description
mta receive generate -mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta receive maximum -recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive disable-dsn

To stop the generation and delivery of a Delivery Status Notification (DSN) every time a failure occurs in a T.37 offramp call from a Cisco IOS gateway, use the **mta receive disable-dsn** command in global configuration mode. To restart the generation and delivery of DSNs when failures occur, use the **no** form of this command.

mta receive disable-dsn
no mta receive disable-dsn

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is not enabled, and a DSN message is generated from the gateway each time a T.37 offramp call fails.

Command Modes

Global configuration

Command History

Release	Modification
12.4(13)	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The T.37 offramp gateway generates DSN messages when calls are successful and when calls fail. The **mta receive disable-dsn** command disables the generation and delivery of DSN messages for successful calls and for failed calls.

A DSN message confirming a successful call is a useful notification tool with no negative impact on processing. However, when a T.37 offramp call is made from a Cisco IOS gateway, and the call fails (ring but no answer), the gateway automatically generates a DSN for each failure. The DSN is based on the Simple Mail Transport Protocol (SMTP) error (which is temporary), so the SMTP client tries to resend the fax every 5 minutes for up to 24 hours. These multiple DSNs eventually overload the sender's inbox.

Examples

The following example shows how to disable the generation and sending of DSNs from the offramp gateway:

```
mta receive disable-dsn
```

Related Commands

Command	Description
debug fax mta	Troubleshoots the fax mail transfer agent.
mta receive generate	Specifies the type of fax delivery response message that a T.37 fax off-ramp gateway should return.

mta receive generate

Note The **mta receive generate** command replaces the **mta receive generate-mdn** command.

To specify the type of fax delivery response message that a T.37 fax off-ramp gateway should return, use the **mta receive generate** command in global configuration mode. To return to the default, use the **no** form of this command.

mta receive generate [{**mdn** | **permanent-error**}]
no mta receive generate [{**mdn** | **permanent-error**}]

Syntax Description

mdn	Optional. Directs the T.37 off-ramp gateway to process response message disposition notifications (MDNs) from an Simple Mail Transfer Protocol (SMTP) server.
permanent-error	Optional. Directs the T.37 off-ramp fax gateway to classify all fax delivery errors as permanent so that they are forwarded in DSN messages with descriptive error codes to an mail transfer agent (MTA).

Command Default

MDNs are not generated and standard SMTP status messages are returned to the SMTP client with error classifications of permanent or transient.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced as **mta receive generate-mdn**.
12.0(4)T	The **mta receive generate-mdn** command was integrated into Cisco IOS Release 12.0(4)T.
12.3(7)T	The **mta receive generate-mdn** command was replaced by the **mta receive generate** command, which uses the **mdn** and **permanent-error**keywords.

Usage Guidelines

When the **mdn** keyword is used to enable MDN on a sending device, a flag is inserted in the off-ramp message e-mail header, requesting that the receiving device generate an MDN. The MDN is then returned to the sender when the e-mail message that contains the fax image is opened. Use this command to enable the receiving device--the off-ramp gateway--to process the response MDN.

Depending on the configuration, usage, and features of the mailers used at a site, it might be desirable to enable or disable MDN generation. Specifications for MDN are described in RFC 2298. Delivery status notification (DSN) generation cannot be disabled.

The **permanent-error** keyword directs the T.37 off-ramp fax gateway to classify all fax delivery errors as permanent so that they are forwarded in a DSN with descriptive error codes to the originating MTA. The descriptive error codes allow the MTA to control fax operations directly because the MTA can examine the error codes and make decisions about how to proceed with each fax (whether to retry or cancel, for example).

If this command is not used, the default is to return standard SMTP status messages to SMTP clients using both permanent and transient error classifications.

