

mgcp persistent through mmoip aaa send-id secondary

- mgcp persistent, on page 3
- mgcp piggyback message, on page 4
- mgcp playout, on page 5
- mgcp profile, on page 7
- mgcp quality-threshold, on page 9
- mgcp quarantine mode, on page 11
- mgcp quarantine persistent-event disable, on page 13
- mgcp request retries, on page 14
- mgcp request timeout, on page 15
- mgcp restart-delay, on page 17
- mgcp rtp payload-type, on page 18
- mgcp rtp unreachable timeout, on page 21
- mgcp rtrcac, on page 23
- mgcp sched-time, on page 24
- mgcp sdp, on page 25
- mgcp sgcp disconnect notify, on page 27
- mgcp sgcp restart notify, on page 29
- mgcp src-cac, on page 30
- mgcp timer, on page 31
- mgcp tse payload, on page 34
- mgcp vad, on page 36
- mgcp validate call-agent source-ipaddr, on page 37
- mgcp validate domain-name, on page 38
- mgcp voice-quality-stats, on page 42
- microcode reload controller, on page 44
- midcall-signaling, on page 45
- min-se (SIP), on page 47
- mmoip aaa global-password, on page 49
- mmoip aaa method fax accounting, on page 50
- mmoip aaa method fax authentication, on page 52
- mmoip aaa receive-accounting enable, on page 53

- mmoip aaa receive-authentication enable, on page 54
- mmoip aaa receive-id primary, on page 55
- mmoip aaa receive-id secondary, on page 57
- mmoip aaa send-accounting enable, on page 59
- mmoip aaa send-authentication enable, on page 60
- mmoip aaa send-id primary, on page 61
- mmoip aaa send-id secondary, on page 63

mgcp persistent

To configure the sending of persistent events from the Media Gateway Control Protocol (MGCP) gateway to the call agent, use the **mgcp persistent**command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp persistent {**hookflash** | **offhook** | **onhook**}
no mgcp persistent {**hookflash** | **offhook** | **onhook**}

Syntax Description

hookflash	Sends persistent hookflash events to the call agent.
offhook	Sends persistent off-hook events to the call agent.
onhook	Sends persistent on-hook events to the call agent.

Command Default

The **hookflash** keyword is disabled for persistence. The **offhook** keyword is enabled for persistence. The **onhook** keyword is disabled for persistence.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Persistent events are those events that, once they are detected, are defined as reportable to the call agent whether or not the call agent has explicitly requested to be notified of their occurrence; that is, even if they are not included in the list of RequestedEvents that the gateway is asked to detect and report. Such events can include fax tones, continuity tones, and on-hook transition. Each event has an associated action for the gateway to take.

Use this command for each type of persistent event that should override the default behavior.

Examples

The following example configures the gateway to send persistent on-hook events to the call agent:

```
Router(config)# mgcp persistent onhook
```

Related Commands

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

mgcp piggyback message

To enable piggyback messages, use the **mgcp piggyback message**command in global configuration mode. To disable piggyback messages, use the **no** form of this command.

mgcp piggyback message
no mgcp piggyback message

Syntax Description

This command has no arguments or keywords.

Command Default

Piggyback messages are enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the network gateway cannot handle piggyback messages, us e the no form of this command to disable the piggyback messages and to enable Media Gateway Control Protocol (MGCP) 1.0, Network-based Call Signaling (NCS), and Trunking Gateway Control Protocol (TGCP). Piggyback messaging is not available to Simple Gateway Control Protocol (SGCP) and MGCP 0.1.

The term piggyback message refers to a situation in which a gateway or a call agent sends more than one MGCP message in the same User Datagram Protocol (UDP) packets. The recipient processes the messages individually, in the order received. However, if a message must be retransmitted, the entire datagram is resent. The recipient must be capable of sorting out the messages and keeping track of which messages have been handled or acknowledged.

Piggybacking is used during retransmission of a message to send previously unacknowledged messages to the call agent. This maintains the order of events the call agent receives and makes sure that RestartInProgress (RSIP) messages are always received first by a call agent.

Examples

The following example disables piggyback messages:

```
Router(config)# no
mgcp piggyback message
```

Related Commands

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

mgcp playout

To tune the jitter-buffer packet size attempted for MGCP-controlled connections, use the **mgcp playout** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp playout {**adaptive** *init-milliseconds min-milliseconds max-milliseconds* | **fax** *milliseconds* | **fixed** *milliseconds* [**no-timestamps**]}
no mgcp playout {**adaptive** | **fax** | **fixed**}

Syntax Description

adaptive *init -milliseconds min-milliseconds max-milliseconds*	Sets the range, in milliseconds (ms), for the jitter-buffer packet size. Range for each value is 4 to 250. Note that *init-milliseconds* must be between *min-milliseconds* and *max-milliseconds*. Default: 60 4 200.
fax *milliseconds*	Sets the value for the fax playout buffer size. Range: 1 to 700. Default: 300. **Note** The range and default value might vary with different platforms. See the platform digital signal processor (DSP) specifications before setting this value.
fixed *milliseconds*	Sets the fixed size, in milliseconds, for the jitter-buffer packet size. Range: 4 to 1000. There is no default value.
no-timestamps	(Optional) Fixes the jitter buffer at a constant delay without time stamps.

Command Default

The MGCP jitter playout-delay buffer is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.2(11)T	This command was implemented on the Cisco AS5850.
12.2(13)T	This command was modified. The **fax** keyword was added.
15.1(1.8)T	This command was modified. The **no-timestamps** keyword was added and the fixed range value was increased from 250 to 1000.

Examples

The following example configures a jitter buffer to an initial playout of 100 ms, minimum buffer size of 50 ms, and maximum buffer size of 150 ms:

```
Router(config)# mgcp playout adaptive 100 50 150
```

The following example configures a fax playout buffer size of 200 ms.

```
Router(config)# mgcp playout fax 200
```

The following example configures a jitter buffer to a fixed playout of 120 ms:

```
Router(config)# mgcp playout fixed 120
```

The following example configures a jitter buffer to a fixed playout of 65 ms delay without time stamps:

```
Router(config)# mgcp playout fixed 65 no-timestamps
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
playout-delay	Tunes the playout buffer on DSPs to accommodate packet jitter caused by switches in the WAN.
playout-delay mode	Selects fixed or adaptive mode for playout delay from the jitter buffer on DSPs.

mgcp profile

To create and configure a Media Gateway Control Protocol (MGCP) profile to be associated with one or more MGCP endpoints or to configure the default MGCP profile, use the **mgcp profile** command in global configuration mode. To delete the profile, use the **no**form of this command.

mgcp profile {*profile-name* | **default**}
no mgcp profile {*profile-name* | **default**}

Syntax Description

profile-name	Identifying name for the user-defined profile to be configured. The name can be a maximum of 32 characters.
default	The default profile is to be configured.

Command Default

If this command is not used, there are no MGCP profiles created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.4(24)T3	The maximum number of MGCP profiles that can be configured was increased from 13 (12 plus 1 default) to 29 (28 plus 1 default).

Usage Guidelines

An MGCP profile is a subset of endpoints on a media gateway. More than one MGCP profile can be configured on a gateway at the same time. Prior to Cisco IOS Release 12.2(24)T3, the maximum number of MGCP profiles was 13 (12 plus 1 default). Beginning in Cisco IOS Release 12.2(24)T3, the maximum number of MGCP profiles is 29 (28 plus 1 default). The **voice-port** command in MGCP profile configuration mode associates endpoints with the profile.

There are two types of MGCP parameters: global and profile-related. The parameters that are configured in MGCP profile configuration mode are the profile-related parameters. However, endpoints do not need to belong to an MGCP profile. When endpoints are not associated with any MGCP profile, values for the profile-related MGCP parameters are provided by a *default profile* . Although all of the parameters for the default profile have default values, they can also be configured in the same way that an MGCP profile is configured by simply using the **default** keyword instead of a profile name. The main difference between a default profile and a user-defined profile is that there is no voice-port or call-agent association in the default profile, but they are required in user-defined profiles. When configuring the default profile, do not use the **call-agent** command or the **voice-port** command.

This command initiates MGCP profile configuration mode, in which you create an MGCP profile for an endpoint or a set of endpoints on a media gateway, and you set parameters for that profile or for the default profile.

Examples

The following example shows the definition of the MGCP profile named newyork:

