

sccp through service-type call-check

- sccp, on page 3
- sccp blf-speed-dial retry-interval, on page 5
- sccp ccm, on page 6
- sccp ccm group, on page 9
- sccp codec mask, on page 11
- sccp ip precedence, on page 13
- sccp local, on page 14
- sccp plar, on page 16
- sccp switchback timeout guard, on page 17
- scenario-cause, on page 18
- sdspfarm tag, on page 20
- sdspfarm transcode sessions, on page 22
- sdspfarm units, on page 23
- secondary, on page 24
- secure-ciphersuite, on page 27
- security, on page 29
- security acl, on page 31
- security izct, on page 32
- security mode, on page 34
- sequence-numbers, on page 36
- server (auto-config application), on page 38
- server (presence), on page 39
- server (RLM), on page 41
- server absent reject, on page 43
- server flow-control, on page 44
- server registration-port, on page 47
- server routing, on page 49
- server trigger arq, on page 50
- server trigger brq, on page 53
- server trigger drq, on page 56
- server trigger irr, on page 59
- server trigger lcf, on page 62
- server trigger lrj, on page 65

- server trigger lrq, on page 68
- server trigger rai, on page 71
- server trigger rrq, on page 74
- server trigger urq, on page 77
- service, on page 80
- service dsapp, on page 82
- service-flow primary upstream, on page 88
- service-map, on page 89
- service-relationship, on page 90
- service-type call-check, on page 91

sccp

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

To enable the Skinny Client Control Protocol (SCCP) protocol and its related applications (transcoding and conferencing), use the **sccp** command in global configuration mode. To disable the protocol, use the **no** form of this command.

sccp
no sccp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

SCCP and its related applications (transcoding and conferencing) become enabled only if digital-signal-processor (DSP) resources for these applications are configured, DSP-farm service is enabled, and the Cisco CallManager registration process is completed.

The **no** form of this command disables SCCP and its applications by unregistering from the active Cisco CallManager, dropping existing connections, and freeing allocated resources.

Examples

The following example sets related values and then enables SCCP:

```
Router(config)# sccp ccm 10.10.10.1 priority 1
Router(config)# sccp local fastEthernet 0/0
Router(config)# sccp switchback timeout guard 180
Router(config)# sccp ip precedence 5
Router(config)# sccp
Router(config)# end
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
show dspfarm	Displays summary information about DSP resources.
show sccp	Displays the SCCP configuration information and current status.

sccp blf-speed-dial retry-interval

To set the retry timeout for Busy Lamp Field (BLF) notification for speed-dial numbers on SCCP phones registered to an external Cisco Unified CME router, use the **sccp blf-speed-dial retry-interval**command in presence configuration mode. To reset to the default, use the **no** form of this command.

sccp blf-speed-dial retry-interval *seconds* **limit** *number*
no sccp blf-speed-dial retry-interval

Syntax Description

seconds	Retry timeout in seconds. Range: 60 to 3600. Default: 60.
limit *number*	Maximum number of retries. Range: 10 to 100. Default: 10.

Command Default

Retry timeout is 60 seconds; retry limit is 10.

Command Modes

Presence configuration (config-presence)

Command History

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

Usage Guidelines

This command specifies how frequently the router attempts to subscribe for the line status of an external directory number when the BLF speed-dial feature is configured on a SCCP phone. This retry mechanism is used when either the presentity does not exist or the router receives a terminated NOTIFY from the external presence server. If the subscribe request toward the external server fails after the configured number of retries, the subscribe request from the phone is rejected.

Examples

The following example shows the BLF speed-dial retry interval set to 100 seconds and the limit to 25:

```
Router(config)# presence
Router(config-presence)# sccp blf-speed-dial retry-interval 100 limit 25
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence global	Displays configuration information about the presence service.

sccp ccm

To add a Cisco Unified Communications Manager server to the list of available servers and set various parameters--including IP address or Domain Name System (DNS) name, port number, and version number--use the **sccp ccm** command in global configuration mode. To remove a particular server from the list, use the **no** form of this command.

NM-HDV or NM-HDV-FARM Voice Network Modules
sccp ccm {*ipv4-addressipv6-addressdns*} **priority** *priority* [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]
no sccp ccm {*ipv4-addressipv6-addressdns*}

NM-HDV2 or NM-HD-1V/2V/2VE Voice Network Modules
sccp ccm {*ipv4-addressipv6-addressdns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]
no sccp ccm {*ipv4-addressipv6-addressdns*}

Syntax Description

ipv4 -address	IPv4 address of the Cisco Unified Communications Manager server.
ipv6-address	IPv6 address of the Cisco Unified Communications Manager server.
dns	DNS name.
identifier *identifier-number*	Specifies the number that identifies the Cisco Unified Communications Manager server. The range is 1 to 65535.
priority *priority*	Specifies the priority of this Cisco Unified Communications Manager server relative to other connected servers. The range is 1 (highest) to 4 (lowest). **Note** This keyword is required only for NM-HDV and NM-HDV-FARM modules. Do not use this keyword if you are using the NM-HDV2 or NM-HD-1V/2V/2VE; set the priority using the **associate ccm** command in the Cisco Unified Communications Manager group.
port *port -number*	(Optional) Specifies the TCP port number. The range is 1025 to 65535. The default is 2000.
version *version -number*	(Optional) Cisco Unified Communications Manager version. Valid versions are **3.0**, **3.1**, **3.2**, **3.3**, **4.0**, **4.1**, **5.0.1**, **6.0**, and **7.0+**. There is no default value.
trustpoint	(Optional) Specifies the trustpoint for Cisco Unified Communications Manager certificate.
label	Cisco Unified Communications Manager trustpoint label.

Command Default

The default port number is 2000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.3(8)T	This command was modified. The **identifier** keyword and additional values for Cisco Unified Communications Manager versions were added.
12.4(11)XW	This command was modified. The **6.0** keyword was added to the list of version values.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. Support for IPv6 was added. The **version** keyword and *version-number*argumentwere changed from being optional to being required, and the **7.0+** keyword was added.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **trustpoint**keyword and the *label* argument were added.

Usage Guidelines

You can configure up to four Cisco Unified Communications Manager servers--a primary and up to three backups--to support digital signal processor (DSP) farm services. To add the Cisco Unified Communications Manager server to a Cisco Unified Communications Manager group, use the **associate ccm** command.

IPv6 support is provided for registration with Cisco Unified CM version 7.0 and later.

To enable Ad Hoc or Meet-Me hardware conferencing in Cisco Unified CME, you must first set the **version** keyword to **4.0** or a later version.

Beginning with Cisco IOS Release 12.4(22)T users manually configuring the **sccp ccm**command must provide the version. Existing router configurations are not impacted because automatic upgrade and downgrade are supported.

Examples

The following example shows how to add the Cisco Unified Communications Manager server with IP address 10.0.0.0 to the list of available servers:

```
Router(config)# sccp ccm 10.0.0.0 identifier 3 port 1025 version 4.0
```

The following example shows how to add the Cisco Unified CallManager server whose IPv6 address is 2001:DB8:C18:1::102:

```
Router(config)# sccp ccm 2001:DB8:C18:1::102 identifier 2 version 7.0
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
sccp ccm group	Creates a Cisco Unified Communications Manager group and enters SCCP Cisco Unified Communications Manager configuration mode.
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified Communications Manager.

Command	Description
show sccp	Displays SCCP configuration information and current status.

sccp ccm group

To create a Cisco Unified Communications Manager group and enter SCCP Cisco CallManager configuration mode, use the **sccp ccm group** command in global configuration mode. To remove a particular Cisco Unified Communications Manager group, use the **no** form of this command.

sccp ccm group *group-number*
no sccp ccm group *group-number*

Syntax Description

group-number	Number that identifies the Cisco Unified Communications Manager group. Range is 1 to 50.

Command Default

No groups are defined, so all servers are configured individually.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. The group number range was increased to 50.

Usage Guidelines

Use this command to group Cisco Unified Communications Manager servers that are defined using the **sccp ccm** command. You can associate designated DSP farm profiles using the **associate profile** command so that the DSP services are controlled by the Cisco Unified Communications Manager servers in the group.

Examples

The following example enters SCCP Cisco CallManager configuration mode and associates Cisco Unified Communications Manager 25 with Cisco Unified Communications Manager group 10:

```
Router(config)#
sccp ccm group 10
Router(config-sccp-ccm)# associate ccm 25 priority 2
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
associate profile	Associates a DSP farm profile with a Cisco Unified Communications Manager group.
bind interface	Binds an interface with a Cisco Unified Communications Manager group.

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager connections fails.
sccp ccm	Adds a Cisco Unified Communications Manager server to the list of available servers.

sccp codec mask

To mask a codec type so that it is not used by Cisco CallManager, use the **sccp codec mask**command in global configuration mode. To unmask a codec, use the **no** form of this command.

sccp codec *codec* **mask**
no sccp codec *codec* **mask**

Syntax Description

codec	Codec to mask. Values are the following: • **g711alaw** • **g711ulaw** • **g729abr8** • **g729ar8** • **g729br8** • **g729r8**

Command Default

No codecs are masked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH4	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4(11)XJ2	The **gsmefr**and **gsmfr**keywords were removed as configurable codec options for all platforms with the exception of the **gsmfr** codec on the Cisco AS5400 and AS5350 with MSAv6 dsps.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command prevents the voice gateway from reporting codec types that are masked so that Cisco CallManager only selects codec types that are supported by the endpoints.