Examples

The following example allows a T.37 off-ramp gateway to process response MDNs:

```
Router(config)# mta receive generate mdn
```

The following example directs a T.37 off-ramp gateway to classify all fax delivery errors as permanent and forward the errors and descriptive text using SMTP DSNs to the MTA:

```
Router(config)# mta receive generate permanent-error
```

Related Commands

Command	Description
mdn	Requests that a message disposition notification be generated when a fax-mail message is processed (opened).
mta receive aliases	Specifies a host name that is accepted as an SMTP alias for off-ramp faxing.
mta receive generate-mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.
mta receive maximum-recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive generate-mdn

Note The **mta receive generate-mdn** command was replaced by the **mta receive generate** command in Cisco IOS Release 12.3(7)T.

To specify that the off-ramp gateway process a response message disposition notification (MDN) from a Simple Mail Transfer Protocol (SMTP) server, use the **mta receive generate-mdn**command in global configuration mode. To disable MDN generation, use the **no** form of this command.

mta receive generate-mdn
no mta receive generate-mdn

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global 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.
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

When MDN is enabled on a sending device, a flag is inserted in the off-ramp message e-mail header, requesting that the receiving device generate the MDN and return that message to the sender when the e-mail message that contains the fax image is opened. Use this command to enable the receiving device--the off-ramp gateway--to process the response MDN.

Depending on the configuration, usage, and features of the mailers used at a site, it might be desirable to enable or disable MDN generation. Specifications for MDN are described in RFC 2298. Delivery status notification (DSN) generation cannot be disabled.

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

Examples

The following example enables the receiving device to generate MDNs:

```
mta receive generate-mdn
```

Related Commands

Command	Description
mdn	Requests that a message disposition notification be generated when the fax-mail message is processed (opened).
mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
mta receive maximum -recipients	Specifies the maximum number of recipients for all SMTP connections.

mta receive maximum-recipients

To specify the maximum number of simultaneous recipients for all Simple Mail Transfer Protocol (SMTP) connections, use the **mta receive maximum-recipients**command in global configuration mode. To reset to the default, use the **no** form of this command.

mta receive maximum-recipients *number*
no mta receive maximum-recipients

Syntax Description

number	Maximum number of simultaneously recipients for all SMTP connections. Range is from 0 to 1024. The default is 0.

Command Default

0 recipients

Command Modes

Global 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.
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

Use thiscommand to configure the maximum number of resources that you want to allocate for fax usage at any one time. You can use this command to limit the resource usage on the gateway. When the value for the *number*argument is set to 0, no new connections can be established. Which is particularly useful when one is preparing to shut down the system.

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

The default of 0 recipients means that incoming mail messages are not accepted; therefore, no faxes are sent by the off-ramp gateway.

Note Unless the transmitting mailer supports the X-SESSION SMTP service extension, each incoming SMTP connection is allowed to send to only one recipient and thus consume only one outgoing voice feature card (VFC).

Examples

The following example sets the maximum number of simultaneous recipients for all SMTP connections to 10:

```
mta receive maximum-recipients 10
```

Related Commands

Command	Description
mta receive aliases	Specifies a host name accepted as an SMTP alias for off-ramp faxing.
mta receive generate -mdn	Specifies that the off-ramp gateway process a response MDN from an SMTP server.

mta send filename

To specify a filename for a TIFF file attached to an e-mail, use the mta send filename command in global configuration mode. To disable the configuration after the command has been used, use the **no** form of this command.

mta send filename [*string*] [**date**]
no mta send filename

Syntax Description

string	(Optional) Name of the TIFF file attached to an e-mail. If this text string does not contain an extension for the filename, ".tif" is added to the formatted filename.
date	(Optional) Adds today's date in the format yyyymmdd to the filename of the TIFF attachment.

Command Default

The formatted filename for TIFF attachments is "Cisco_fax.tif"

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use this command to specify the filename for a TIFF file attached to an e-mail.

