

session through sgcp tse payload

- session, on page 3
- session group, on page 4
- session protocol (dial peer), on page 5
- session protocol (Voice over Frame Relay), on page 7
- session protocol aal2, on page 9
- session protocol multicast, on page 10
- session refresh, on page 11
- session start, on page 12
- session target (MMoIP dial peer), on page 14
- session target (POTS dial peer), on page 17
- session target (VoATM dial peer), on page 18
- session target (VoFR dial peer), on page 21
- session target (VoIP dial peer), on page 23
- session target, on page 28
- session transport, on page 29
- session transport (H.323 voice-service), on page 31
- session transport (SIP), on page 32
- session-set, on page 34
- session-timeout, on page 35
- set, on page 36
- set http client cache stale, on page 38
- set pstn-cause, on page 39
- set sip-status, on page 42
- settle-call, on page 45
- settlement, on page 46
- settlement roam-pattern, on page 48
- sgcp, on page 49
- sgcp call-agent, on page 51
- sgcp graceful-shutdown, on page 53
- sgcp max-waiting-delay, on page 55
- sgcp modem passthru, on page 57
- sgcp quarantine-buffer disable, on page 59
- sgcp request retries, on page 61

- sgcp request timeout, on page 63
- sgcp restart, on page 65
- sgcp retransmit timer, on page 67
- sgcp timer, on page 69
- sgcp tse payload, on page 71
- source filter, on page 73

session

To associate a transport session with a specified session group, use the **session** command in backhaul session manager configuration mode. To delete the session, use the **no** form of this command.

session group *group-name remote-ip remote-port local-ip local-port priority*
no session group *group-name remote-ip remote-port local-ip local-port priority*

Syntax Description

group -name	Session-group name.
remote -ip	Remote IP address.
remote -port	Remote port number. Range is from 1024 to 9999.
local -ip	Local IP address.
local -port	Local port number. Range is from 1024 to 9999.
priority	Priority of the session-group. Range is from 0 to 9999; 0 is the highest priority.

Command Default

No default behavior or values

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

It is assumed that the server is located on a remote machine.

Examples

The following example associates a transport session with the session group "group5" and specifies the parameters:

```
Router(config-bsm)# session group
 group5
 172.13.2.72 5555 172.18.72.198 5555 1
```

session group

To associate a transport session with a specified session group, use the **session group**command in backhaul session-manager configuration mode. To delete the session, use the **no** form of this command.

session group *group-name remote-ip remote-port local-ip local-port priority*
no session group *group-name remote-ip remote-port local-ip local-port priority*

Syntax Description

group -name	Session-group name.
remote -ip	Remote IP address.
remote -port	Remote port number. Range is from 1024 to 9999.
local -ip	Local IP address.
local -port	Local port number. Range is from 1024 to 9999.
priority	Priority of the session group. Range is from 0 to 9999; 0 has the highest priority.

Command Default

No default behavior or values.

Command Modes

Backhaul session-manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.

Usage Guidelines

The server is assumed to be located on a remote machine.

Examples

The following example associates a transport session with the session group named "group5" and specifies the keywords described above:

```
session group
 group5
 172.16.2.72 5555 192.168.72.198 5555 1
```

session protocol (dial peer)

To specify a session protocol for calls between local and remote routers using the packet network, use the **session protocol** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**aal2-trunk** | **cisco** | **sipv2** | **smtp**}
no session protocol

Syntax Description

aal2 -trunk	Dial peer uses ATM adaptation layer 2 (AAL2) nonswitched trunk session protocol.
cisco	Dial peer uses the proprietary Cisco VoIP session protocol.
sipv2	Dial peer uses the Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP). Use this keyword with the SIP option.
smtp	Dial peer uses Simple Mail Transfer Protocol (SMTP) session protocol.

Command Default

No default behaviors or values

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP peers on the Cisco 3600 series.
12.0(3)XG	This command was modified to support VoFR) dial peers.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300.
12.1(1)XA	This command was implemented for VoATM dial peers on the Cisco MC3810. The **aal2-trunk** keyword was added.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **sipv2** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release. The **aal2-trunk** and **smtp** keywords are not supported on the Cisco 7200 series in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

The **cisco**keyword is applicable only to VoIP on the Cisco 1750, Cisco 1751, Cisco 3600 series, and Cisco 7200 series routers.