Note You must enable this command before Skinny Client Control Protocol (SCCP) is enabled. If the **sccp codec mask** command is used when SCCP is active, you must disable the SCCP using the **no sccp** command and then re-enable **sccp** for the **sccp codec mask** command to take effect.

Examples

The following example shows how to mask codec type G.711 ulaw and G.729r8:

```
sccp codec g711ulaw mask
sccp codec g729r8 mask
```

Related Commands

Command	Description
sccp	Enables SCCP and related applications.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
sccp local	Selects the local interface that SCCP applications use to register with Cisco CallManager.
show sccp	Displays SCCP configuration information and current status.

sccp ip precedence

To set the IP precedence value to be used by Skinny Client Control Protocol (SCCP), use the **sccp ip precedence** command in global configuration mode. To reset to the default, use the **no** form of this command.

sccp ip precedence *value*
no sccp ip precedence

Syntax Description

value	IP precedence value. Range is from 1 (lowest) to 7 (highest).

Command Default

5

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

Examples

The following example sets IP precedence to the highest possible value:

```
Router# sccp ip precedence 1
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

sccp local

To select the local interface that Skinny Client Control Protocol (SCCP) applications (transcoding and conferencing) use to register with Cisco CallManager, use the **sccp local** command in global configuration mode. To deselect the interface, use the **no** form of this command.

sccp local *interface-type interface-number* [**port** *port-number*]
no sccp local *interface-type interface-number*

Syntax Description

interface -type	Interface type that the SCCP application uses to register with Cisco CallManager. The type can be an interface address or a virtual-interface address such as Ethernet.
interface-number	Interface number that the SCCP application uses to register with Cisco CallManager.
port *port-number*	(Optional) Port number used by the selected interface. Range is 1025 to 65535. Default is 2000.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The **port** keyword and *port-number* argument were added.

Usage Guidelines

The router must be equipped with one or more voice network modules that provide DSP resources.

Note If the default port is used by another application, the SCCP application fails to register to Cisco CallManager. Use the port keyword with the *port-number* argument to specify a different port for SCCP to use for registering with Cisco CallManager.

Examples

The following example selects a Fast Ethernet interface for SCCP applications to use to register with Cisco CallManager:

```
sccp local FastEthernet 0/0
```

Related Commands

Command	Description
dsp services dspfarm	Enables DSP-farm services.

Command	Description
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

sccp plar

To enter SCCP PLAR configuration mode, use the **sccp plar** command in global configuration mode. To disable private line automatic ringdown (PLAR) on all ports, use the **no** form of this command.

sccp plar
no sccp plar

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (PLAR is not enabled on any port).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used for enabling PLAR features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control. Use the **voiceport** command to enable a specific analog voice port for PLAR.

Examples

The following example sets PLAR on voice ports 2/0, 2/1, and 2/3:

```
Router(config)# sccp plar
Router(config-sccp-plar)# voiceport 2/0 dial 3660 digit 1234 wait-connect 500 interval 200
Router(config-sccp-plar)# voiceport 2/1 dial 3264 digit 678,,,9*0,,#123 interval 100
Router(config-sccp-plar)# voiceport 2/3 dial 3478 digit 34567 wait-connect 500
```

Related Commands

Command	Description
dial peer voice	Enters dial-peer configuration mode and defines a dial peer.
voiceport	Enables a PLAR connection for an analog phone.

sccp switchback timeout guard

To set the Skinny Client Control Protocol (SCCP) switchback guard timer, use the **sccp switchback timeout guard** command in global configuration mode. To reset to the default, use the **no** form of this command.

sccp switchback timeout guard *seconds*
no sccp switchback timeout guard

Syntax Description

seconds	Guard timer value, in seconds. Range is from 180 to 7200. Default is 1200.

Command Default

1200 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

You can use the guard timer value for the switchback algorithm that follows the Graceful Timer method.

Examples

The following example sets the switchback guard timer value to 180 seconds (3 minutes):

```
Router#
sccp switchback timeout guard 180
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

scenario-cause

To configure new Q.850 call-disconnect cause codes for use if an H.323 call fails, use the **scenario-cause** command in H.323-voice-service configuration mode. To revert to the defaults, use the **no** form of this command.

scenario-cause {**arj-default** | **timeout** {**arq** | **t301** | **t303** | **t310**} *code-id*}
no scenario-cause {**arj-default** | **timeout** {**arq** | **t301** | **t303** | **t310**}}

Syntax Description

arj-default *code-id*	Q.850 call-disconnect cause code for use if a call fails for reasons that are assigned to the Admission Reject (ARJ) default cause code. Range: 1 to 127.
timeout arq *code-id*	Q.850 call-disconnect cause code for use if the H.323 gatekeeper Automatic Repeat Request (ARQ) timer expires. Range: 1 to 127.
timeout t301 *code-id*	Q.850 call-disconnect cause code for use when the H.225 alerting (T301) timer expires. Range: 1 to 127.
timeout t303 *code-id*	Q.850 call-disconnect cause code for use when the H.225 setup (T303) timer expires. Range: 1 to 127.
timeout t310 *code-id*	Q.850 call-disconnect cause code for use when the H.225 call-proceeding (T310) timer expires. Range: 1 to 127.

Command Default

No mapping occurs.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

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

Usage Guidelines

Use this command to configure new Q.850 call-disconnect cause codes for use if an H.323 voice call fails during setup.

Examples

The following example causes a gateway to send the default ARJ cause code of 24 rather than the previous default of 63 when a call fails for reasons that are associated with the ARJ default cause code:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# scenario-cause arj-default 24
```

Related Commands

Command	Description
h225 timeout call-proceeding	Sets the call-proceeding (T310, or call-setup to call-disconnect) disconnect timer.

Command	Description
map q850-cause	Maps a Q.850 call-disconnect cause code to a tone.
q850-cause	Maps a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code.

sdspfarm tag

To permit a digital-signal-processor (DSP) farm to be to registered to Cisco Unified CME and associate it with the MAC address of a Skinny Client Control Protocol (SCCP) interface, use the **sdspfarm tag** command in telephony-service configuration mode. To delete a tag generated by the **sdspfarm tag**command, use the **no** form of this command.

sdspfarm tag *number device-name*
no sdspfarm tag *number device-name*

Syntax Description

number	Numeric name for a DSP farm. Number from 1 to 10.
device-name	Word describing the device, such as the MAC address, of the SCCP client interface that is preceded by the Message Transfer Part (MTP).

Command Default

DSP farm is not created.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.
15.1(4)M	Cisco CME 8.6	This command was modified. The maximum number used to tag a DSP farm was increased to 10.

Usage Guidelines

DSP farm profiles are sets of DSP resources used for conferencing and transcoding only. DSP farms do not include voice termination resources. Use the **show interface**command to find the MAC address of the SCCP client interface.

Examples

The following example declares tag 1 as the MAC address of mac000a.8aea.ca80. The **show interface** command is used to obtain the MAC address.

```
Router#
show interface FastEthernet 0/0
.
.
.
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000a.8aea.ca80 (bia 000a.8aea.ca80)
.
.
.
Router(config)# telephony-service
Router(config-telephony)# sdspfarm tag 1 mac000a.8aea.ca80
```

Related Commands

Command	Description
sdspfarm transcode	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.
sdspfarm units	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.

sdspfarm transcode sessions

To specify the maximum number of transcoding sessions allowed per Cisco CallManager Express (Cisco CME) router, use the **sdspfarm transcode sessions**command in telephony-service configuration mode. To return to the default transcode session of 0, use the **no** form of this command.

sdspfarm transcode sessions *number*
no sdspfarm transcode sessions *number*

Syntax Description

number	Declares the number of DSP farm sessions. Valid values are numbers from 1 to 128.

Command Default

The default is 0.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.

Usage Guidelines

The transcoding is allowed between G.711 and G.729. A session consists of two transcode streams. To configure this information, you must know how many digital-signal-processor (DSP) farms are configured on the network module (NM) farms in your Cisco CME router. DSP farms are sets of DSP resources used for conferencing and transcoding only. DSP farms do not include voice termination resources. To learn how many DSP farms have been configured on your Cisco CME router, use the **show sdspfarm** command.

Examples

The following example sets the maximum number of transcoding sessions allowed on the Cisco CME router to 20:

```
Router(config)# telephony-service

Router(config-telephony)# sdspfarm transcode sessions 20
```

Related Commands

Command	Description
sdspfarm tag	Declares a DSP farm and associates it with an SCCP client interface's MAC address.
sdspfarm unit	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.
show sdspfarm	Displays the status of the configured DSP farms and transcoding streams.

sdspfarm units

To specify the maximum number of digital-signal-processor (DSP) farm profiles that are allowed to be registered to the Skinny Client Control Protocol (SCCP) server, use the **sdspfarm units** command in telephony-service configuration mode. To set the number of DSP farm profiles to the default value of 0, use the **no** form of this command.

sdspfarm units *number*
no sdspfarm units *number*

Syntax Description

number	Number of DSP farms. Valid values are numbers from 0 to 10.

Command Default

The default number is 0.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.
15.1(4)M	Cisco CME 8.6	This command was modified. The command increased support for the maximum number of DSP farms to 10.

Usage Guidelines

DSP farm profiles are sets of DSP resources used for conferencing and transcoding only. DSP farm profiles do not include voice termination resources.

Examples

The following example configures a Cisco CME router to register one DSP farm:

```
Router(config)# telephony-service
Router(config-telephony)# sdspfarm units 1
```

Related Commands

Command	Description
sdspfarm tag	Declares a DSP farm and associates it with the MAC address of an SCCP client interface.
sdspfarm transcode	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.

secondary

To set the backup location for storing call detail records (CDRs) if the primary location becomes unavailable, use the **secondary** command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

secondary { **ftp** *path/filename* **username** *username* **password** { **<0-7>** | **LINE** } *password* | **ifs** *device* **:** *filename* | **sftp** *<server>[:<port>]/<path>* **username** *username* **password** { **0** | **6** } *password* }
no secondary { **ftp** | **ifs** | **sftp** }

Syntax Description

ftp *path /filename*	Name and location of the backup file on an external FTP server. Filename is limited to 25 characters.
ifs *device* **:** *filename*	Name and location of the backup file in flash memory or other internal file system on this router. Values depend on storage devices available on the router, for example flash or slot0. Filename is limited to 25 characters.
sftp *<server>[:<port>]/<path>*	Specifies the SFTP mode of file transfer
password {*0* | *6* } **password** {*<0-7 >*| *LINE* }	Following are the password encryption types– • **0**– Specifies that the subsequent password is in plain text. Type **0** disables encryption. • **6**– Specifies that the subsequent password is encrypted using the AES algorithm. Ensure to provide a string in AES-encrypted format. • **7**– Specifies that the subsequent password is hidden. You must enter a Cisco-proprietary encrypted password string. • **LINE**– The cleartext password.
username *username*	User ID for authentication.
password *password*	Password user enters for authentication.

Command Default

Call records are saved to **flash:cdr**.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified for the following: • To support Type 6 encryption. • To display warning message for insecure protocol usage.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(15)XY	This command was introduced.

Usage Guidelines

This command defines the backup location where accounting records are sent if the file transfer to the primary device fails. The file accounting process retries the primary device, defined with the **primary** command, up to the number of times defined by the **maximum retry-count** command before automatically switching over to the secondary device.

The secondary device is attempted only after the primary device fails after the defined number of retries. If the secondary device also fails, the system logs an error and the file accounting process stops.

To manually switch back to the primary device when it becomes available, use the **file-acct reset** command. The system does not automatically switch back to the primary device.

A syslog warning message is generated if flash becomes full.

The filename you assign is appended with the gateway hostname and time stamp at the time the file is created to make the filename unique. For example, if you specify the filename cdrtest1 on a router with the hostname cme-2821, a file is created with the name cdrtest1.cme-2821.2007_10_28T22_21_41.000, where 2007_10_28T22_21_41.000 is the time that the file was created.

Limit the filename you assign with this command to 25 characters, otherwise it could be truncated when the accounting file is created because the full filename, including the appended hostname and timestamp, is limited to 63 characters.

Starting from Cisco IOS XE 26.2.1 release, it is recommended to use Type 6 (AES) for all credential provisioning to comply with security standards. Usage of Type 0, or 7 triggers a syslog warning. Ensure **password encryption aes** and **key config-key password-encrypt** are enabled to support auto-conversion of Type 0, or 7 to Type 6 reversible encryption. If the encryption commands are not enabled, 0 and 7 password types are not converted to type 6; they remain saved as type 0 and 7.



Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows how to configure external SFTP server with unencrypted type of password:

```
Device(config)#gw-accounting file
Device(config-gw-accounting-file)#secondary sftp sftp://john:doe@abc:23//directory1/directory2

username myname password 0 password
```

The following example shows the warning message being displayed for the usage of insecure FTP protocol:

```
Device(config)#gw-accounting file
Device(config-gw-accounting-file)#secondary ftp server1/cdrtest1 username myname password
0 password
SECURITY WARNING - Module: GATEWAY_ACCOUNTING, Command: secondary ftp server1/cdrtest1
username myname password 0 *,
Reason: No encryption is configured, Description: Gateway accounting primary file transfer
 configured with insecure FTP protocol -
vulnerable to credential theft,
Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
```

The following example enables type 6 auto-conversion:

```
Router(config)# password encryption aes
Router(config)# key config-key password-encrypt
Old Key:
New Key :
Confirm Key :
Router(config)# gw-accounting file
Router(config-gw-accounting-file)# secondary sftp
sftp://john:doe@abc:23//directory1/directory2 username myname password 0 password
Router(config-gw-accounting-file)# end

Router#do sh run | sec gw-accou
primary sftp sftp://john:doe@abc:23//directory1/directory2 username myname password 6
EMSefGVigEAMP][YVUF\ZPDbCD^PJQ
```

The following example shows the backup location of the accounting file is set to flash:cdrtest2:

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

Related Commands

Command	Description
file-acct reset	Manually switches back to the primary device for file accounting.
maximum retry-count	Sets the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device.
primary	Sets the primary location for storing the CDRs generated for file accounting.

secure-ciphersuite

To configure the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE, use the **secure-ciphersuite** command in media profile stream-service configuration mode. To revert to the command default, use the **no** form of this command.

secure-ciphersuite *list*
no secure-ciphersuite *list*

Syntax Description

list	List of cipher suites supported with the WebSockets in CUBE. Starting from Cisco IOS XE Dublin 17.12.1a, CUBE supports GCM cipher in addition to the other supported ciphers. The following list of cipher suites are supported for WebSocket connections: • aes-128-cbc-sha • dhe-rsa-aes-cbc-sha2 • ecdhe-rsa-aes-cbc-sha2 • rsa-aes-cbc-sha2 • ecdhe-ecdsa-aes-gcm-sha2 • ecdhe-rsa-aes-gcm-sha2

Command Default

By default, all cipher suites including GCM cipher suites are supported for WebSocket connections.

Command Modes

Media Profile Stream-Service configuration mode (cfg-mediaprofile)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on CUBE.
Cisco IOS XE Dublin 17.12.1a	Added support for GCM cipher negotiation for WebSocket based media forking.

Usage Guidelines

Use the **secure-ciphersuite** command to configure the cipher suites (encryption algorithms) for encryption over HTTPS for a WebSocket connection in CUBE.

Configure **no secure-ciphersuite** to enable the default behavior. However, you can limit negotiation to a selected set of one or more cipher suites using **secure-ciphersuite** *list* command.

Starting from Cisco IOS XE Dublin 17.12.1a, CUBE supports GCM cipher suites for WebSocket connections in addition to the other supported ciphers.

Examples

The following example shows how to configure secure ciphers for WebSockets in CUBE:

```
Device(config)#media profile stream-service 1
```

```
Device(cfg-mediaprofile)#secure-ciphersuite ?
  aes-128-cbc-sha           Encryption tls_with_aes-128-cbc-sha2 ciphersuite
  dhe-rsa-aes-cbc-sha2      Encryption tls_rsa_with_cbc_sha2 ciphersuite
  ecdhe-rsa-aes-cbc-sha2    Encryption tls_rsa_with_aes-cbd-sha2 ciphersuite
  rsa-aes-cbc-sha2          Encryption tls_rsa_with_aes_cbc_sha2 ciphersuite
  ecdhe-ecdsa-aes-gcm-sha2  Encryption tls_rsa_with_ecdhe-ecdsa-aes-gcm-sha2 ciphersuite
  ecdhe-rsa-aes-gcm-sha2    Encryption tls_rsa_with_aes-gcm-sha2 ciphersuite
Device(cfg-mediaprofile)#secure-ciphersuite tls_rsa_with_cbc_sha2
  WS Client Secure Ciphersuite: tls_rsa_with_cbc_sha2
Device(cfg-mediaprofile)#
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in the media profile configuration mode.
description (media-profile)	Specifies a description for the media profile.
media class	Applies the media class at the dial peer level.

security

To enable authentication and authorization on a gatekeeper, use the **security** command in gatekeeper configuration mode. To disable security, use the **no** form of this command.

security {**any** | **h323-id** | **e164**} {**password default** *password* | **password separator** *character*}
no security {**any** | **h323-id** | **e164**} {**password default** *password* | **password separator** *character*}

Syntax Description

any	Uses the first alias of an incoming registration, admission, and status (RAS) protocol registration, regardless of its type, to identify the user to RADIUS/TACACS+.
h323 -id	Uses the first H.323 ID type alias to identify the user to RADIUS/TACACS+.
e164	Uses the first E.164 address type alias to identify the user to RADIUS/TACACS+.
password default *password*	Default password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The password must be identical to the password on the authentication server.
password separator *character*	Character that endpoints use to separate the H.323-ID from the piggybacked password in the registration. Specifying this character allows each endpoint to supply a user-specific password. The separator character and password are stripped from the string before it is treated as an H.323-ID alias to be registered. Note that passwords may only be piggybacked in the H.323-ID, not the E.164 address, because the E.164 address allows a limited set of mostly numeric characters. If the endpoint does not wish to register an H.323-ID, it can still supply an H.323-ID consisting of just the separator character and password. This H.323-ID consisting of just the separator character and password are understood to be a password mechanism and no H.323-ID is registered.