Examples

The following example specifies a formatted filename of "abcd.tif" for the TIFF attachment:

```
Router(config)# mta send filename abcd
```

The following example specifies a formatted filename and extension of "abcd.123" for the TIFF attachment:

```
Router(config)# mta send filename abcd.123
```

The following example specifies a formatted filename "abcd_today's date" (so, for July 4, 2002, the filename would be "abcd_20020704.tif") for the TIFF attachment:

```
Router(config)# mta send filename abcd date
```

The following example specifies a formatted filename and extension of "abcd_today's date.123" (so, for July 4, 2002, the filename would be "abcd_20020704.123") for the TIFF attachment:

```
Router(config)# mta send filename abcd.123 date
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.

Command	Description
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send mail-from

To specify a mail-from address (also called the RFC 821 envelope-from address or the return-path address), use the **mta send mail-from**command in global configuration mode. To remove this return-path information, use the **no** form of this command.

mta send mail-from {**hostname** *string* | **username** *string* | **username s**}
no mta send mail-from {**hostname** *string* | **username** *string* | **username s**}

Syntax Description

hostname *string*	Simple Mail Transfer Protocol (SMTP) host name or IP address. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
username *string*	Sender username.
username s	Wildcard that specifies that the username is derived from the calling number.

Command Default

No default behavior or values

Command Modes

Global 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.
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

Use this command to designate the sender of the fax TIFF attachment, which is equivalent to the return path in an e-mail message. If the mail-from address is blank, the postmaster address, configured with the **mta send postmaster** command, is used.

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

Examples

The following example specifies that the mail-from username information is derived from the calling number of the sender:

```
mta send mail-from username $s$
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send origin-prefix

To add information to an e-mail prefix header, use the **mta send origin-prefix**command in global configuration mode. To remove the defined string, use the **no** form of this command.

mta send origin-prefix *string*
no mta send origin-prefix *string*

Syntax Description

string	Text string to add comments to the e-mail prefix header. If this string contains more than one word, the string value should be enclosed within quotation marks ("abc xyz").

Command Default

Null string

Command Modes

Global 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.
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

Store-and-forward fax provides the slot and port number from which an e-mail comes. In the e-mail prefix header information, use this command to define a text string to be added to the front of the e-mail prefix header information. This text string is a prefix string that is added with the modem port and slot number and passed in the originator_comment field of the esmtp_client_engine_open() call. Eventually, this text ends up in the received header field of the fax-mail message; for example:

```
Received (test onramp Santa Cruz slot1 port15) by router-5300.cisco.com for
<test-test@cisco.com> (with Cisco NetWorks); Fri, 25 Dec 1998 001500 -0800
```

Using the command **mta send origin-prefix dog** causes the received header to contain the following information:

```
Received (dog, slot 3 modem 8) by as5300-sj.example.com ....
```

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

Examples

The following example adds information to the e-mail prefix header:

```
mta send origin-prefix "Cisco-Powered Fax System"
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send postmaster

To specify the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination, use the **mta send postmaster**command in global configuration mode. To remove the specification, use the **no** form of this command.

mta send postmaster *e-mail-address*
no mta send postmaster *e-mail-address*

Syntax Description

e -mail-address	Address of the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to its intended destination.

Command Default

No e-mail destination is defined

Command Modes

Global 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.
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

If you have configured a router to generate delivery status notifications (DSNs) and message disposition notifications (MDNs), but you have not configured the sender information (using the **mta send mail-from** command) or the Simple Mail Transfer Protocol (SMTP) server, DSNs and MDNs are delivered to the e-mail address determined by this command.

It is recommended that an address such as "fax-administrator@example.com" be used to indicate fax responsibility. In this example, fax-administrator is aliased to the responsible person. At some sites, this could be the same person as the e-mail postmaster, but most likely is a different person with a different e-mail address.

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

Examples

The following example configures the e-mail address "fax-admin@example.com" as the sender for all incoming faxes. Thus, any returned DSNs are delivered to "fax-admin@example.com" if the mail-from field is blank.