The **aal2-trunk** keyword is applicable only to VoATM on the Cisco 7200 series router.

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

Examples

The following example shows that AAL2 trunking has been configured as the session protocol:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example shows that Cisco session protocol has been configured as the session protocol:

```
dial-peer voice 20 voip
 session protocol cisco
```

The following example shows that a VoIP dial peer for SIP has been configured as the session protocol for VoIP call signaling:

```
dial-peer voice 102 voip
 session protocol sipv2
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.
session target (VoIP)	Configures a network-specific address for a dial peer.

session protocol (Voice over Frame Relay)

To establish a Voice over Frame Relay protocol for calls between the local and remote routers via the packet network, use the **session protocol** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**cisco-switched** | **frf11-trunk**}
no session protocol

Syntax Description

cisco -switched	Proprietary Cisco VoFR session protocol. (This is the only valid session protocol for the Cisco 7200 series.)
frf11 -trunk	FRF.11 session protocol.

Command Default

cisco-switched

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP.
12.0(3)XG	This command was modified to support VoFR on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.0(4)T	The **cisco-switched** and **frf11-trunk** keywords were added for VoFR dial peers.

Usage Guidelines

For Cisco-to-Cisco dial peer connections, Cisco recommends that you use the default session protocol because of the advantages it offers over a pure FRF.11 implementation. When connecting to FRF.11-compliant equipment from other vendors, use the FRF.11session protocol.

Note When using the FRF.11 session protocol, you must also use the **called-number** command.

Examples

The following example configures the FRF.11 session protocol for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 session protocol frf11-trunk
 called-number 5552150
```

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.

Command	Description
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.
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.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
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.

session protocol aal2

To enter voice-service-session configuration mode and specify ATM adaptation layer 2 (AAL2) trunking, use the **session protocol aal2**command in voice-service configuration mode.

session protocol aal2

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

This command applies to VoATM on theCisco 7200 series router.

In the voice-service-session configuration mode for AAL2, you can configure only AAL2 features, such as call admission control and subcell multiplexing.

Examples

The following example accesses voice-service-session configuration mode, beginning in global configuration mode:

```
voice service voatm
 session protocol aal2
```

session protocol multicast

To set the session protocol as multicast, use the **session protocol multicast** command in dial-peer configuration mode. To reset to the default protocol, use the **no** version of this command.

session protocol multicast
no session protocol multicast

Syntax Description

This command has no arguments or keywords.

Command Default

Default session protocol: Cisco.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.1(2)XH	This command was introduced for the Cisco Hoot and Holler over IP application on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(8)T	This command was implemented on the Cisco 1750 and Cisco 1751.

Usage Guidelines

Use this command for voice conferencing in a hoot and holler networking implementation. This command allows more than two ports to join the same session simultaneously.

Examples

The following example shows the use of the **session protocol multicast** dial-peer configuration command in context with its accompanying commands:

```
dial-peer voice 111 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:237.111.0.111:22222
 ip precedence 5
 codec g711ulaw
```

Related Commands

Command	Description
session target ipv4	Assigns the session target for voice-multicasting dial peers.

session refresh

To enable SIP session refresh globally, use the **session refresh**command in SIP configuration mode. To disable the session refresh, use the **no** form of this command.

session refresh
no session refresh

Syntax Description

This command has no arguments or keywords.

Command Default

No session refresh

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the SIP **session refresh**command to send the session refresh request.

Examples

The following example sets the session refresh under SIP configuration mode:

```
Router(conf-serv-sip)# Session refresh
```

Related Commands

Command	Description
voice-class sip session refresh	Enables session refresh at dial-peer level.

session start

To start a new instance (session) of a Tcl IVR 2.0 application, use the **session start** command in application configuration mode. To stop the session and remove the configuration, use the **no** form of this command.

session start *instance-name application-name*
no session start *instance-name*

Syntax Description

instance-name	Alphanumeric label that uniquely identifies this application instance.
application-name	Name of the Tcl application. This is the name of the application that was assigned with the **service** command.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application session start** (global configuration) command.