```
Router(config)# mgcp profile newyork

Router(config-mgcp-profile)# call-agent 10.14.2.200 4000 service-type mgcp version 1.0
Router(config-mgcp-profile)# voice-port 0:1
Router(config-mgcp-profile)# package persistent mt-package
Router(config-mgcp-profile)# timeout tsmax 100
Router(config-mgcp-profile)# timeout tdinit 30
Router(config-mgcp-profile)# timeout tcrit 600
Router(config-mgcp-profile)# timeout tpar 600
Router(config-mgcp-profile)# timeout thist 60
Router(config-mgcp-profile)# timeout tone mwi 600
Router(config-mgcp-profile)# timeout tone ringback 600
Router(config-mgcp-profile)# timeout tone ringback connection 600
Router(config-mgcp-profile)# timeout tone network congestion 600
Router(config-mgcp-profile)# timeout tone busy 600
Router(config-mgcp-profile)# timeout tone dial 600
Router(config-mgcp-profile)# timeout tone dial stutter 600
Router(config-mgcp-profile)# timeout tone ringing 600
Router(config-mgcp-profile)# timeout tone ringing distinctive 600
Router(config-mgcp-profile)# timeout tone reorder 600
Router(config-mgcp-profile)# timeout tone cot1 600
Router(config-mgcp-profile)# timeout tone cot2 600
Router(config-mgcp-profile)# max1 retries 10
Router(config-mgcp-profile)# no max2 lookup
Router(config-mgcp-profile)# max2 retries 10
Router(config-mgcp-profile)# exit
```

Related Commands

Command	Description
call-agent	Defines the call agent for an MGCP profile.
mgcp	Starts and allocates resources for the MGCP daemon.
voice-port	Enters voice-port configuration mode.

mgcp quality-threshold

To set the jitter buffer size threshold, latency threshold, and packet-loss threshold parameters, use the **mgcp quality-threshold** command in global configuration mode. To reset to the defaults, use the **no** form of this command.

mgcp quality-threshold {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*}
no mgcp quality-threshold {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*}

Syntax Description

hwm -cell-loss *value*	High-water-mark cell loss count, when the ATM package is enabled. Range is from 5000 to 25000. Default is 10000.
hwm -jitter-buffer*value*	High-water-mark jitter buffer size, in milliseconds. Range is from 100 to 200. Default is 150.
hwm -latency*value*	High-water-mark latency value, in milliseconds. Range is from 250 to 400. Default is 300.
hwm -packet-loss *value*	High-water-mark packet loss value, in milliseconds. Range is from 5000 to 25,000. Default is 10000.
lwm -cell-loss *value*	Low-water-mark cell loss count, when the ATM package is enabled. Range is from 1 to 3000. Default is 1000.
lwm -jitter-buffer *value*	Low-water-mark jitter buffer size, in milliseconds. Range is from 4 to 60. Default is 30.
lwm -latency *value*	Low-water-mark latency value, in milliseconds. Range is from 125 to 200. Default is 150.
lwm -packet-loss *value*	Low-water-mark packet-loss value, in milliseconds. Range is from 1 to 3000. Default is 1000.

Command Default

High-water-mark cell loss count: 10000 cells High-water-mark jitter buffer size: 150 ms High-water-mark latency value: 300 ms High-water-mark packet loss value: 10000 ms Low-water-mark cell loss count:1000 cells Low-water-mark jitter buffer size: 30 ms Low-water-mark latency value: 150 ms Low-water-mark packet-loss value:1000 ms

Command Modes

Global configuration

Command History

Release	Modification
11.3(3)T	The default was changed to 100 milliseconds.
12.1(1)T	This command was implemented on the Cisco AS5300.

Release	Modification
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810. The **hwm-cell-loss** and **lwm-cell-loss**keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The following impact the quality of voice calls:

- **Cell loss** (the number of ATM cells lost during transmission)
- **Jitter buffer** (storage area containing active call voice packets that have been received from the network and are waiting to be decoded and played)
- **Latency** (network delay in sending and receiving packets)
- **Packet loss** (number of packets lost per 100,000 packets for a given call)

For good voice quality, the system should perform below the low water mark values. As the values go higher, voice quality degrades. The system generates a report when the values go above the high water marks levels. Set the high water marksand low water marks values sufficiently apart so that you receive reports on poor performance, but not so close together that you receive too much feedback.

Enter each parameter as a separate command.

Examples

The following example sets various keywords to new values:

```
Router(config)# mgcp quality-threshold hwm-jitter-buffer 100
Router(config)# mgcp quality-threshold hwm-latency 250
Router(config)# mgcp quality-threshold hwm-packet-loss 5000
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp package -capability	Activates various packages on the gateway.
mgcp playout	Tunes the jitter buffer packet size.

mgcp quarantine mode

To configure the mode for Media Gateway Control Protocol (MGCP) quarantined events, use the **mgcp quarantine mode**command inglobal configuration mode. To reset to the default, use the **no**form of this command.

mgcp quarantine mode [**discard** | **process**] [**loop** | **step**]
no mgcp quarantine mode

Syntax Description

discard	Enables discarding of quarantined events instead of processing. Observed events are not reported to the call agent, even if the call agent is ready to receive them.
loop	Enables loop mode for quarantined events instead of stepping. After receiving a request from the call agent, the gateway reports the observed events to the call agent in multiples without waiting for subsequent requests.
process	Enables processing of quarantined events instead of discarding. Observed events are reported to the call agent when the call agent is ready to receive them.
step	Enables step mode for quarantined events instead of looping. After receiving a request from the call agent, the gateway reports observed events individually to the call agent, one for each request.

Command Default

If no event is specified the default is **step**.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XA	This command was modified to support MGCP.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

Quarantine events are defined as events that have been detected by the gateway before the arrival of the MGCP NotificationRequest command but that have not yet been notified to the call agent. They are held in the quarantine buffer until receipt of the MGCP NotificationRequest command, when the gateway is expected to generate either one notification (step by step) or multiple notifications (loop) in response to this request (the default is exactly one), based on the configuration of **the mgcp quarantine mode** command.

This command supports backward compatibility with SGCP implementations running under the MGCP application. SGCP does not have a way to allow the call agent to control the quarantine mode. MGCP has this functionality.

When the gateway is in the notification state, the interdigit timer (Tcrit) is not started.

When the gateway receives an unsuccessful NotificationRequest, the current RequestEventList and SignalEventList are emptied. The ObservedEventList and quarantine buffer are also emptied.

Changes to the quarantine mode only take effect when the gateway is rebooted or the MGCP application is restarted.

Examples

The following example starts the MGCP application:

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

The following example stops the MGCP application:

```
Router(config)# no mgcp
```

The following example turns on processing of quarantined events and sends observed events to the call agent:

```
Router(config)# mgcp quarantine mode process
```

The following example turns off processing of quarantined events:

```
Router(config)# no mgcp quarantine mode discard
```

The following example sends observed events to the call agent in loop mode:

```
Router(config)# mgcp quarantine mode process loop
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp quarantine persistent -event disable	Disables handling of persistent call events in the quarantine buffer.

mgcp quarantine persistent-event disable

To disable handling of persistent call events in the Media Gateway Control Protocol (MGCP) quarantine buffer, use the **mgcp quarantine persistent-events disable** command in global configuration mode. To reset to the default state, use the **no** form of this command.

mgcp quarantine persistent-event disable
no mgcp quarantine persistent-event disable

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent events are held in the events buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XA	This command was modified to support MGCP.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command enables the reporting of persistent events immediately to the call agent rather than holding the events in quarantine. Persistent events are events defined as reportable whether or not the call agent explicitly has requested to be notified of their occurrence. Quarantining means that the gateway observes events but does not report them to the call agent until the call agent indicates readiness to receive notifications. By default, all events, including persistent events, are quarantined when they are detected, even when the gateway is in a notification state. When the **mgcp quarantine persistent-event disable** command is configured, however, persistent events are reported to the call agent immediately by an MGCP Notify command.

Examples

The following example disables quarantine buffer handling of persistent events:

```
Router(config)# mgcp quarantine persistent-event disable
```

Related Commands

Command	Description
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp quarantine mode	Configures MGCP event quarantine buffer handling mode.

mgcp request retries

This command was added in Cisco IOS Release 12.1(1)T. Beginning in Cisco IOS Release 12.2(2)XA and Cisco IOS Release 12.2(4)T, this command is supported no longer. It has been replaced by the MGCP profile **max1 retries** and **max2 retries** commands.

mgcp request timeout

To specify how long a Media Gateway Control Protocol (MGCP) gateway waits for a call-agent response to a request before retransmitting the request, use the **mgcp request timeout** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp request timeout {*timeout-value* | **max** *maxtimeout-value*}
no mgcp request timeout [**max**]

Syntax Description

timeout -value	Time, in milliseconds, to wait for a response to a request. Range is 1 to 10000. Default is 500.
max *maxtimeout -value*	Maximum timeout, in milliseconds. Default is 4000.

Command Default

timeout-value: 500 ms maxtimeout-value: 4000 ms

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3660, and Cisco uBR924.
12.1(5)XM	This command was implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XA	The **max** keyword was added to this command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T and implemented on the Cisco uBR925.
12.2(11)T	This command was implemented on the Cisco AS5850.

Usage Guidelines

The request timeout value sets the initial time period that an MGCP gateway waits for a response from the call agent before retransmitting the message. The interval doubles with each retransmission. The request timeout maximum value sets an upper limit on the timeout interval.

Examples

The following example sets a router to wait 40 ms for a reply to the first request before retransmitting and limits subsequent interval maximums to 10,000 ms (10 seconds):

```
Router(config)# mgcp request timeout 40
Router(config)# mgcp request timeout max 10000
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp request retries	Specifies the number of times to retry sending the mgcp command.

mgcp restart-delay

To select the delay value sent in the Restart in Progress (RSIP) graceful teardown, use the **mgcp restart-delay** command in global configuration mode. To reset to the default, use the **no** form of this command.

mgcp restart-delay *value*
no mgcp restart-delay

Syntax Description

value	Restart delay value, in seconds. Range is 0 to 600. The default is 0.

Command Default

0 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to send an RSIP message indicating when the connection in the gateway is to be torn down.

Examples

The following example sets the restart delay to 30 seconds:

```
Router(config)# mgcp restart-delay 30
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp max -waiting-delay	Specifies the MGCP maximum waiting delay after a restart.

mgcp rtp payload-type

To specify use of the correct Real-time Transport Protocol (RTP) payload type for backward compatibility in Media Gateway Control Protocol (MGCP) networks, use the **mgcp rtp payload-type** command in global configuration mode. To restore default values for payload types, use the **no** form of this command.

Fax and Modem Codecs
mgcp rtp payload-type {**cisco-codec-fax-ack** | **cisco-codec-fax-ind** | **cisco-pcm-switch-over-alaw127** | **cisco-pcm-switch-over-ulaw 126**}
no mgcp rtp payload-type {**cisco-codec-fax-ack** | **cisco-codec-fax-ind** | **cisco-pcm-switch-over-alaw127** | **cisco-pcm-switch-over-ulaw 126**}

Named Signaling and Telephony Events
mgcp rtp payload-type {**nse** | **nte**} *number*
no mgcp rtp payload-type {**nse** | **nte**}

Voice Codecs
mgcp rtp payload-type {**clear-channel** | **g726r16** | **g726r24**} **static**
no mgcp rtp payload-type {**clear-channel** | **g726r16** | **g726r24**}

Syntax Description

cisco-codec-fax-ack	Payload type for Cisco codec fax acknowledgment.
cisco-codec-fax-ind	Payload type for Cisco codec fax indication.
cisco -pcm-switch-over-alaw 127	Payload type for upspeed to the G.711 a-law codec.
cisco -pcm-switch-over-ulaw 126	Payload type for upspeed to the G.711 mu-law codec.
nse	Payload type for named signaling events (NSE).
nte	Payload type for named telephony events (NTE).
number	Indicates the payload-type value. The valid range for NSE and NTE payload is from 96 to127. Default for NSE is 100. Default for NTE is 99.
clear -channel	Payload type for clear channel codec.
g726r16	Payload type for the G.726 codec at a bit rate of 16 kbps.
g726r24	Payload type for the G.726 codec at a bit rate of 24 kbps.
static	Static payload type.

Command Default

Fax and modem codecs: static RTP payload type Voice codecs: dynamic RTP payload range from 96 to 127 (default for NSE is 100; default for NTE is 99)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced on the following platforms: Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5400HPX, and Cisco AS5850.
12.4(6)T	The **nse** and **nte**named signalling and telephony events keywords were added.
12.4(15)T5	The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords were added.
12.4(18a)	The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords were added.
12.4(13f)	The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords were added.

Usage Guidelines

Cisco IOS Release 12.2(11)T introduced an RTP payload type negotiation for MGCP VoIP calls different from previous Cisco IOS images. To ensure interoperability between gateways using different Cisco IOS images, follow these guidelines:

- For fax and modem codecs--If either the originating or terminating MGCP gateway is running Cisco IOS Release 12.2(11)T or a later release and the other gateway is running a release earlier than Cisco IOS Release 12.2(11)T, use the **mgcp rtp payload-type** command on the gateway with the later release.
- For voice codecs--If you are using a Clear Channel, G.726R16, or G.726R24 codec, and either the originating or terminating MGCP gateway is running Cisco IOS Release 12.2(11)T or a later release and the other gateway is running a release earlier than Cisco IOS Release 12.2(11)T, use the **mgcp rtp payload-type**command on the gateway with the later release.

If both the originating and terminating gateways are using Cisco IOS Release 12.2(11)T or a later release, this command is not required.

The **cisco-codec-fax-ack**and **cisco-codec-fax-ind**keywords are used to change the default dynamic payload type for the Cisco fax relay feature to a different dynamic payload type.

Note NSE and NTE cannot be configured to use the same value. An error message will be generated by the command parser if the same value is entered.

Examples

The following example specifies use of dynamic RTP payload type for fax and modem calls for mu-law pulse code modulation (PCM) calls in an MGCP network in which the other gateway is running a release of Cisco IOS software that is earlier than Release 12.2(11)T:

```
Router# mgcp rtp payload-type cisco-pcm-switch-over-ulaw 126
```

The following example specifies use of a static RTP payload type for a G.726R16 codec in an MGCP network in which the other gateway is running a release of Cisco IOS software that is earlier than Release 12.2(11)T:

```
Router# mgcp rtp payload-type g726r16 static
```

The following examples configure the gateway to use RTP payload 104 for NSE events and payload 108 for NTE events. These payload types are used when the gateway is advertising capabilities via

the Session Definition Protocol (SDP). If the gateway is recieving the SDP, the payload types configured in the remote SDP will be used instead.

```
Router# mgcp rtp payload-type nse 104

Router# mgcp rtp payload-type nte 108
```

Related Commands

Command	Description
mgcp codec	Selects the default codec type and its optional packetization period value.

mgcp rtp unreachable timeout

To enable detection of an unreachable remote VoIP endpoint, use the **mgcp rtp unreachable timeout**command in global configuration mode. To disable detection, use the **no**form of this command.

mgcp rtp unreachable timeout *timer-value*
no mgcp rtp unreachable timeout

Syntax Description

timer -value	Time, in milliseconds, that the system waits for voice packets from the unreachable endpoint. Range is 500 to 10000.

Command Default

Detection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines



Note This command replaces the previously hidden **mgcp rtp icmp timeout** command .

Thiscommand is useful for preventing calls from remaining open when the remote endpoint is no longer available.

For example, suppose an IP phone makes a call through a gateway to another IP phone. During the call, the call agent goes down and the remote IP phone hangs up. Normally, the call agent would tell the gateway to tear down the call. In this case, the gateway continues to treat the call as active and sends more voice packets to the remote IP phone. The remote IP phone returns Internet Control Message Protocol (ICMP) port unreachable messages to the gateway. If the **mgcp rtp unreachable timeout** command is enabled, the gateway tears down the call. If the command is disabled, the call is left open.

The *timer-value* argument tells the gateway how long to wait before tearing down the call. After receiving the ICMP the unreachable message, the gateway starts a timer. If the gateway does not receive any voice packets by the end of the timer-value period, the gateway tears down the call. If some voice packets arrive before the end of the timer-value period, the gateway resets the timer and leaves the call in active state.

Examples

The following example sets the Real-Time Transport Protocol (RTP) unreachable timer to 1500 ms:

```
Router(config)# mgcp rtp unreachable timeout 1500
```

Related Commands

Command	Description
mgcp	Initiates the MGCP daemon.
mgcp timer	Configures RTP stream host detection.

mgcp rtrcac

To enable Media Control Gateway Protocol (MGCP) Service Assurance (SA) Agent Call Admission Control (CAC) on an MGCP gateway supporting VoIP, use the **mgcp rtrcac** command in global configuration mode. To disable SA Agent checking on the gateway, use the **no** form of this command.

mgcp rtrcac
no mgcp rtrcac

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use thiscommandto initiate or disable MGCP SA Agent CAC on the MGCP gateway.

Examples

The following example enables MGCP SA Agent CAC:

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

Related Commands

Command	Description
call fallback active	Enables a call request to fall back to alternate dial peers in case of network congestion.
mgcp	Starts and allocates resources for the MGCP daemon.
rtr responder	Enables the SA Agent Responder feature.

mgcp sched-time

To configure the scheduled timer value for Media Gateway Control Protocol (MGCP), use the **mgcp sched-time** command in global configuration mode. To disable the configuration, use the **no** form of this command.

mgcp sched-time *milliseconds*
no mgcp sched-time

Syntax Description

milliseconds	Schedule timer value, in milliseconds (ms). The range is from 12 to 40.

Command Default

The scheduled timer value for MGCP is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **mgcp sched-time** command is used to configure the MGCP process a specified time to run before it yields to a process of a lower or the same priority. The schedule timer value must be from 12 to 40 ms, the minimum and maximum time, respectively, a process can run. This ensures that the MGCP process is not suspending too often.

Examples

The following example shows how to configure the scheduled timer value for MGCP:

```
Router# configure terminal
Router(config)# mgcp sched-time 15
```

Related Commands

Command	Description
show mgcp	Displays values for MGCP parameters.

mgcp sdp

To specify parameters for Session Definition Protocol (SDP) operation in Media Gateway Control Protocol (MGCP), use the **mgcp sdp**command inglobal configuration mode. To disable the parameters, use the **no** form of this command.

mgcp sdp {**notation undotted** | **simple** | **xpc-codec**}
no mgcp sdp {**notation undotted** | **simple** | **xpc-codec**}

Syntax Description

notation undotted	Enables undotted SDP notation for the codec string in SDP.
simple	Enables simple mode of SDP operation for MGCP.
xpc -codec	Enables initial generation of the X-pc-codec field, which is used during codec negotiation in SDP for Network-based Call Signaling (NCS) and Trunking Gateway Control Protocol (TGCP).

Command Default

notation undotted: disabled**simple:**disabled**xpc-codec:**disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XA	The **notation undotted** and **xpc-codec** keywords were added.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.

Usage Guidelines

This command allows you to configure SDP fields to meet the requirements of your call agent.

The **notation undotted**keyword is for the G.726-16 and G.729 codecs. The codec strings G.726-16 and G.729 are dotted notation. The codec notation format is selected dynamically in the following order of preference:

1. The notation used in SDP for MGCP packets from the call agent.
2. The notation used in the a: parameter of the Local connection option for MGCP packets from the call agent.
3. The notation set by the **mgcp sdp notation undotted** command.

The **simple** keyword**, w**hen enabled, causes the gateway not to generate the following SDP fields: o (origin and session identifier), s (session name), and t (session start time and stop time). Certain call agents require this modified SDP to send data through the network.

The **xpc-codec** keyword, in TGCP and NCS, defines a new field (X-pc-codec) in the SDP for codec negotiation. To be backward compatible with nonpacket-cable SDPs, the initial generation of the X-pc-codec field is

suppressed by default. However, if a received SDP contains this field, the X-pc-codec field is read and generated in response to continue with the codec negotiation.

Examples

The following example configures simple mode for SDP:

```
Router(config)# mgcp sdp simple
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp sgcp disconnect notify

To enable enhanced endpoint synchronization after a disconnected procedure in a Simple Gateway Control Protocol (SGCP) version 1.5 network, use the **mgcp sgcp disconnect notify** command in global configuration mode. To disable this feature, use the **no** form of this command.

mgcp sgcp disconnect notify
no mgcp sgcp disconnect notify

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is used with SGCP version 1.5 to provide enhanced messaging capability for an endpoint that undergoes the disconnected procedure. It does not apply to gateways that run Media Control Gateway Protocol (MGCP) or other versions of SGCP.

An SGCP endpoint may lose communication with its call agent because the call agent is temporarily off line or because of faults in the network. When a gateway recognizes that an endpoint has lost its communication with the call agent (has become disconnected), it attempts to restore contact. If contact is not established before the disconnected timer expires, the disconnected procedure is initiated.

The disconnected procedure consists of the endpoint sending a Restart In Progress (RSIP) message to the call agent, stating that the endpoint was disconnected and is now trying to reestablish connectivity. If the **mgcp sgcp disconnect notify** command has been configured on the gateway, a special disconnected RSIP message is sent. When contact is reestablished, the call agent may decide to audit the endpoint using an Audit Endpoint (AUEP) command with additional I, ES, and RM parameters, which are defined as follows:

- I--List of connection identifiers for current connections on the endpoint
- ES--Event state of the endpoint (off-hook or on-hook)
- RM--Restart method reason for the last RSIP (graceful, forced, restart, or disconnected)

Endpoint synchronization with the call agent is achieved by the exchange of the disconnected RSIP message and the endpoint audit.

Examples

The following example enables disconnected RSIP messaging between SGCP endpoints and a call agent:

```
Router(config)# mgcp sgcp disconnect notify
```

Related Commands

Command	Description
mgcp sgcp restart notify	Enables the MGCP application to process SGCP-type RSIP messages.
show mgcp	Displays information for MGCP and SGCP parameters.

mgcp sgcp restart notify

To trigger the Media Gateway Control Protocol (MGCP) application to process Simple Gateway Control Protocol (SGCP)-type restart in progress (RSIP) messages, use the **mgcp sgcp restart notify**command in global configuration mode. To cancel the trigger, use the **no**form of this command.

mgcp sgcp restart notify
no mgcp sgcp restart notify

Syntax Description

This command has no arguments or keywords.

Command Default

SGCP does not send any RSIP messages when the protocol type is configured as SGCP.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 3600 series.
12.1(5)XM	This command was modified for MGCP and implemented on the Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command is used to send RSIP messages from the router to the SGCP call agent. The RSIP messages are used to indicate whether the T1 controller is up or down so that the call agent can synchronize with the router. RSIP messages are also sent when the **mgcp** command is entered, enabling the MGCP daemon.

Examples

The following example specifies that the system sends an RSIP notification to the SGCP call agent when the T1 controller state changes:

```
Router(config)# mgcp sgcp restart notify
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp src-cac

To enable System Resource Check (SRC) Call Admission Control (CAC) on a Media Gateway Control Protocol (MGCP) gateway supporting VoIP, use the **mgcp src-cac** command in global configuration mode. To disable system resource checking on the gateway, use the **no** form of this command.

mgcp src-cac
no mgcp src-cac

Syntax Description

This command has no arguments or keywords.

Command Default

System resource checking is disabled.

Command Modes

Global configuration

Command History

Releases	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

When this command is entered, all system-resource checks of CPU utilization, memory utilization, and maximum number of calls are performed for every call setup or modification request received from the call agent.

Examples

The following example enables MGCP VoIP SRC CAC:

```
Router(config)# mgcp src-cac
```

Related Commands

Command	Description
call threshold global	Sets threshold values for SRC CAC parameters.
mgcp	Starts and allocates resources for the MGCP daemon.

mgcp timer

To configure how a gateway detects the Real-Time Transport Protocol (RTP) stream host, use the **mgcp timer** command in global configuration mode. To reset to the defaults, use the **no** form of this command.

mgcp timer {**receive-rtcp** *timer* | **net-cont-test** *timer* | **nse-response t38** *timer* | **toh-time** *timer*}
no mgcp timer {**receive-rtcp** | **net-cont-test** | **toh-time**}

Syntax Description

receive -rtcp *timer*	Multiples of the RTCP report transmission interval, in milliseconds. Range is 1 to 100. Default is 5.
net -cont-test *timer*	Continuity-test timeout interval for VoIP and VoATM adaptation layer 2 (VoAAL2) calls, in milliseconds. Range is from 100 to 3000. The default is 200. **Note** This keyword was previously called **rtp-nse**.
nse -response t38 *timer*	Timeout period, in milliseconds, for awaiting T.38 named signaling event (NSE) responses from a peer gateway. Range is from 100 to 3000. The default is 200.
toh-time *timer*	Tone on hold in milliseconds, for specifying the duration of silence between 3 beep groupings. Range is from 1 to 65500. The default is 10.

Command Default

receive-rtcp *timer* : 5 ms**net-cont-test** *timer*: 200 ms **nse-response t38** *timer*: 200 ms **toh-time** *timer*: 10 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced for Simple Gateway Control Protocol (SGCP) on the Cisco AS5300.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620).
12.1(5)XM	This command was modified to support Media Gateway Control Protocol (MGCP). The **rtp-nse** keyword was changed to the **net-cont-test**keywordwithout change of functionality.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200.
12.2(2)XB	This command was modified. The **nse-response t38** option was added to support MGCP T.38.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5400, and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 1751 and Cisco 1760.

Release	Modification
12.3(10)T	This command was modified. The **toh-time** keyword was added to adjust the duration of silence between the 3 beep groupings used for tone on hold.

Usage Guidelines

Use this command to specify the RTP Control Protocol (RTCP) transmission interval for VoIP calls and the continuity-test timeout interval for VoIP and VoATM adaptation layer 2 (VoAAL2) calls.

The **receive-rtcp**keyword is the timer used by a gateway to disconnect a VoIP call when IP connectivity is lost with the remote gateway. After receiving each RTP or RTCP packet from the remote gateway, the receiving gateway starts a timer. The period of the timer is determined by multiplying the value configured using the **mgcp timer receive-rtcp**command with the value configured using **ip rtcp report interval** command. If the timer expires before the next packet is received from the remote gateway, the receiving gateway disconnects the call and notifies the call agent.

The net -cont-test keyword uses the terminating gateway to verify the network connectivity with the originating gateway before ringing the called party. To do this, the terminating gateway sends a command packet to the originating gateway and starts a timed for the *timer*period. If the timer expires before any acknowledgement from the originating gateway is received, the terminating gateway does not ring the called party, but instead disconnects the call and alerts the call agent.

The **nse-response t38**option sets the timer for awaiting T.38 NSE responses. This timer is configured to tell the terminating gateway how long to wait for an NSE from a peer gateway. The NSE from the peer gateway can either acknowledge the switch and its readiness to accept packets or indicate that it cannot accept T.38 packets.

The **toh-time** *timer* option sets the duration of silence between the 3 beep groupings used for tone on hold.

Examples

The following example sets the multiplication factor to 10 (or x*10, where x is the interval that is set with the ip rtcp report interval command):

```
Router(config)# mgcp timer receive-rtcp 10
```

The following example sets the net-cont-test timer to 1500 ms (1.5 seconds):

```
Router(config)#
mgcp timer net-cont-test 1500
```

The following example enables MGCP fax relay and sets the gateway wait time to 300 ms for an NSE from a peer gateway:

```
Router(config)# mgcp timer nse-response t38 300
```

The following example enables tone on hold timer and set the duration of silence between the 3 beep groupings to 200 ms:

```
Router(config)# mgcp timer toh-time 200
```

Related Commands

Command	Description
ip rtcp report interval	Configures the minimum interval for RTCP report transmissions.
mgcp	Starts the MGCP daemon.

Command	Description
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.
mgcp tse payload	Sets the TSE payload for fax and modem calls.

mgcp tse payload

Note This command is no longer supported. It has been replaced by the **mgcp rtp payload-type** command.

To enable inband telephony signaling events (TSEs) and specify the payload value to be used during fax and modem pass-through and network continuity tests, use the **mgcp tse payload** command in global configuration mode. To disable these signaling events, use the **no**form of this command.

mgcp tse payload *value*
no mgcp tse payload

Syntax Description

value	TSE payload value. Range is from 98 to 119. The default is 100.

Command Default

100

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced for Simple Gateway Control Protocol (SGCP) on the Cisco MC3810 and on the Cisco 3600 series (except the Cisco 3620).
12.1(5)XM	This command was modified to support 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 router.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3620, and Cisco AS5300.
12.4(3rd)T	This command was replaced by the **mgcp rtp payload-type** command.

Usage Guidelines

Because this command is disabled by default, you must specify a TSE payload value. Both gateways must have the same payload value.

If you configure the **mgcp modem passthrough mode**command using the **nse** keyword, you must configure this command.

Examples

The following example sets NSE mode for VoIP modem pass-through and sets the TSE payload:

```
Router(config)# mgcp modem passthrough voip mode nse
Router(config)# mgcp tse payload 100
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
mgcp modem passthrough mode	Sets the method for changing speeds for modem and fax transmissions on the gateway.

mgcp vad

To enable voice activity detection (VAD) silence suppression for Media Gateway Control Protocol (MGCP), use the **mgcp vad** command in global configuration mode. To disable VAD silence suppression, use the **no** form of this command.

mgcp vad
no mgcp vad

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to tell the MGCP gateway to turn VAD silence suppression on or off.

If VAD silence suppression is turned on, silence is not sent over the network, only audible speech. Sound quality is slightly degraded but the connection monopolizes much less bandwidth.

Examples

The following example turns VAD silence suppression on:

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

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.

mgcp validate call-agent source-ipaddr

To enable the Media Gateway Control Protocol (MGCP) application to validate that packets are received from a configured call agent, use the mgcp validate **call-agent**source-ipaddr command in global configuration mode. To disable the validation feature, use the **no** form of this command.

mgcp validate call-agent source-ipaddr
no mgcp validate call-agent source-ipaddr

Syntax Description

This command has no arguments or keywords.

Command Default

No validation occurs.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

This command verifies that incoming packets are received from MGCP or Cisco CallManager configured call agents only. When the command is enabled, all MGCP messages received from call agents that are not configured in MGCP or Cisco CallManager are dropped. Use the mgcp validate call-agent source-ipaddr command in place of access lists to filter out packets from unconfigured call agents. Use the **mgcp bind control source-interface** *interface*command to restrict the MGCP application from responding to unconfigured call agent requests on nonsecure interfaces. Use the **ccm-manager config server** *server address* command to configure the Cisco CallManager address to be used when verifying incoming packets.

Examples

The following example shows that MGCP call-agent validation is enabled:

```
Router(config)# mgcp validate call-agent source-ipaddr
```

Related Commands

Command	Description
ccm-manager config server	Configures the Cisco CallManager address used in verifying incoming packets.
mgcp bind control source-interface	Restricts the MGCP application from responding to unconfigured call agent requests on nonsecure interfaces.
mgcp call-agent	Configures the IP address for the primary or default Cisco CallManager server and designates the optional destination UDP port number for the specified Cisco CallManager server.
show mgcp srtp	Displays active MGCP SRTP calls.

mgcp validate domain-name

To enable validation of a hostname and domain (or a specific IP address) received as part of the endpoint name in MGCP messages against those configured on the gateway, use the **mgcp validate domain-name** command in global configuration mode. To disable Media Gateway Control Protocol (MGCP) endpoint validation, use the **no** form of this command.

mgcp validate domain-name
no mgcp validate domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

Hostname and domain (or IP address) validation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(17)	The default state of this command was changed to disabled.
12.3(11)T8; 12.3(14)T5	The default state of this command was changed to disabled.
12.4(1c); 12.4(3b); 12.4(5)	The default state of this command was changed to disabled.
12.4(2)T2; 12.4(4)T1; 12.4(6)T	The default state of this command was changed to disabled.