```
mta send postmaster fax-admin@example.com
```

Related Commands

Command	Description
mta send mail -from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin -prefix	Adds information to an e-mail prefix header.
mta send return -receipt-to	Specifies the address to which where MDNs are sent.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send return-receipt-to

To specify the address to which message disposition notifications (MDNs) are sent, use the **mta send return-receipt-to**command in global configuration mode. To remove the address, use the **no** form of this command.

mta send return-receipt-to {**hostname** *string* | **username** *string* | **s**}
no mta send return-receipt-to {**hostname** *string* | **username** *string* | **s**}

Syntax Description

hostname *string*	Simple Mail Transfer Protocol (SMTP) host name or IP address where MDNs are sent. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
username *string*	Username of the sender to which MDNs are to be sent.
s	Wildcard that specifies that the calling number (ANI) generates the disposition-notification-to e-mail address.

Command Default

No address is defined

Command Modes

Global 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.
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

Use this command to specify where you want MDNs to be sent after a fax-mail is opened.

Note Store-and-forward fax supports the Eudora proprietary format, meaning that the header that store-and-forward fax generates is in compliance with RFC 2298 (MDN).

Note Multimedia Mail over IP (MMoIP) dial peers must have MDN enabled in order to generate return receipts in off-ramp fax-mail messages.

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

Examples

The following example configures "xyz" as the user and "server.com" as the SMTP mail server to which MDNs are sent:

```
mta send return-receipt-to hostname server.com
mta send return-receipt-to username xyz
```

Related Commands

Command	Description
mta send mail -from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin -prefix	Adds information to the e-mail prefix header.
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send server	Specifies a destination mail server or servers.
mta send subject	Specifies the subject header of an e-mail message.

mta send server

To specify a destination mail server or servers, use the **mta send server**command in global configuration mode. To remove the specification, use the **no** form of this command.

mta send server {*host nameip-address*}
no mta send server {*host nameip-address*}

Syntax Description

hostname	Hostname of the destination mail server.
ip -address	IP address of the destination mail server.

Command Default

IP address defined as 0.0.0.0

Command Modes

Global 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.
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

Use this command to provide a backup destination server in case the first configured mail server is unavailable. This command is not intended to be used for load distribution.

You can configure up to ten different destination mail servers using this command. If you configure more than one destination mail server, the router attempts to contact the first mail server configured. If that mail server is unavailable, it contacts the next configured destination mail server.

DNS mail exchange (MX) records are not used to look up host names provided to this command.

Note When you use thiscommand, configure the router to perform name lookups using the **ip name-server** command.

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

Examples

The following example defines the mail servers "xyz.example.com" and "abc.example.com" as the destination mail servers:

```
mta send server xyz.example.com
mta send server abc.example.com
```

Related Commands

Command	Description
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to the e-mail prefix header.
mta send postmaster	Specifies the mail-server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send subject	Specifies the subject header of an e-mail message.

mta send success-fax-only

To configure the router to send only successful fax messages and drop failed fax messages, use the **mta send success-fax-only** command in global configuration mode. To disable this functionality, use the **no** form of this command.

mta send success-fax-only
no mta send success-fax-only

Syntax Description

This command has no arguments or keywords.

Command Default

The router is configured to send all fax messages.

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.

Examples

The following example shows how to configure the router to send only successful fax messages drop failed fax messages:

```
Router# configure terminal
Router(config)# mta send success-fax-only
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	Specifies the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.

mta send subject

To specify the subject header of an e-mail message, use the **mta send subject**command in global configuration mode. To remove the string, use the **no** form of this command.

mta send subject *string*
no mta send subject *string*

Syntax Description

string	Subject header of an e-mail message.

Command Default

Null string

Command Modes

Global 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.
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

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

Note The string does not have to be enclosed in quotation marks.

Examples

The following example defines the subject header of an e-mail message as "fax attachment":

```
mta send subject fax attachment
```

Related Commands

Command	Description
mta send mail-from	Specifies the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address).
mta send origin-prefix	Adds information to an e-mail prefix header.