Command Default

No default

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Use this command to enable identification of registered aliases by RADIUS/TACACS+. If the alias does not exist in RADIUS/TACACS+, the endpoint is not allowed to register.

A RADIUS/TACACS+ server and encryption key must have been configured in Cisco IOS software for security to work.

Only the first alias of the proper type is identified. If no alias of the proper type is found, the registration is rejected.

This command does not allow you to define the password mechanism unless the security type (**h323-id** or **e164** or **any**) has been defined. Although the **no security password** command undefines the password

mechanism, it leaves the security type unchanged, so security is still enabled. However, the **no security** command disables security entirely, including removing any existing password definitions.

Examples

The following example enables identification of registrations using the first H.323 ID found in any registration:

```
security h323id
```

The following example enables security, authenticating all users by using their H.323-IDs and a password of qwerty2x:

```
security h323-id
security password qwerty2x
```

The next example enables security, authenticating all users by using their H.323-IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security h323-id
security password separator !
```

If a user registers with an H.323-ID of joe!024aqx, the gatekeeper authenticates user joe with password 024aqx, and if that is successful, registers the user with the H.323-ID of joe. If the exclamation point is not found, the user is authenticated with the default password, or a null password if no default has been configured.

The following example enables security, authenticating all users by using their E.164 IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security e164
security password separator !
```

If a user registers with an E.164 address of 5551212 and an H.323-ID of !hs8473q6, the gatekeeper authenticates user 5551212 and password hs8473q6. Because the H.323-ID string supplied by the user begins with the separator character, no H.323-ID is registered, and the user is known only by the E.164 address.

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius -server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

security acl

To configure access-list based filtering on the gatekeeper, use the **security acl**command in gatekeeper configuration mode. To disable, use the no form of this command.

security acl {**answerarq** | **lrq**} *access-list-number*
no security acl {**answerarq** | **lrq**}

Syntax Description

answerarq	Filters incoming answer admission requests (AnswerARQ) using IP access-lists.
lrq	Filters incoming location requests (LRQs) using IP access-list.
access-list-number	Number of an access list that was configured using the access-list command. This is a decimal number from 1 to 99 or from 1300 to 1999. Only standard IP access lists numbered 1 through 99 are supported for the Tokenless Call Authorization feature.

Command Default

No default behavior or values.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.3(5)	This command was introduced.

Usage Guidelines

The **security acl** command configures the gatekeeper to use IP access lists for security. Use this command in conjunction with the **access-list** command to configure access-list based AnswerARQ and LRQ requests filtering on a gatekeeper. The gatekeeper will process only those requestswhich have been sent by sources that are permitted access by the specified IP access list. Requests sent by sources which have been denied by the specified IP access lists, will be rejected.

Examples

The following example shows how to configure a gatekeeper to use a previously configured IP access list with an IP access list number of 30 for call authorization:

```
Router(config-gk)# security acl answerarq 30
```

The following example shows how to configure a gatekeeper to use a previously configured IP access list with an IP access list number of 20 for LRQ filtering:

```
Router(config-gk)# security acl lrq 20
```

Related Commands

Command	Description
access -list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

security izct

To configure the gatekeeper to include the destination E.164 alias in the IZC token hash, use the **security izct** command in gatekeeper configuration mode. To not include destination E.16 alias in IZC token hash, use the **no** form of this command.

security izct password *password* [**hash** {**dest-alias** | **src-alias** | **dest-csa** | **src-csa** | **dest-epid** | **src-epid**}]
no security izct *password* [**hash** {**dest-alias** | **src-alias** | **dest-csa** | **src-csa** | **dest-epid** | **src-epid**}]

Syntax Description

password *password*	Specifies the password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The password must be identical to the password on the authentication server.
hash	Specifies the options to be used in hash generation.
dest-alias	Specifies that the destination alias be included in hash generation.
src-alias	Specifies that the source alias be included in hash generation.
dest-csa	Specifies that the destination csa be included in hash generation.
src-csa	Specifies that the source alias be included in hash generation.
dest-epid	Specifies that the destination epid be included in hash generation.
src-epid	Specifies that the source epid be included in hash generation.

Command Default

Destination E.16 alias are not included in IZC token hash.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.3(5)	This command was introduced.
12.4(15)XZ	The **dest-alias, src-alias, dest-csa, src-csa, dest-epid,**and **src-epid**keywords were added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Configure the **security izct** command on the gatekeeper that generates the InterZone Clear Token (IZCT) hash to prevent rogue endpoints from sending an ARQ message with one called number and then changing the called number when they send the SETUP message to the terminating endpoint. When this command is configured, modification of the called number after the IZCT hash is generated by the trunking gateway will not be allowed. The IZCT token generated is valid only for 30 seconds and the IZCT hash token generated by terminating gatekeeper (TGK) can be used for multiple calls.

The call is rejected if any intermediate entity, such as a Cisco Gatekeeper Transaction Message Protocol (GKTMP) server (on the originating gatekeeper) or the originating gateway (using number translation rules), tries to modify the called number after the token is prepared during address resolution.

- The **hash** keyword at originating gateway (OGW) and TGK do not need to match.
- More than one **hash** keyword can be configured for the **security izct**command.

The **security izct**command must be configured at OGK or TGK in order to enable the feature.

When configuring an OGW to an OGK to a TGK and to a TGW. The **security izct**command is optional at the OGK, and required at the TGK. If hash parameter is not specified at the TGK, then dest-alias (default) will be used for hash token computation.

The **no** version of this command the requires the keyword argument combinations as defined in the preceding command syntax table.

Examples

The following example prevents modification of the called number after the IZCT hash is generated by the trunking gateway:

```
Router(config-gk)# security izct password example hash dest-alias
```

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

security mode

To set the security mode for a specific dial peer using Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) services in a secure Cisco Unified CME network, use the **security mode** command in dial peer configuration mode. To return to the default, use the **no** form of this command.

security mode {**authenticated** | **none** | **encrypted** | **system**}
no security mode

Syntax Description

authenticated	Sets the security mode to authenticated and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through the secure TLS connection on TCP port 2443.
none	SCCP signaling is not secure.
encrypted	Sets the security mode to encrypted and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through Secure Real-Time Transport Protocol (SRTP).
system	Enables the security mode specified at the global level by the **stcapp security mode** command.

Command Default

Security mode specified at the global level is enabled.

Command Modes

Dial peer configuration (config-dialpeer)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify security mode on the voice gateway for Cisco Unified CME phone authentication and encryption.

Set the SCCP signaling security mode globally using the **stcapp security mode** command in global configuration mode. If you use both the **stcapp security mode** and the **security mode**commands, the dial-peer level command, **security mode**, overrides the global setting.

Examples

The following example selects secure SCCP signaling in authenticated mode:

```
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# security mode authenticated
```

The following example selects encrypted secure SCCP signaling and encryption through SRTP:

```
Router(config)# dial-peer voice 2 pots
Router(config-dialpeer)# security mode encrypted
```

Related Commands

Command	Description
stcapp security mode	Enables security for STCAPP endpoints and specifies the security mode to be used for setting up the TLS connection.

sequence-numbers

To enable the generation of sequence numbers in each frame generated by the digital signal processor (DSP) for Voice over Frame Relay applications, use the **sequence-numbers** command in dial-peer configuration mode. To disable the generation of sequence numbers, use the **no** form of this command.

sequence-numbers
no sequence-numbers

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines

Sequence numbers on voice packets allow the digital signal processor (DSP) at the playout side to detect lost packets, duplicate packets, or out-of-sequence packets. This helps the DSP to mask out occasional drop-outs in voice transmission at the cost of one extra byte per packet. The benefit of using sequence numbers versus the cost in bandwidth of adding an extra byte to each voice packet on the Frame Relay network must be weighed to determine whether to disable this function for your application.

Another factor to consider is that this command does not affect codecs that require a sequence number, such as G.726. If you are using a codec that requires a sequence number, the DSP generates one regardless of the configuration of this command.

Examples

The following example disables generation of sequence numbers for VoFR frames for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 no sequence-numbers
```

Related Commands

Command	Description
called -number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial -peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.

Command	Description
destination -pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf -relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
session protocol (Voice over Frame Relay)	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal -type	Sets the signaling type to be used when connecting to a dial peer.

server (auto-config application)

To configure the IP address or name of the TFTP server for an auto-configuration application, use the **server** command in auto-config application configuration mode. To remove the IP address or name, use the **no** form of this command.

{**server** *ip-address* | *domain-name* [*ip-addressdomain-name*] [*ip-addressdomain-name*]}
no server

Syntax Description

ip-address	Specifies the IP address of the TFTP server.
domain-name	Specifies the domain name of the TFTP server.

Command Default

No default behavior or values.

Command Modes

Auto-config application configuration (auto-config-app)

Command History

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

Examples

The following example shows the **server** command used to configure two TFTP servers for an auto-configuration application:

```
Router(auto-config-app)# server 172.18.240.45 172.18.240.55
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the Skinny Client Control Protocol (SCCP) application.
show auto-config	Displays the current status of auto-config applications.

server (presence)

To specify the IP address of a presence server for sending presence requests from internal watchers to external presence entities, use the **server**command in presence configuration mode. To remove the server, use the **no** form of this command.

server *ip-address*
no server

Syntax Description

ip-address	IP address of the remote presence server.