Usage Guidelines

- This command starts a new session, or instance, of a Tcl IVR 2.0 application. It cannot start a session for a VoiceXML application because Cisco IOS software cannot start a VoiceXML application without an active call leg.
- You can start an application instance only after the Tcl application is loaded onto the gateway with the **service** command.
- If this command is used, the session restarts if the gateway reboots.
- If the application session stops running, it does not restart unless the gateway reboots. A Tcl script might intentionally stop running by executing a "call close" command for example, or it might fail because of a script error.
- You can start multiple instances of the same application by using different instance names.

Examples

The following example starts a session named my_instance for the application named demo:

```
application
session start my_instance demo
```

The following example starts another session for the application named demo:

```
application
session start my_instance2 demo
```

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a Tcl IVR 2.0 application.
service	Loads a specific, standalone application on a dial peer.
show call application services registry	Displays a one-line summary of all registered services.
show call application sessions	Displays summary or detailed information about voice application sessions.

session target (MMoIP dial peer)

To designate an e-mail address to receive T.37 store-and-forward fax calls from a Multimedia Mail over IP (MMoIP) dial peer, use the **session target**command indial peer configuration mode. To remove the target address, use the **no** form of this command.

session target mailto: {*name* | **d** | **m** | **e**} [**@***domain-name*]
no session target

Syntax Description

mailto:	Matching calls are passed to the network using Simple Mail Transfer Protocol (SMTP) or Extended Simple Mail Transfer Protocol (ESMTP).
name	String that can be an e-mail address, name, or mailing list alias.
d	Macro that is replaced by the destination pattern of the gateway access number, which is the called number or dialed number identification service (DNIS) number.
m	Macro that is replaced by the redirecting dialed number (RDNIS) if present; otherwise, it is replaced by the gateway access number (DNIS). This macro requires use of the fax detection interactive voice response (IVR) application. **Note** Other strings can be passed to mailto in place of **m** if you modify the fax detection application Tool Command Language (Tcl) script or VoiceXML document. For more information, see to the readme file that came with the Tcl script or the *Cisco VoiceXML Programmer's Guide.*
e	Macro that is replaced by the DNIS, the RDNIS, or a string that represents a valid e-mail address, as specified by the *cisco-mailtoaddress* variable in the transfer tag of the VoiceXML fax detection document. By default, if the *cisco-mailtoaddress* variable is not specified in the fax detection document, the DNIS is mapped to **e**. If **e** is not specified for the **session target mailto** command in the MMoIP dial peer, but the *cisco-mailtoaddres* s variable is specified in the transfer tag of the fax detection document, then whatever is specified in the MMoIP dial peer takes precedence; the *cisco-mailtoaddress* variable is ignored. **Note** If a domain name is configured with this command, the VoiceXML document should pass only the username portion of the e-mail address and not the domain. If the domain name is passed from *cisco-mailtoaddress,* the **session target mailto** command should specify only **e**.
@ *domain-name*	(Optional) String that contains the domain name to be associated with the target address, preceded by the at sign (@); for example, *@mycompany.com* .

Command Default

No default behavior or values

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(4)T	This command was modified to support store-and-forward fax.
12.1(5)XM1	The **m**keyword was introduced for the fax detection feature on the Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	The **e**keyword was introduced for VoiceXML fax detection on the Cisco AS5300.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to deliver e-mail to one recipient by specifying one e-mail name, or to deliver e-mail to multiple recipients by specifying an e-mail alias as the *name* argument and having that alias expanded by the mailer.

Use the **m** macro to include the redirecting dialed number (RDNIS) as part of the e-mail name when using the fax detection IVR application. If **m** is specified and RDNIS is not present in the call information, the access number of the gateway (the dialed number, or DNIS) is used instead. For example, if the calling party originally dialed 6015550111 to send a fax, and the call was redirected (forwarded on busy or no answer) to 6015550122 (the gateway), the RDNIS is 6015550111, and the DNIS is 6015550122.

Use the **e** macro to map the *cisco-mailtoaddress* variable in the VoiceXML fax detection document to the username portion of the e-mail address when sending a fax. If the VoiceXML document does not specify the *cisco-mailtoaddress* variable in the transfer tag, the application maps the DNIS to the e-mail address username.