Command	Description
mta send postmaster	To which an e-mail message should be delivered. Specifies the mail server postmaster account to which if it cannot be delivered to the intended destination.
mta send return-receipt-to	Specifies the address to which MDNs are sent.
mta send server	Specifies a destination mail server or servers.

mta send with-subject

To configure the subject attached with called or calling numbers, use the **mta send with-subject** command in global configuration mode. To disable the subject attached with called or calling numbers, use the **no** form of this command.

mta send with-subject {**d** | **s** | **both**}
no mta send with-subject

Syntax Description

d	Configures the subject attached with called number.
s	Configures the subject attached with calling number.
both	Configures the subject attached with both called and calling numbers.

Command Default

The subject is not attached with the calling or called numbers.

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 **mta send with-subject both** command instructs the router to include the calling and called party number in the "Subject:" line of the e-mail. This helps to route the fax e-mail to the appropriate mailbox.

Examples

The following example shows how to include the calling and the called party number in the "Subject:" line of the e-mail:

```
Router# configure terminal
Router(config)# mta send with-subject both
```

Related Commands

Command	Description
mta send origin-prefix	Adds information to an e-mail prefix header.
mta send postmaster	Specifies the mail server postmaster account to which an e-mail message should be delivered if it cannot be delivered to the intended destination.
mta send server	Specifies a destination mail server or servers.

music-threshold

To specify the threshold for on-hold music for a specified voice port, use the **music-threshold**command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

music-threshold *decibels*
no music-threshold *decibels*

Syntax Description

decibels	On-hold music threshold, in decibels (dB). Range is from -70 to -10 (integers only). The default is -38 dB.

Command Default

-38 dB

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(4)T	This command was implemented on the Cisco MC3810.
12.3(4)XD	The range of values for the *decibels*argument was increased.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Usage Guidelines

Use thiscommand to specify the decibel level of music played when calls are put on hold. This command tells the firmware to pass steady data above the specified level. It affects the operation of voice activity detection (VAD) only when the voice port is receiving voice.

If the value for this command is set too high, VAD interprets music-on-hold as silence, and the remote end does not hear the music. If the value for this command is set too low, VAD compresses and passes silence when the background is noisy, creating unnecessary voice traffic.

Examples

The following example sets the decibel threshold to -35 for the music played when calls are put on hold:

```
voice port 0:D
 music-threshold -35
```

The following example sets the decibel threshold to -35 for the music played when calls are put on hold on a Cisco 3600 series router:

```
voice-port 1/0/0
```

music-threshold -35

mwi

To enable message-waiting indication (MWI) for a specified voice port, use the **mwi**command in voice-port configuration mode. To disable MWI for a specified voice port, use the **no** form of this command.

mwi
no mwi

Syntax Description

This command has no arguments or keywords.

Command Default

MWI is disabled by default.

Command Modes

Voice-port configuration

Command History

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

Usage Guidelines

Use the **mwi** command to enable MWI functionality on the voice port and the **mwi-server** command to configure the voice-mail server to send MWI notifications. If the voice port does not have MWI enabled, the voice gateway returns a 481 Call Leg/Transaction Does Not Exist message to the voice-mail server. If there are multiple dial peers associated with the same FXS voice port, multiple subscriptions are sent to the voice-mail server.

Examples

The following example shows MWI set on a voice port.

```
voice-port 2/2
 cptone us
 mwi
```

Related Commands

Command	Description
mwi-server	Specifies voice-mail server settings on a voice gateway or UA.

mwi (supplementary-service)

To set the type of message waiting indication (MWI) when a voicemail is available, use the **mwi** command in supplementary-service configuration mode. To return to the default setting, use the **no** form of this command.

mwi {**audible** | **visible** | **both**}
no mwi

Syntax Description

audible	Audible message waiting indication (AMWI) is enabled.
visible	Visible message waiting indication (VMWI) is enabled.
both	Default configuration. Both AMWI and VMWI are enabled.