Command Default

A remote presence server is not used.

Command Modes

Presence configuration (config-presence)

Command History

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

Usage Guidelines

This command specifies the IP address of a presence server that handles presence requests when the watcher and presence entity (presentity) are not collocated. The router acts as the presence server and processes all presence requests and status notifications when a watcher and presentity are both internal. If a subscription request is for an external presentity, the request is sent to the remote server specified by this command.

Examples

The following example shows a presence server with IP address 10.10.10.1:

```
Router(config)# presence
Router(config-presence)# allow subscribe
Router(config-presence)# server 10.10.10.1
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
max-subscription	Sets the maximum number of concurrent watch sessions that are allowed.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.

Command	Description
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

server (RLM)

To identify an RLM server, use the **server** RLM configuration command. To remove the identification, use the **no** form of this command

server *name-tag*
no server *name-tag*

Syntax Description

name -tag	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Command Default

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

Each server can have multiple entries of IP addresses or aliases.

Examples

The following example identifies the RLM server and defines the associated IP addresses:

```
rlm group 1
 server rl-server
 link address 10.1.4.1 source Loopback1 weight 4
 link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.

Command	Description
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

server absent reject

To configure the gatekeeper to reject new registrations or calls when the connection to the Gatekeeper Transaction Message Protocol (GKTMP) server is down, use the **server absent reject** command in gatekeeper configuration mode. To disable, use the no form of this command.

server absent reject {**arq** | **rrq**}
no server absent reject {**arq** | **rrq**}

Syntax Description

arq	Reject call admission request (ARQ) messages.
rrq	Reject registration request (RRQ) messages.

Command Default

By default, registrations and calls are not rejected.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660 and Cisco MC3810.

Usage Guidelines

This command configures the gatekeeper to reject new registrations or calls when it is unable to reach the GKTMP server because the TCP connection between the gatekeeper and GKTMP server is down. If multiple GKTMP servers are configured, the gatekeeper tries all of them and rejects registrations or calls only if none of the servers respond. You can also use this feature for security or service denial if a connection with the server is required to complete a registration.



Note This command assumes that RRQ and ARQ triggers are used between the gatekeeper and GKTMP server.

Examples

The following example directs the gatekeeper to reject registrations when it cannot connect to the GKTMP server:

```
Router# show gatekeeper configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 no shutdown
 server absent reject rrq
.
.
.
```

server flow-control

To enable flow control on the Cisco IOS gatekeeper (GK) and reset all thresholds to default, use the **server flow-control** command in gatekeeper configuration mode. To disable GK flow control, use the **no** form of this command.

server flow-control [**onset** *value*] [**abatement** *value*] [**qcount** *value*]
no server flow-control

Syntax Description

onset *value*	(Optional) Percentage of the server timeout value that is used to mark the server as usable or unusable. Range is from 1 to 100. The default is 80.
abatement *value*	(Optional) Percentage of the server timeout value that is used to mark the server as unusable or usable. Range is from 1 to 100. The default is 50. **Note** The abatement value must be less than the onset value.
qcount *value*	(Optional) Threshold length of the outbound queue on the GK. The queue contains messages waiting to be transmitted to the server. The TCP socket between the GK and Gatekeeper Transaction Message Protocol (GKTMP) server queues messages if it has too many to transmit. If the count of outbound queue length on the server reaches the qcount value, the server is marked unusable. Range is from 1 to 1000. The default is 400.

Command Default

The gatekeeper will send a maximum of 1000 RRQ messages.

Command Modes

Gatekeeper configuration (config-gk)

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.

Usage Guidelines

Suppose the server timeout value is 3 seconds, the onset value is 50, and the abatement value is 40. When the average response time from the server to the Gatekeeper Transaction Message Protocol (GKTMP) reaches 1.5 seconds (the onset percentage of the server timeout value), the server is marked as unusable. During the period that the server is marked as unusable, REQUEST ALV messages are still sent to the unusable server. When the response time is lowered to 1.2 seconds (the abatement percentage of the timeout value), the server is marked usable again, and the GKTMP resumes sending messages to the server.

When the **server flow-control** command is configured on its own the default is value 400. If you change one parameter using the **server flow-control** command, all other parameters revert to the default values. For example, if the onset is configured at 70 percent and you use the **server flow-control**command to set the abatement level, the onset resets to the default (80 percent).

Examples

The following example uses the command with the default values:

```
Router# server flow-control
```

The following example enables the GKTMP Interface Resiliency Enhancement feature with an onset level of 50:

```
Router# server flow-control onset 50
*Mar  8 20:05:34.081: gk_srv_handle_flowcontrol: Flow control enabled
Router# show running-config
Building configuration...
Current configuration : 1065 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname snet-3660-3
!
.
.
.
gatekeeper
 zone local snet-3660-3 cisco.com
 zone remote snet-3660-2 cisco.com 209.165.200.225 1719
 zone prefix snet-3660-2 408*
 lrq forward-queries
 no use-proxy snet-3660-3 default inbound-to terminal
 no use-proxy snet-3660-3 default outbound-from terminal
 no shutdown
 server registration-port 8000
 server flow-control onset 50
!
.
.
.
end
```

The following example enables the GKTMP Interface Resiliency Enhancement feature:

```
Router# show gatekeeper status
Gatekeeper State: UP
    Load Balancing:   DISABLED
    Flow Control:     ENABLED
    Zone Name:        snet-3660-3
    Accounting:       DISABLED
    Endpoint Throttling:        DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:              unlimited
    Current Remote Bandwidth:              0 kbps
    Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

The following example shows the server statistics, including timeout encountered, average response time, and the server status:

```
Router# show gatekeeper server
            GATEKEEPER SERVERS STATUS
            =========================
Gatekeeper Server listening port: 8250
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 3.1
```

```
Gatekeeper-ID: Gatekeeper1
------------------------
  RRQ  Priority: 5
    Server-ID: Server43
    Server IP address: 209.165.200.254:40118
    Server type: dynamically registered
    Connection Status: active
    Trigger Information:
      Trigger unconditionally
    Server Statistics:
    REQUEST RRQ Sent=0
    RESPONSE RRQ Received = 0
    RESPONSE RCF Received = 0
    RESPONSE RRJ Received = 0
    Timeout encountered=0
    Average response time(ms)=0
    Server Usable=TRUE
```

Related Commands

Command	Description
timer server timeout	Specifies the timeout value for a response from a back-end GKTMP server.

server registration-port

To configure the listener port for the server to establish a connection with the gatekeeper, use the **server registration-port** command in gatekeeper configuration mode. To force the gatekeeper to close the listening socket so that no more new registration takes place, use the **no** form of this command.

server registration-port *port-number*
no server registration-port *port-number*

Syntax Description

port -number	Port number on which the gatekeeper listens for external server connections. Range is from 1 to 65535. There is no default.

Command Default

No registration port is configured.

Note If the gatekeeper is to communicate with network servers, a registration port must be configured on it.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.2(11)T	This command was implemented on the Cisco 3700 series.

Usage Guidelines

Use this command to configure a server registration port to poll for servers that want to establish connections with the gatekeeper.

Note The no form of this command forces the gatekeeper on this router to close the listen socket, so it cannot accept more registrations. However, existing connections between the gatekeeper and servers are left open.

Examples

The following example establishes a listener port for a server connection with a gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server registration-port 20000
```

Related Commands

Command	Description
server trigger	Configure static server triggers for specific RAS messages to be forwarded to a specified server.

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server routing

To specify the type of circuit messages sent to the Gatekeeper Transaction Message Protocol (GKTMP) server, use the **server routing**command in gatekeeper configuration mode. To return to the default, use the **no** form of this command.

server routing {**both** | **carrier** | **trunk-group**}
no server routing {**both** | **carrier** | **trunk-group**}

Syntax Description

both	Sends both types of information in GKTMP messages.
carrier	Sends only carrier information in GKTMP messages. This is the default.
trunk -group	Sends only trunk-group information in GKTMP messages.

Command Default

Carrier

Command Modes

Gatekeeper configuration (config-gk)

Command History

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

Usage Guidelines

Use this command to route carrier and trunk-group messages from the gatekeeper to the GKTMP server.

The **carrier**keyword sends the "I" and "J" tags in the GKTMP messages. The **trunk-group**keyword sends the "P" and "Q" tags in the GKTMP messages. The **both**keyword sends both sets of tags.