Usage Guidelines

The **mgcp validate domain-name** command enables validation of a hostname and domain (or specific IP address) received as part of the endpoint name sent from the call agent (CA) or Cisco CallManager against those configured on the gateway. If the hostname or domain (or IP address) is not valid, the system returns a 500 error with appropriate comment.

Use the **mgcp validate domain-name** command before configuring MGCP globally in a VoIP network. (See the Cisco Unified CallManager and Cisco IOS Interoperability Guide for global MGCP configuration information.)



Note Only MGCP messages received from the CA or Cisco CallManager are validated .

You can display the current setting for MGCP domain name validation using the **show running-config** command. To show only MGCP information, limit the display output to the section on MGCP (see the "Examples" section).

Note When MGCP domain name validation is disabled, the output of the **show running-config** command does not include this command--it displays only when domain name validation is enabled. However, if your system is running a software image released before the default for this feature was changed, MGCP domain name validation is turned on by default and will appear in the **show running-config** command output only if validation is disabled.

Once you enable the MGCP validate domain name feature, you should verify that the appropriate endpoint name is included as part of incoming MGCP messages. Performing this verification helps to ensure that incoming messages with invalid hostnames, domain names, and IP addresses are rejected while valid incoming messages are still allowed to reach their target endpoint (host). Enabling this validation feature without verifying this information can cause all incoming messages, even those using valid names or addresses, to be rejected (see the "Examples" section).

Examples

The following examples show how to enable MGCP domain name validation, how to verify that validation is enabled in the running configuration, and how to verify and match the hostname, domain name, or IP address specified in incoming MGCP messages to the gateway configuration.

Use the following command to enable MGCP domain name validation:

```
Router(config)# mgcp validate domain-name
```

Use the following command to verify that MGCP domain name validation is enabled:

```
Router(config)# show running-config | section mgcp
```

or

```
Router(config)# show running-config | include mgcp validate
mgcp validate domain-name
Router(config)#
```

Use the following commands and processes to verify that hostname and domain name are configured so that all and only valid incoming messages are accepted by the gateway.

After enabling domain name validation, enable debug tracing for MGCP packets:

```
Router# debug mgcp packets
Media Gateway Control Protocol packets debugging for all endpoints is on
Router#
```

Generate a call to the gateway from a CA or Cisco CallManager. That call will generate debug messages on the gateway so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco CallManager):

```
Router#
*Mar 14 02:29:11.512: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@Router2821.example.com MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 02:29:11.512: MGCP Packet sent to 192.0.2.135:2427--->
500 3 Endpoint name contains an invalid host or domain
<---
```

Because the hostname in the incoming message (aaln/S2/SU0/0@Router2821.example.com) does not match the hostname of the gateway (Router), the message was rejected (replied to with a NACK). To resolve this, change the hostname of the gateway:

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname Router2821
Router2821(config)# end
Router2821#
```

Generate another call to the gateway from the CA or Cisco CallManager. That call will generate more debug messages so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco CallManager):

```
*Mar 14 03:01:12.480: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@Router2821.example.com MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 03:01:12.480: MGCP Packet sent to 192.0.2.135:2427--->
200 3 OK
<---
```

The validation is successful and an ACK (positive response) is sent back to the CA or Cisco CallManager because the hostname now matches. This same process also applies to validation for the domain name. Use the following commands to set the domain name for the gateway and to view current configuration for domain name and hostname:

```
Router2821# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2821(config)# ip domain-name example.com
Router2821(config)# end
Router2821# show running-config
Building configuration...
.
.
.
hostname Router2821
.
.
.
ip domain name example.com
.
.
.
.
Router2821#
```

Use the following commands and processes to verify that the IP address for the gateway is configured so that all and only valid incoming messages are accepted by the gateway:

```
Router2821# show ip interface brief
Interface                  IP-Address       OK?    Method    Status    Protocol
GigabitEthernet0/0         192.0.2.189    YES    NVRAM     up        up
Router2821#
```

Generate a call to the gateway from the CA or Cisco CallManager. That call will generate debug messages so that you can view the endpoint information included in the incoming MGCP message and the response from the gateway to the CA (or Cisco CallManager). If the MGCP message is

directed to a specific IP address instead of a domain or hostname, you will see debug messages similar to the following:

```
*Mar 14 03:16:52.356: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@[192.0.2.190] MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 03:16:52.356: MGCP Packet sent to 192.0.2.135:2427--->
500 3 Endpoint name contains an invalid host or domain
<---
```

Because the IP address specified in the incoming message (aaln/S2/SU0/0@192.0.2.190) does not match the IP address of the GigE 0/0 interface (192.0.2.189), the message was rejected (replied to with a NACK). To resolve this, change the IP address specified by the CA or Cisco CallManager for this gateway and generate another call to this gateway. If the IP addresses match, you will see debug messages similar to the following:

```
*Mar 14 03:16:10.360: MGCP Packet received from 192.0.2.135:2427--->
RQNT 3 aaln/S2/SU0/0@[192.0.2.189] MGCP 0.1
R: L/hd(N)
X:1
<---
*Mar 14 03:16:10.364: MGCP Packet sent to 192.0.2.135:2427--->
200 3 OK
<---
```

Because the IP address now specified in the incoming MGCP message matches the IP address of the gateway, the message was accepted and replied to with an ACK (positive response).

Related Commands

Command	Description
mgcp call-agent	Configures the IP address for the primary or default Cisco CallManager server and designates the optional destination UDP port number for the specified Cisco CallManager server.
show ccm-manager	Displays a list of Cisco CallManager servers and their current status and availability.

mgcp voice-quality-stats

To enable voice-quality statistics reporting for the Media Gateway Control Protocol (MGCP), use the **mgcp voice-quality-stats** command in global configuration mode. To turn off voice-quality statistics reporting, use the no form of this command.

mgcp voice-quality-stats [**priority** *variable* | **all**]
no mgcp voice-quality-stats [**priority** *variable* | **all**]

Syntax Description

priority <*value*>	Selects numeric parameters 1 or 2 to indicate priority.
all	Selects all VQ parameters.

Command Default

Voice-quality statistics reporting is turned off.

Command Modes

Global configuration

Command History

Release	Modification
12.3(3)	This command was introduced.
12.4(4)T	**The priority** and **all** keywords were introduced.

Usage Guidelines

- The request for digital signal processor (DSP) statistics is controlled by the RTP Control Protocol (RTCP) statistics polling interval. The polling interval is configurable by entering the **ip rtcp report interval** command. Statistics are polled every 5 seconds by default.



Note The Cisco PGW 2200 must have a patch the supports DSP statistics in order to collect data in the call detail records (CDRs).

- This command does not generate any output on the console; it adds additional quality statistics parameters in the MGCP Delete Connection (DLCX) ACK message that is sent to the call agent.

Cisco IOS Release 12.4(4)T supports only priority levels 1 and 2.

- The keyword **priority** uses a value of 1 or 2 to indicate the priority of the parameters.



Note Choosing priority 2 is similar to using the keyword **all** where all the paramters are selected.

The corresponding set of VQ parameters are sent in the MGCP DLCX message based on the priority selected.

Examples

The following example enables voice-quality statistics reporting for MGCP:

```
Router> enable
Router# configure terminal
Router(config)# mgcp voice-quality-stats
Router(config)# end
```

The following example shows the VQ parameters selected for priority 1:

```
mgcp voice-quality-stats priority 1
16:38:20.461771 10.0.5.130:2427 10.0.5.133:2427 MGCP..... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/IN: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0,
DSP/CR: CR=0, MN=0, CT=0, TT=0,
DSP/DC: DC=0,
DSP/CS: CS=0, SC=0, TS=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0
```

The following example shows all the VQ parameters selected for the keyword **all**:

```
mgcp voice-quality-stats all

16:38:20.461771 10.0.5.130:2427 10.0.5.133:2427 MGCP..... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/PE: PC=0, IC=0, SC=0, RM=0, BO=0, EE=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/ER: RD=0, TD=0, RC=0, TC=0
DSP/IC: IC=0
DSP/EC: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0, JX=0,
DSP/KF: KF=0, AV=0, MI=0, BS=0, NB=0, FL=0,
DSP/CS: CR=0, AV=0, MN=0, MX=0, CS=0, SC=0, TS=0, DC=0,
DSP/RF: ML=0, MC=0, R1=0, R2=0, IF=0, ID=0, IE=0, BL=0, R0=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0,
DSP/DL: RT=0, ED=0
```

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, parser, and CAC.
ip rtcp report interval	Configures the RTCP statistics polling interval.

microcode reload controller

To reload the firmware and field programmable gate array (FPGA) without reloading the Cisco IOS image, use the **microcode reload controller** command in privileged EXEC mode.

microcode reload controller {**t1** | **e1** | **j1**} *x/y*

Syntax Description

t1	T1
e1	E1
j1	J1 controller.
x / *y*	Controller slot and unit numbers. The slash must be typed.

Command Default

No microcode reload activity is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)XH	This command was introduced 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.
12.2(8)T	The **j1** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Loopbacks in the running configuration are restored after this command is entered. If the controller is in a looped state before this command is issued, the looped condition is dropped. You have to reinitiate the loopbacks from the remote end by entering the **no loop**command from the controller configuration.

Examples

The following example shows how to start the microcode reload activity:

```
Router# microcode reload controller j1 3/0
TDM-connections and network traffic will be briefly disrupted.
Proceed with reload microcode?[confirm]
Router#
*Mar  3 209.165.200.225: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.226: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.227: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state to)
*Mar  3 209.165.200.227: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.228: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state top
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
```

midcall-signaling

To configure the method that is used for signaling messages, use the **midcall-signaling** command in SIP configuration mode, or voice class tenant configuration mode, or dial peer configuration mode. To disable the mid-call signaling feature, use the **no** form of this command.

midcall-signaling {**passthru media-change** | **block** | **preserve-codec**} **[system]**
no midcall-signaling

Syntax Description

passthru media-change	Passes SIP messages that involve media-change from one IP leg to another IP leg.
block	Blocks all SIP messages during mid-call.
preserve-codec	Preserves codec that is negotiated during call initialization. Mid-call codec change is disabled.
system	Specifies that the mid-call signaling feature uses the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Midcall-signaling is disabled. Codec negotiation in the middle of a call is enabled.

Command Modes

SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T. The **media-change** and **block** keywords were added.
15.3(2)S, 15.3(1)T	This command was modified. The **preserve-codec** keyword was added.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

The **midcall-signaling** command distinguishes between the way Cisco Unified Communications Express and Cisco Unified Border Element handle signaling messages. Most SIP-to-SIP video and SIP-to-SIP reinvite based supplementary services require the **midcall-signaling** command to be configured before configuring other supplementary services. Supplementary service features that are functional without configuring **midcall-signaling** include: session refresh, fax, and refer-based supplementary services. The **midcall-signaling** command is for SIP-to-SIP calls only. All other calls (H323-to-SIP, and H323-to-H323) do not require the

midcall-signaling command be configured. The **allow-connections sip-to-sip** command must be configured before the **midcall-signaling** command.

Configuring the Session Refresh with Reinvites feature on a dial-peer basis is not supported.

Examples

The following example shows SIP messages that are configured to passthrough from one IP leg to another IP leg:

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling passthru
```

The following example shows SIP messages that are configured to media passthru from one IP leg to another IP leg:

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling passthru media-change
```

The following example shows how to block SIP messages.

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling block
```

The following example shows how to disable codec negotiation in the middle of a call and retains the codec that is negotiated at the start of the call.

```
Router(config)#voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# midcall-signaling preserve-codec
```

The following example shows SIP messages that are configured to pass thru from one IP leg to another IP leg in the voice class tenant configuration mode:

```
Router(config-class)# midcall-signaling passthru system
```

Related Commands

Command	Description
allow-connections	Allows connections between specific types of endpoints in a Cisco Unified BE.

min-se (SIP)

To change the minimum session expiration (Min-SE) header value for all calls that use the Session Initiation Protocol (SIP) session timer, use the **min-se**command in SIP configuration mode. To reset to the default, use the **no** form of this command.

min-se *time* **session-expires** *interval*
no min-se

Syntax Description

time	Length of time, in seconds. Range: 90–86400 (1 day). Default: 1800.
session-expires *interval*	Indicates that the session expires time interval. Range is 90–86400. Default: 1800.

Command Default

1800 seconds (30 minutes)

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(9)T	This command was modified. The default time was changed 90–1800 seconds.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)T	This command was modified. The **session-expires**keyword was added.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

A proxy, user-agent client, and user-agent server can all have a configured minimum value indicating the smallest session interval that they accept. If they all happen to have a different configured minimum value, the highest minimum value is used. This command sets the minimum timer that is conveyed in the Min-SE header in the initial INVITE request.

The recommended value for this command is 1800 seconds (30 minutes), which is the default value. The value cannot be set below 90 seconds because excessive INVITEs create problems for routers. Once set, the value affects all calls that are originated by the router.

If you do not configure the session expires interval and configure only the min-se value, then the session expires interval takes the value that is configured for the min-se.

Examples

The following example sets the expiration timer to 90 seconds:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# min-se 90 session-expires 1800
```

Related Commands

Command	Description
show sip -ua min-se	Shows the current value of the Min-SE header.

mmoip aaa global-password

To define a password to be used with CiscoSecure for Microsoft Windows NT when using store and forward fax, use the **mmoip aaa global-password**command in global configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa global-password *password*
no mmoip aaa global-password *password*

Syntax Description

password	Password for CiscoSecure for Windows NT to be used with store and forward fax. The maximum length is 64 alphanumeric characters.

Command Default

No password is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

CiscoSecure for Windows NT might require a separate password in order to complete authentication, no matter what security protocol you use. This command defines the password to be used with CiscoSecure for Windows NT. All records on the Microsoft Windows NT server use this defined password.

This command applies to on-ramp store and forward fax functions when using a modem card. It is not used with voice feature cards.

Examples

The following example specifies a password (password) when CiscoSecure for Microsoft Windows NT is used with store and forward fax:

```
mmoip aaa global-password password
```

mmoip aaa method fax accounting

To define the name of the method list to be used for authentication, authorization, and accounting (AAA) accounting with store-and-forward fax, use the **mmoip aaa method fax accounting**command in global configuration mode. To reset to the undefined state, use the **no** form of this command.

mmoip aaa method fax accounting *method-list-name*
no mmoip aaa method fax accounting *method-list-name*

Syntax Description

method -list-name	List of accounting methods to be used with store-and-forward fax.

Command Default

No AAA accounting method list is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)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 defines the name of the AAA accounting method list to be used with store-and-forward fax. The method list itself, which defines the type of accounting services provided for store-and-forward fax, is defined using the **aaa accounting** command in global configuration mode. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists used in store-and-forward fax are applied globally.

After the accounting method lists have been defined, they are enabled by using the **mmoip aaa receive-accounting enable**command.

This command applies to both on-ramp and off-ramp store-and-forward fax functions when a modem card is used. It is not used with voice feature cards.

Examples

The following example specifies a AAA accounting method list (called "list3") to be used with store-and-forward fax:

```
aaa new-model
mmoip aaa method fax accounting list3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when RADIUS or TACACS+ is used.

Command	Description
mmoip aaa receive-accounting enable	Enables on-ramp store-and-forward fax for AAA accounting services.

mmoip aaa method fax authentication

To define the name of the method list to be used for authentication, authorization, and accounting (AAA) authentication with store and forward fax, use the **mmoip aaa method fax authentication** command inglobal configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa method fax authentication *method-list-name*
no mmoip aaa method fax authentication *method-list-name*

Syntax Description

method -list-name	List of authentication methods to be used with store and forward fax.

Command Default

No AAA authentication method list is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command defines the name of the AAA authentication method list to be used with store and forward fax. The method list itself, which defines the type of authentication services provided for store and forward fax, is defined using the **aaa authentication** global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), AAA authentication method lists used with store and forward fax are applied globally on the Cisco AS5300 universal access server.

After the authentication method lists have been defined, they are enabled by using the **mmoip aaa receive-authentication enable**command.