Command Default

Both AMWI and VMWI are enabled by default.

Command Modes

Supplementary-service configuration (config-stcapp-suppl-serv)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **mwi** command to enable MWI as audible only (AMVI), visible only (VMWI), or both (AMVI/VMWI).

When a voicemail is available, you go offhook to hear a special AMWI tone or you go onhook to see an MWI light (when the phone is equipped with one).

Examples

The following example shows how to set the type of MWI on voice ports 2/1, 2/2, and 2/3:

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/1
Router(config-stcapp-suppl-serv-port)# fallback-dn 3001
Router(config-stcapp-suppl-serv)# port 2/2
Router(config-stcapp-suppl-serv-port)# fallback-dn 3102
Router(config-stcapp-suppl-serv-port)# mwi visible
Router(config-stcapp-suppl-serv)# port 2/3
Router(config-stcapp-suppl-serv-port)# fallback-dn 3203
Router(config-stcapp-suppl-serv-port)# mwi audible
```

Related Commands

Command	Description
stcapp supplementary-services	Enters supplementary-service configuration mode for configuring STCAPP supplementary-service features on an FXS port.

mwi-server

To specify voice-mail server settings on a voice gateway or user agent (UA), use the **mwi-server** command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

mwi-server {**ipv4:***destination-address* | **dns:***host-name*} [{**expires** *seconds*}] [{**port** *port*}] [{**transport** {**tcp** | **udp**}}] [{**unsolicited**}]
no mwi-server

Syntax Description

ipv4: *destination -address*	IP address of the voice-mail server.
dns: *host -name*	Host device housing the domain name server that resolves the name of the voice-mail server. • *host -name* --String that contains the complete host name to be associated with the target address; for example, **dns:test.cisco.com**.
expires *seconds*	(Optional) Subscription expiration time, in seconds. The range is 1 to 999999. The default is 3600.
port *port*	(Optional) Defines the port number on the voice-mail server. The default is 5060.
transport {**tcp** | **udp**	(Optional) Defines the transport protocol to the voice-mail server. Choices are **tcp** or **udp**. UDP is the default.
unsolicited	(Optional) Requires the voice-mail server to send a SIP notification message to the voice gateway or UA if the mailbox status changes. Removes the requirement that the voice gateway subscribe for MWI service.

Command Default

Voice-mail server settings are disabled by default.

Command Modes

SIP user-agent configuration

Command History

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

Usage Guidelines

Using the **mwi-server** command a user can request that the UA subscribe to a voice-mail server requesting notification of mailbox status. When there is a status change, the voice-mail server notifies the UA. The UA then indicates to the user that there is a change in mailbox status with an MWI tone when the user takes the phone off-hook.

Only one voice-mail server can be configured per voice gateway. Use the **mwi-server** command with the **mwi** command to enable MWI functionality on the voice port. If the voice port does not have MWI enabled, the voice gateway returns a 481 Call Leg/Transaction Does Not Exist message to the voice-mail server. MWI status is always reset after a router reload.

Examples

The following example specifies voice-mail server settings on a voice gateway. The example includes the **unsolicited** keyword, enabling the voice-mail server to send a SIP notification message to the voice gateway or UA if the mailbox status changes.

```
sip-ua
 mwi-server dns:test.cisco.com expires 60 port 5060 transport udp unsolicited
```

For unsolicited Notify, the Contact header derives the voice-mail server address. If the unsolicited MWI message does not contain a Contact header, configure the voice-mail server on the gateway with the following special syntax to accept MWI Notify messages.

```
sip-ua
 mwi-server ipv4:255.255.255.255 unsolicited
```

Related Commands

Command	Description
mwi	Enables MWI for a specified voice port.
sip-us	Enables SIP user-agent configuration mode.
voice-port	Enters voice-port configuration mode.