Examples

The following example enables trunk-group information to be sent in GKTMP messages from the gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server routing trunk-group
```

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger arq

To configure the admission request (ARQ) trigger statically on the gatekeeper, use the **server trigger arq**command in gatekeeper configuration mode. Submode commands are available after the **server trigger arq**command is entered. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of this command.

server trigger arq *gkid priority server-id server-ip-address server-port*
no server trigger arq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info -only	Use to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the Gatekeeper Transaction Message Protocol (GKTMP) server application.
shutdown	Use to temporarily disables a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send ARQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value* -- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

redirect -reason *reason-number*	Use to send ARQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason -number*-- Range is from 0 to 65535. Currently-used values are: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration(config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the admission request (ARQ) static server trigger. The gatekeeper checks incoming gateway ARQ messages for the configured trigger information. If an incoming ARQ message contains the specified trigger information, the gatekeeper sends the ARQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the ARQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the ARQ messages, the gatekeeper sends all ARQ messages to the GKTMP server application.

If the gatekeeper receives an ARQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming ARQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two ARQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two ARQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming ARQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one ARQ trigger registration message with the same priority but for different GKTMP servers, the gatekeeper retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all ARQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger arq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_arqtrigger)# exit
```

The following example configures an ARQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any ARQ message that contains H.323 ID "3660-gw1", e-mail ID "joe.xyz.com", or a redirect reason 1. All other ARQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger arq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-arqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-arqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-arqtrigger)# redirect-reason 1
Router(config-gk-arqtrigger# exit
```

If the ARQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger arq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_arqtrigger)# destination-info e164 1800....
Router(config-gk_arqtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming ARQ messages for the destination H.323 ID, e-mail ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the ARQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" ARQ trigger registration had been defined with a priority 1 instead of priority 2, the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those ARQ messages that contain a destination E.164 address that starts with 1800. All other ARQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger brq

To configure the bandwidth request (BRQ) trigger statically on the gatekeeper, use the **server trigger brq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger brq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger brq *gkid priority server-id server-ip-address server-port*
no server trigger brq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
redirect -reason *reason-number*	Use to send BRQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason-number*-- Range is from 0 to 65535. Currently used values are as follows: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This the command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the bandwidth request (BRQ) static server trigger. The gatekeeper checks incoming gateway BRQ messages for the configured trigger information. If an incoming BRQ message contains the specified trigger information, the gatekeeper sends the BRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the BRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the BRQ messages, the gatekeeper sends all BRQ messages to the GKTMP server application.

If the gatekeeper receives BRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming BRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two BRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two BRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming BRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one BRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all BRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger brq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_brqtrigger)# exit
```

The following example configures BRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any BRQ message containing redirect reason 1 or redirect reason 2. All other BRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger brq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-brqtrigger)# redirect-reason 1
Router(config-gk-brqtrigger)# redirect-reason 2
Router(config-gk-brqtrigger# exit
```

If the BRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger brq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_brqtrigger)# redirect-reason 10
Router(config-gk_brqtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming BRQ messages for redirect reasons 1 or 2 before checking for redirect reason 10. If any one of those conditions is met, the gatekeeper sends the BRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" BRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those BRQ messages that contain a redirect reason 10. All other BRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger drq

To configure the disengage request (DRQ) trigger statically on the gatekeeper, use the **server trigger drq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger drq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger drq *gkid priority server-id server-ip-address server-port*
no server trigger drq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the Reliability, Availability, and Serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send automatic repeat request (ARQ) RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

call info type { **fax** | **modem** | **voice**	Use to send ARQ RAS messages containing a specified call info type to the GKTMP server application. The following types can be used: • **fax** • modem • **voice**
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.
12.4(4)T	The **call-info-type** submode command was added.

Usage Guidelines

Use this command and its optional submode commands to configure the disengage request (DRQ) static server trigger. The gatekeeper checks incoming gateway DRQ messages for the configured trigger information. If an incoming DRQ message contains the specified trigger information, the gatekeeper sends the DRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the DRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the DRQ messages, the gatekeeper sends all DRQ messages to the GKTMP server application.

If the gatekeeper receives a DRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming DRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two DRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two DRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming DRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one DRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeeper retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper together with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all DRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger drq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_drqtrigger)# exit
```

The following example configures DRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any DRQ message containing an H.323 ID "3660-gw1" or e-mail ID "joe.xyz.com". All other DRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger drq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-drqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-drqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-drqtrigger# exit
```

If the DRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger drq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_drqtrigger)# destination-info e164 1800....
Router(config-gk_drqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming DRQ messages for the destination H.323 ID or e-mail ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the DRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" DRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server Server-west only those DRQ messages that contain a destination E.164 address starting with 1800. All other DRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger irr

To configure the information request response (IRR) trigger statically on the gatekeeper, use the **server trigger irr**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger irr**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger irr *gkid priority server-id server-ip-address server-port*
no server trigger irr *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send IRR RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

redirect -reason *reason-number*	Use to send IRR RAS messages containing a specific redirect reason to the GKTMP server application. • *reason -number*--Range is from 0 to 65535. Currently used values are the following: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the information request response (IRR) static server trigger. The gatekeeper checks incoming gateway IRR messages for the configured trigger information. If an incoming IRR message contains the specified trigger information, the gatekeeper sends the IRR message to the GKTMP server application. In addition, the IRR message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the IRR messages, the gatekeeper sends all IRR messages to the GKTMP server application.

If the gatekeeper receives an IRR trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming IRR RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two IRR trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two IRR trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming IRR messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one IRR trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all IRR messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger irr sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_irrtrigger)# exit
```

The following example configures an IRR trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any IRR message containing an H.323 ID "3660-gw1", e-mail ID "joe.xyz.com, or a redirect reason 1. All other IRR messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger irr alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-irrtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-irrtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-irrtrigger)# redirect-reason 1
Router(config-gk-irrtrigger# exit
```

If the IRR registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger irr alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_irrtrigger)# destination-info e164 1800....
Router(config-gk_irrtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming IRR messages for the destination H.323 ID, e-mail ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the IRR message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" IRR trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those IRR messages that contain a destination E.164 address starting with 1800. All other IRR messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lcf

To configure the location confirm (LCF) trigger statically on the gatekeeper, use the **server trigger lcf**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lcf**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger lcf *gkid priority server-id server-ip-address server-port*
no server trigger lcf *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send LCF RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

remote -ext-address e164 *value*	Use to send LCF RAS messages that contain a specified remote extension address to the GKTMP server application.
	• **e164** --Remote extension address is an E.164 address.
	• *value* --Value against which to compare the destination address in the RAS messages. The following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the location confirm (LCF) static server trigger. The gatekeeper checks incoming gateway LCF messages for the configured trigger information. If an incoming LCF message contains the specified trigger information, the gatekeeper sends the LCF message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LCF message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LCF messages, the gatekeeper sends all LCF messages to the GKTMP server application.

If the gatekeeper receives an LCF trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LCF RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LCF trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LCF trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LCF messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LCF trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LCF messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lcf sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lcftrigger)# exit
```

The following example configures an LCF trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any LCF message containing an H.323 ID "3660-gw1", e-mail ID joe.xyz.com, or a remote extension address starting with 1408. All other LCF messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lcf alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lcftrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lcftrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lcftrigger)# remote-ext-address e164 1408....
Router(config-gk-lcftrigger# exit
```

If the LCF registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lcf alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lcftrigger)# remote-ext-address e164 1800....
Router(config-gk_lcftrigger)# exit
```

then gatekeeper "alpha" checks all incoming LCF messages for the destination H.323 ID, e-mail ID, or remote extension address 1408 before checking for the remote extension address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LCF message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LCF trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LCF messages that contain a remote extension address E.164 address starting with 1800. All other LCF messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lrj

To configure the location reject (LRJ) trigger statically on the gatekeeper, use the **server trigger lrj**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrj**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger lrj *gkid priority server-id server-ip-address server-port*
no server trigger lrj *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send LRJ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the location reject (LRJ) static server trigger. The gatekeeper checks incoming gateway LRJ messages for the configured trigger information. If an incoming LRJ message contains the specified trigger information, the gatekeeper sends the LRJ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRJ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRJ messages, the gatekeeper sends all LRJ messages to the GKTMP server application.

If the gatekeeper receives an LRJ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LRJ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRJ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LRJ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRJ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LRJ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LRJ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lrj sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrjtrigger)# exit
```

The following example configures an LRJ trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any LRJ message containing an H.323 ID "3660-gw1" or e-mail ID joe.xyz.com. All other LRJ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrj alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lrjtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lrjtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lrjtrigger# exit
```

If the LRJ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrj alpha 2 Server-west 10.10.10.10 1751
```

```
Router(config-gk_lrjtrigger)# destination-info e164 1800....
Router(config-gk_lrjtrigger)# exit
```

then gatekeeper "alpha" checks all incoming LRJ messages for the destination H.323 ID or email ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRJ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LRJ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LRJ messages that contain a destination E.164 address starting with 1800. All other LRJ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lrq

To configure the location request (LRQ) trigger statically on the gatekeeper, use the **server trigger lrq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger lrq *gkid priority server-id server-ip-address server-port*
no server trigger lrq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send LRQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

redirect -reason *reason-number*	Use to send LRQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason -number*--Range is from 0 to 65535. Currently used values are the following: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the location request (LRQ) static server trigger. The gatekeeper checks incoming gateway LRQ messages for the configured trigger information. If an incoming LRQ message contains the specified trigger information, the gatekeeper sends the LRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRQ messages, the gatekeeper sends all LRQ messages to the GKTMP server application.

If the gatekeeper receives an LRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrqtrigger)# exit
```