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

Examples

The following example specifies a AAA authentication method list (called xyz) to be used with store and forward fax:

```
aaa new-model
mmoip aaa method fax authentication xyz
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa receive -authentication enable	Enables on-ramp store and forward fax AAA authentication services.

mmoip aaa receive-accounting enable

To enable on-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa receive-accounting enable**command in global configuration mode. To disable on-ramp AAA services, use the **no** form of this command.

mmoip aaa receive-accounting enable
no mmoip aaa receive-accounting enable

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.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

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

Examples

The following example specifies an AAA method list (called xyz) to be used with inbound store-and-forward fax. In this example, store-and-forward fax is configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa receive-accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

mmoip aaa receive-authentication enable

To enable on-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa receive-authentication enable**command in global configuration mode. To disable on-ramp AAA services, use the **no** form of this command.

mmoip aaa receive-authentication enable
no mmoip aaa receive-authentication enable

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.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an AAA method list has been defined using both the **aaa authentication** command and the **mmoip aaa method fax authentication** command.

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

Examples

The following example specifies an AAA method list (called xyz) to be used with inbound store-and-forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is configured for store-and-forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa receive-authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store-and-forward fax.

mmoip aaa receive-id primary

To specify the primary location from which the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for on-ramp faxing, use the **mmoip aaa receive-id primary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa receive-id primary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}
no mmoip aaa receive-id primary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

ani	AAA uses the calling party telephone number (automatic number identification [ANI]) as the AAA account identifier.
dnis	AAA uses the called party telephone number (dialed number identification service [DNIS]) as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the hostname and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.
redialer -id	AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer -dnis	AAA uses the called party telephone number (dialed number identification service [DNIS]) as the AAA account identifier that is captured by the redialer if a redialer device is present.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)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

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the ANI, DNIS, gateway ID, redialer ID, or redialer DNIS be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for inbound or on-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the secondary identifier using the **mmoip aaa receive-id secondary** command.

AAA does not use these methods sequentially. If the primary identifier is defined and AAA cannot authenticate the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously--for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

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

Examples

The following example defines the DNIS captured by the redialer as the primary AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa receive-id primary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive -id secondary	Specifies the secondary location from which AAA retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined.

mmoip aaa receive-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined, use the **mmoip aaa receive-id secondary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa receive-id secondary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}
no mmoip aaa receive-id secondary {**ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}

Syntax Description

ani	AAA uses the calling party telephone number (automatic number identification or ANI) as the AAA account identifier.
dnis	AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.
redialer -id	AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer -dnis	AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier that is captured by the redialer if a redialer device is present.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was introduced on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the ANI, DNIS, gateway ID, redialer DNIS, or redialer ID be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for inbound or on-ramp user authentication with store-and-forward fax if the primary identifier has not been defined.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the primary identifier using the **mmoip aaa receive-id primary** command.

AAA does not use these methods sequentially--meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

Defining only the secondary identifier enables you to service two different scenarios simultaneously--for example, if you are offering fax services to two different companies, one of which uses redialers and the other does not. In this case, configure the **mmoip aaa receive-id primary** command to use the redialer DNIS, and configure the **mmoip aaa receive-id secondary** command to use ANI. With this configuration, when a user dials in and the redialer DNIS is not null, the redialer DNIS is used as the authentication identifier. If a user dials in and the redialer DNIS is null, ANI is used as the authentication identifier.

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

Examples

The following example defines the DNIS captured by the redialer as the secondary AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa receive-id secondary redialer-dnis
```

Related Commands

Command	Description
mmoip aaa receive -id primary	Specifies the primary location where AAA retrieves its account identification information for on-ramp faxing.

mmoip aaa send-accounting enable

To enable off-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa send-accounting enable**command in global configuration mode. To reset to the default, use the **no** form of this command.

mmoip aaa send-accounting enable
no mmoip aaa send-accounting enable

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.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an AAA method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.

This command applies to off-ramp store-and-forward fax functions when using a modem card. It is not used with voice feature cards.

Examples

The following example specifies an AAA method list (called xyz) to be used with outbound store-and-forward fax. In this example, store-and-forward fax is configured to track start and stop connection accounting records.

```
aaa new-model
mmoip aaa method fax accounting xyz
aaa accounting connection sherman stop-only radius
mmoip aaa send-accounting enable
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store-and-forward fax.

mmoip aaa send-authentication enable

To enable off-ramp authentication, authorization, and accounting (AAA) services, use the **mmoip aaa send-authentication enable**command in global configuration mode. To disable off-ramp AAA services, use the **no** form of this command.

mmoip aaa send-authentication enable
no mmoip aaa send-authentication enable

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.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command enables AAA services if an AAA method list has been defined using both the **aaa authentication** command and the **mmoip aaa method fax authentication** command.

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

Examples

The following example specifies an AAA method list (called xyz) to be used with outbound store-and-forward fax. In this example, RADIUS authentication (and if the RADIUS server fails, then local authentication) is configured for store-and-forward fax.

```
aaa new-model
mmoip aaa method fax authentication xyz
aaa authentication login peabody radius local
mmoip aaa send-authentication enable
```

Related Commands

Command	Description
aaa authentication	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
mmoip aaa method fax authentication	Defines the name of the method list to be used for AAA authentication with store-and-forward fax.

mmoip aaa send-id primary

To specify the primary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id primary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa send-id primary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}
no mmoip aaa send-id primary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

Syntax Description

account -id	AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the X-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
envelope -from	AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope -to	AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the primary identifier for outbound or off-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the secondary identifier using the **mmoip aaa send-id secondary** command. AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA uses the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it checks to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially--meaning that if the primary identifier is defined and AAA cannot authenticate the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id primary** command in the X-account ID field of the e-mail header. This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id primary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id primary** command with the **account-id** keyword. This particular keyword enables store-and-forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

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

Examples

The following example specifies the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa send-id primary envelope-to
```

Related Commands

Command	Description
mmoip aaa receive -id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send -id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.

mmoip aaa send-id secondary

To specify the secondary location where the authentication, authorization, and accounting (AAA) protocol retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id secondary** command in global configuration mode. To remove the definition of the account identification source, use the no form of this command.

mmoip aaa send-id secondary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}
no mmoip aaa send-id secondary {**account-id** | **envelope-from** | **envelope-to** | **gateway**}

Syntax Description

account -id	AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the X-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
envelope -from	AAA uses the account username from the fax-mail header as the AAA account identifier.
envelope -to	AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
gateway	AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: *router-name.domain-name*.

Command Default

No account identification source is defined

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XJ	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(4)T	This command was implemented on the Cisco 1750.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With store-and-forward fax, you can specify that the account ID, username, or recipient name from the e-mail header information be used to identify the user for authentication. This command defines what AAA uses for the secondary identifier for outbound or off-ramp user authentication with store-and-forward fax.

Store-and-forward fax allows you to define either a primary or a secondary identifier. You configure the primary identifier using the **mmoip aaa send-id primary** command. AAA extracts the authentication identifier information from the defined sources. If the field is blank (meaning undefined), AAA uses the secondary identifier source if configured. The secondary identifier is used only when the primary identifier is null. In this case, when AAA sees that the primary identifier is null, it checks to see if a secondary identifier has been defined and use that value for user authentication.

AAA does not use these methods sequentially--meaning that if the primary identifier is defined and AAA cannot match the primary identifier information, it does not use the secondary identifier for authentication. Authentication simply fails.

When you enable authentication, the on-ramp gateway inserts whatever value you configure for the **mmoip aaa receive-id secondary** command in the X-account ID field of the e-mail header (if store-and-forward fax uses the defined secondary identifier). This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway. For example, if the **mmoip aaa receive-id secondary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account ID field of the e-mail header of the fax-mail message.

If you want to use this configured gateway value in the X-account ID field, you must configure the **mmoip aaa send-id secondary** command with the **account-id** keyword. This particular keyword enables store-and-forward fax to generate end-to-end authentication and accounting tracking records. If you do not enable authentication on the on-ramp gateway, the X-account ID field is left blank.

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

Examples

The following example specifies the recipient name as defined in the envelope-to field of the e-mail header to be used as the AAA authentication identifier for store-and-forward fax:

```
aaa new-model
mmoip aaa send-id secondary envelope-to
```

Related Commands

Command	Description
mmoip aaa receive -id secondary	Specifies the secondary location where AAA retrieves its account identification information for off-ramp faxing.
mmoip aaa send -id primary	Specifies the primary location where AAA retrieves its account identification information for off-ramp faxing.