The following example configures an LRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any LRQ message containing an H.323 ID "3660-gw1", e-mail ID joe.xyz.com, or a redirect reason 1. Other LRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lrqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lrqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lrqtrigger)# redirect-reason 1
Router(config-gk-lrqtrigger# exit
```

If the LRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lrqtrigger)# destination-info e164 1800....
Router(config-gk_lrqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming LRQ messages for the destination H.323 ID, email ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LRQ messages that contain a destination E.164 address starting with 1800. All other LRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger rai

To configure the resources available indicator (RAI) trigger statically on the gatekeeper, use the **server trigger rai**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rai**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger rai *gkid priority server-id server-ip-address server-port*
no server trigger rai *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint -type *value*	Use to send RAI RAS messages that contain a particular endpoint type to the GKTMP server application. • *value* --Value against which to compare the endpoint type in the RAS messages. Valid endpoint types are the following: • **gatekeeper**--Endpoint is an H.323 gatekeeper. • **h320-gateway**--Endpoint is an H.320 gateway. • **mcu**--Endpoint is a multipoint control unit (MCU). • **other-gateway**--Endpoint is another type of gateway not specified on this list. • **proxy**--Endpoint is an H.323 proxy. • **terminal**--Endpoint is an H.323 terminal. • **voice-gateway**--Endpoint is a voice gateway.
info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

supported -prefix *value*	Use to send RAI RAS messages that contain a specific supported prefix to the GKTMP server application. • *value* --Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the resources available indicator (RAI) static server trigger. The gatekeeper checks incoming gateway RAI messages for the configured trigger information. If an incoming RAI message contains the specified trigger information, the gatekeeper sends the RAI message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RAI message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RAI messages, the gatekeeper sends all RAI messages to the GKTMP server application.

If the gatekeeper receives an RAI trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming RAI RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RAI trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two RAI trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RAI messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one RAI trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all RAI messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger rai sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_raitrigger)# exit
```

The following example configures an RAI trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any RAI message that contain an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. All other RAI messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger rai alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-raitrigger)# endpoint-type mcu
Router(config-gk-raitrigger)# endpoint-type proxy
Router(config-gk-raitrigger)# supported-prefix 1#
Router(config-gk-raitrigger# exit
```

If the RAI registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rai alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_raitrigger)# supported-prefix 1234*
Router(config-gk_raitrigger)# exit
```

Then gatekeeper "alpha" checks all incoming RAI messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RAI message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" RAI trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those RAI messages that contain a supported prefix of 1234*. All other RAI messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger rrq

To configure the registration request (RRQ) trigger statically on the gatekeeper, use the **server trigger rrq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rrq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger rrq *gkid priority server-id server-ip-address server-port*
no server trigger rrq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint -type *value*	Use to send RRQ RAS messages containing a particular endpoint type to the GKTMP server application. • *value* --Value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are the following: • **gatekeeper**--Endpoint is an H.323 gatekeeper. • **h320-gateway**--Endpoint is an H.320 gateway. • **mcu**--Endpoint is a multipoint control unit (MCU). • **other-gateway**--Endpoint is another type of gateway not specified on this list. • **proxy**--Endpoint is an H.323 proxy. • **terminal**--Endpoint is an H.323 terminal. • **voice-gateway**--Endpoint is a voice gateway.
info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

supported -prefix *value*	Use to send RRQ RAS messages containing a specific supported prefix to the GKTMP server application. • *value* --Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the registration request (RRQ) static server trigger. The gatekeeper checks incoming gateway RRQ messages for the configured trigger information. If an incoming RRQ message contains the specified trigger information, the gatekeeper sends the RRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RRQ messages, the gatekeeper sends all RRQ messages to the GKTMP server application.

If the gatekeeper receives an RRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming RRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two RRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one RRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all RRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger rrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_rrqtrigger)# exit
```

The following example configures an RRQ trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any RRQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. Other RRQ messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger rrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-rrqtrigger)# endpoint-type mcu
Router(config-gk-rrqtrigger)# endpoint-type proxy
Router(config-gk-rrqtrigger)# supported-prefix 1#
Router(config-gk-rrqtrigger# exit
```

If the RRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_rrqtrigger)# supported-prefix 1234*
Router(config-gk_rrqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming RRQ messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" RRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those RRQ messages that contain a supported prefix of 1234*. All other RRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger urq

To configure the unregistration request (URQ) trigger statically on the gatekeeper, use the **server trigger urq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger urq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger urq *gkid priority server-id server-ip-address server-port*
Submode Commands:
info-only
shutdown
endpoint-type *value*
supported-prefix *value*
no server trigger urq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint -type *value*	Use to send URQ RAS messages containing a particular endpoint type to the GKTMP server application. • *value* --Value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are the following: • **gatekeeper**--Endpoint is an H.323 gatekeeper. • **h320-gateway**--Endpoint is an H.320 gateway. • **mcu**--Endpoint is a multipoint control unit (MCU). • **other-gateway**--Endpoint is another type of gateway not specified on this list. • **proxy**--Endpoint is an H.323 proxy. • **terminal**--Endpoint is an H.323 terminal. • **voice-gateway**--Endpoint is a voice gateway.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
supported -prefix *value*	Use to send URQ RAS messages containing a specific supported prefix to the GKTMP server application. • *value* --Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the unregistration request (URQ) static server trigger. The gatekeeper checks incoming gateway URQ messages for the configured trigger information. If an incoming URQ message contains the specified trigger information, the gatekeeper sends the URQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the URQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the URQ messages, the gatekeeper sends all URQ messages to the GKTMP server application.

If the gatekeeper receives a URQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming URQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two URQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two URQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming URQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one URQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The the **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all URQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger urq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_urqtrigger)# exit
```

The following example configures a URQ trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any URQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. Other URQ messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger urq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-urqtrigger)# endpoint-type mcu
Router(config-gk-urqtrigger)# endpoint-type proxy
Router(config-gk-urqtrigger)# supported-prefix 1#
Router(config-gk-urqtrigger# exit
```

If the URQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger urq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_urqtrigger)# supported-prefix 1234*
Router(config-gk_urqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming URQ messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the URQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" URQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those URQ messages that contain a supported prefix of 1234*. All other URQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

service

To load and configure a specific, standalone application on a dial peer, use the **service** command in application configuration mode. To remove the application from the dial peer, use the **no** form of this command.

service [**alternate** | **default**] *service-name* *location*
no **service** [**alternate** | **default**] *service-name* *location*

Syntax Description

alternate	(Optional) Alternate service to use if the service that is configured on the dial peer fails.
default	(Optional) Specifies that the default service ("DEFAULT") on the dial peer is used if the alternate service fails.
service-name	Name that identifies the voice application, service, or package. This is a user-defined name and does not have to match the script name.
location	Directory and filename of the Tcl script or VoiceXML document in URL format. For example, the following are valid locations: • built-in applications (builtin:*filename*) • flash memory (flash:filename) • HTTP server (http://../filename) • HTTPS (HTTP over Secure Socket Layer (SSL)) server (https://../filename) • TFTP server (tftp://../filename)

Command Default

The default service ("DEFAULT") is used if no other services are configured.

Command Modes

Application configuration (config-app)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(15)T	The *location* argument was modified to accept an HTTPS server URL. The description of the *location* argument was modified to describe how to specify the location for built-in applications.
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to load a service on the gateway. A service is a standalone application, such as a VoiceXML document or a Tcl script.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows a debit application configured on the dial peer using insecure HTTP protocol displays a warning message:

```
Device(config)#application
Device(config-app)#service debit http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg
SECURITY WARNING - Module: CONFIG_VOICE, Command: service debit
http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: service debitcard configured with FTP/HTTP/TFTP URL protocol,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
Device(config-app-param)#
```

Examples

The following example shows a debitcard application configured on the dial peer.

```
Router(config)# application
Router(config-app)# service debitcard
tftp://server-1//tftpboot/scripts/app_debitcard.2.0.2.8.tcl
```

The following example shows the VoiceXML application myapp located on an HTTPS server configured on the dial peer.

```
Router(config)# application
Router(config-app)# service myapp https://myserver/myfile.vxml
```

The following example shows the auto-attendant (AA) service, called aa, which is a Tcl script embedded in the Cisco IOS software.

```
Router(config)# application
Router(config-app)# service queue builtin:app-b-acd
```

Related Commands

Command	Description
application (application configuration)	Configures an application on a dial peer.
call application alternate	Specifies an alternate application to use if the application that is configured in the dial peer fails.
call application voice	Defines the name of a voice application and specifies the location of the Tcl or VoiceXML document to load for this application.

service dsapp

To configure supplementary IP Centrex-like services for FXS phones on voice gateways to interwork with SIP-based softswitches, use the **service dsapp**command in the gateway-application configuration mode. Hookflash triggers a supplementary feature based on the current state of the call. To reset to the defaults, use the **no** form of this command.

service dsapp [*paramspace* **dialpeer** *dial-peer tag*] [*paramspace* **disc-toggle-time** *seconds*] [*paramspace* **callWaiting** *TRUEFALSE*] [*paramspace* **callConference** *TRUEFALSE*] [*paramspace* **blind-xfer-wait-time** *seconds*] [*paramspace* **callTransfer** *TRUEFALSE*]
no service dsapp

Syntax Description

paramspace	Defines a package or service on the gateway, the parameters in that package or service become available for configuration when you use this argument.
dialpeer *dial-peer tag*	(Optional) Specifies the fixed dialpeer used to setup the call to the SIP server (trunk) side.
disc-toggle-time *seconds*	(Optional) Specifies the seconds to wait before switching to a call on hold if the active call disconnects. You can specify a range between 10 and 30 seconds.
callWaiting *TRUE* | *FALSE*	Toggles support for call waiting.
callConference *TRUE* | *FALSE*	Toggles support for call conferencing used to establish two calls with a single connection such that all three parties can talk together.
blind-xfer-wait-time *seconds*	Specifies the seconds to wait before triggering a blind call transfer. You can specify a range between 0 and 10 seconds. If you specify 0 seconds, no blind transfer call occurs.
callTransfer *TRUE* | *FALSE*	Toggles support for call transfers.

Command Default

If no supplementary features are defined, the defaults are as follows:

- **dialpeer** : -1
- **disc-toggle-time** : 10 seconds
- **callWaiting** : TRUE (enabled)
- **callConference** : TRUE (enabled)
- **blind-xfer-wait-time** : 0 seconds
- **callTransfer** : TRUE (enabled)

Command Modes

Gateway-application configuration (config-app-param)

Command History

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

Usage Guidelines

Use the **service dsapp**command to configure supplementary Centrex-like features on FXS phones to interwork with SIP-based softswitches. Hookflash triggers supplementary features based on the current state of the call:

- Call Hold
- Call Waiting
- Call Transfer
- 3-Way Conference

Call Hold

Allows a call to be placed in a non-active state (with no media exchange). The table below summarizes the hookflash feature support for Call Hold.

Table 1: Call Hold Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash	Held call for remote party.	Second dial tone for FXS phone.
Call on hold	Hookflash	Active call.	FXS line connects to call.
Call on hold and active call	Hookflash	Active and held calls are swapped.	FXS line connects to previous held call.
	On hook	Active call is dropped.	Reminder ring on FXS line.
	Call on hold goes on hook	Call on hold is dropped.	None.
	Active call goes on hook	Active call is dropped	Silence.

Call Waiting

Allows a second call to be received while the phone is active with a call. The table below summarizes the hookflash feature support for Call Waiting.

Table 2: Call Waiting Hookflash Services

State	Action	Result	Response to FXS Line
Active call and waiting call	Hookflash.	Swap active call and waiting call.	FXS line connects to waiting call.
	Active call goes on hook.	Active call is disconnected.	Silence.
	Waiting call goes on hook.	Stay connected to active call.	None.
	On hook.	Active call is dropped.	Reminder ring on FXS line.

Call Transfer

With call transfer, you can do the following:

- Put an active call on hold while establishing a second call.
- Set up a call between two users
- Transfer calls by using these options
  - -Blind transfer
  - Semi-attended transfer
  - Attended transfer

The table below summarizes the hookflash feature support for Call Transfer.

Table 3: Call Transfer Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash.	Call is placed on hold.	Second dial tone.
Call on hold and outgoing dialed or alerting or active call	On hook.	Call on hold and active call.	
Call on hold and outgoing active call	Active call goes on hook.	Held call remains; active call dropped.	Silence.
Call on hold and outgoing active call	Call on hold goes on hook.	Active call remains; call on hold dropped.	None.
Call on hold and outgoing alerting call	Hookflash.	Active call dropped.	FXS line connects to previous held call.

3-Way Conference

Establishes two calls with a single connection, so that three parties can talk together. The table below summarizes the hookflash feature support for 3-way conferencing.

Table 4: 3-Way Conference Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash	Call on hold.	Second dial tone.
Call on hold and active call		Join call on hold and active call.	Media mixing of both calls.

Examples

Enabling the DSApp Service

You can configure DSApp services either to a specific dial-peer, or globally to all dial peers. The following example shows the configuration to enable DSApp on a specific dial peer:

```
Gateway#
```

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(conf-app)#

dial-peer voice 1000 pots
Gateway(config-app)#
service dsapp
```

The following example shows the configuration to enable DSApp globally on all dial peers:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)# global
Gateway(config-app-global)#
service default dsapp
```

Configuring Call Hold

The following example shows the configuration to enable the Call Hold feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service dsapp
Gateway
(config-app-param)#
param callHold TRUE
```

Configuring Call Waiting

The following example shows the configuration to enable the Call Waiting feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service

dsapp
Gateway
```

```
(config-app-param)#
param callWaiting TRUE
```

Configuring Call Transfer

The following example shows the configuration to enable the Call Transfer feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service dsapp
Gateway
(config-app-param)#
param callTransfer TRUE
```

Configuring 3-Way Conferencing

The following example shows the configuration to enable the 3-Way Conferencing feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service dsapp
Gateway
(config-app-param)#
param callConference TRUE
```

Configuring Disconnect Toggle Time

In this example, a disconnect toggle time is configured that specifies the amount of time in seconds the system should wait before committing the call transfer after the originating call is placed on hook.

```
Gateway#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#
application
Gateway(config-app)#
service dsapp
Gateway(config-app-param)#
param disc-toggle-time 10
```

Configuring Blind Transfer Wait Time

In this example, a blind transfer call wait time is configured that specifies the amount of time in seconds the system should wait before committing the call transfer, after the originating call is placed on hook.

```
Gateway#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#
application
Gateway(config-app)#
service dsapp
Gateway(config-app-param)#
param blind-xfer-wait-time 10
```

Configuring a Fixed Dial Peer Used for Outgoing Calls on SIP Trunk Side

In this example, a fixed dial peer is configured to set up a call to the SIP server (trunk) side.

```
Gateway#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#
application
Gateway(config-app)#
service dsapp
Gateway(config-app-param)#
param dialpeer 5000
```

Related Commands

Command	Description
offer call-hold	Specifies the method of call hold on the gateway.

service-flow primary upstream

To assign a quality of service (QoS) policy to the data traveling between the cable modem and the multiple service operator (MSO) cable modem termination system (CMTS), use the **service-flow primary upstream** command in interface configuration mode. To disable the QoS policy, use the **no** form of this command.

service-flow primary upstream
no service-flow primary upstream

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

This command is supported in the upstream direction only. Service flows are unidirectional.

Examples

The following example assigns a QoS policy to the data traveling between the cable modem and the MSO CMTS:

```
Router# configure terminal
Router(config)# interface Cable-Modem 0/2/0

Router(config-if)# service-flow primary upstream
```

service-map

To configure the HTTP application service map for the phone proxy instance, use the **service-map** command in phone proxy configuration mode. To remove the HTTP application service map, use the **no** form of the command.

service-map server-addr ipv4 *http-ipv4-address* **port** *http-server-port-number* **acc-addr ipv4** *access-ipv4-address***port** *access-port-number*
no service-map server-addr ipv4 *http-ipv4-address* **port** *http-server-port-number* **acc-addr ipv4** *access-ipv4-address***port** *access-port-number*

Syntax Description

http-ipv4-address	Specifies the IPv4 address of the HTTP server.
port *http-server-port-number*	The port number of the HTTP server. The range is 1 to 65535.
acc-addr ipv4 *access-ipv4-address*	Specifies the IPv4 address of the access side server.
port *access-port-number*	The port number of the access side server. The range is 1 to 65535.

Command Default

No HTTP application service map is configured.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

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

Usage Guidelines

Example

The following example shows how to configure an HTTP application service map for the phone proxy instance called “first-pp”:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# service-map server-addr ipv4 192.0.2.50 port 8080 acc-addr ipv4
 10.0.0.8 port 1234
```

service-relationship

To enter Annex G neighbor configuration mode and enable service relationships for the particular neighbor, use the **service-relationship** command in Annex G neighbor configuration mode. To exit this mode, use the **no** form of this command.

service-relationship
no service-relationship

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Annex G neighbor configuration (config-annexg-neigh)

Command History

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

Usage Guidelines

Service relationships are defined to be unidirectional. If a service relationship is established between border element A and border element B, A is entitled to send requests to B and to expect responses. For B to send requests to A and to expect responses, a second service relationship must be established. Repeat this command for each border-element neighbor that you configure.

Note The **no shutdown** command must be used to enable each service relationship.

Examples

The following example enables a service relationship on a border element:

```
Router(config-annexg-neigh)# service-relationship
```

Related Commands

Command	Description
access -policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry -interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time for which a border element attempts delivery.
shutdown	Enables or disables the border element.

service-type call-check

To identify preauthentication requests to the authentication, authorization, and accounting (AAA) server, use the **service-type call-check** command in AAA preauthentication configuration mode. To return this setting to the default, use the **no** form of this command.

service-type call-check
no service-type call-check

Syntax Description

This command has no arguments or keywords.

Command Default

The service type is not set to call-check.

Command Modes

AAA preauthentication configuration (config-preauth)

Command History

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

Usage Guidelines

Setting the service-type attribute to call-check causes preauthentication access requests to include this value, which allows AAA servers to distinguish preauthentication requests from other types of Access-Requests. This command has no effect on packets that are not of the preauthentication type.

Examples

The following example sets the RADIUS service-type attribute to call-check:

```
Router(config)# aaa preauth
Router(config-preauth)# service-type call-check
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.