Examples

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target mailto:marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running the sendmail application, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085550112@sj-offramp.example.com
```

The following example uses the fax detection IVR application. Here, the **session target (MMoIP dial peer)**commandforwards fax calls to an e-mail account that uses the Redirected Dialed Number Identification Service (RDNIS) as part of its address. In this example, the calling party originally dialed 6015550111 to send a fax, and the call was forwarded (on busy or no answer) to 6015550122, which is the incoming number for the gateway being configured. The RDNIS is 6015550111, and the dialed number (DNIS) is 6015550122. When faxes are forwarded from the gateway, the session target in the example is expanded to 6015550111@mail-server.unified-messages.com.

```
dial-peer voice 4 mmoip
 session target mailto:$m$@mail-server.unified-messages.com
```

The following examples configure a session target for a VoiceXML fax detection application. In this example, the VoiceXML document passes just the username portion of the e-mail address, for example, "johnd":

```
dial-peer voice 4 mmoip
 session target mailto:$e$@cisco.com
```

In this example, the VoiceXML document passes the complete e-mail address including domain name, for example, "johnd@cisco.com":

```
dial-peer voice 5 mmoip
 session target mailto:$e$
```

Related Commands

Command	Description
destination-pattern	Specifies either the partial or full E.164 telephone number (depending on your dial plan) used to match the dial peer.
dial-peer voice	Enters dial-peer configuration mode and defines a dial peer.

session target (POTS dial peer)

To designate loopback calls from a POTS dial peer, use the **session target** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session target {**loopback:compressed** | **loopback:uncompressed**}
no session target

Syntax Description

loopback:compressed	All voice data is looped back in compressed mode to the source.
loopback:uncompressed	All voice data is looped back in uncompressed mode to the source.

Command Default

No loopback calls are designated.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and is supported on the Cisco AS5200, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Use this command to test the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

Examples

The following example loops back the traffic from the dial peer in compressed mode:

```
dial-peer voice 10 pots
 session target loopback:compressed
```

Related Commands

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

session target (VoATM dial peer)

To specify a network-specific address for a specified VoATM dial peer, use the **session target** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 3600 Series Routers
session target *interface* **pvc** {*name* | *vpi*/*vcivci*}
no session target

Cisco 7200 Series Routers
session target atm *slot*/*port* **pvc** {*word* | *vpi*/*vcivci*} *cid*
no session target

Syntax Description

serial	Serial interface for the dial-peer address.
atm	ATM interface. The only valid number is 0.
interface	Interface type and interface number on the router.
slot / *port*	Slot and port numbers for the dial-peer address.
pvc	Specific ATM permanent virtual circuit (PVC) for this dial peer.
name	PVC name.
word	(Optional) Name that identifies the PVC. The argument can identify the PVC if a word identifier was assigned when the PVC was created.
vpi / *vci*	ATM network virtual path identifier (VPI) and virtual channel identifier (VCI) of this PVC. Values are as follows: • Cisco 3600 series with Multiport T1/E1 ATM network module with inverse multiplexing over ATM (IMA): *vpi*range is from 0 to 5; *vci* range is from 1 to 255. • OC3 ATM network module: *vpi* range is from 0 to 15; *vci* range is from 1 to 1023.
vci	ATM network virtual channel identifier (VCI) of this PVC.
cid	ATM network channel identifier (CID) of this PVC. Range is from 8 to 255.

Command Default

Command is enabled with no IP address or domain name defined.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was modified to support VoATM, VoHDLC, and POTS dial peers. The command was implemented on the Cisco MC3810.

Release	Modification
12.0(3)XG	This command was modified to support VoFR dial peers. The command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was modified to support VoATM and VoIP dial peers. The command was implemented on the Cisco 3600 series and the Cisco MC3810. Support for VoHDLC was removed.
12.1(1)XA	This command was modified to provide enhanced support for VoATM dial peers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

Use the **session target**command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol that you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

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

You must enter the session protocol aal2-trunk dial-peer configuration command before you can specify a CID for a dial peer for VoATM on the Cisco 7200 series router.



Note This command does not apply to POTS dial peers.

Examples

The following example configures a session target for VoATM. The session target is sent to ATM interface 0 for a PVC with a VCI of 20.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm0 pvc 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085550112@sj-offramp.example.com
```

The following example configures a session target for VoATM. The session target is sent to ATM interface 0, and is for a PVC with a VPI/VCI of 1/100.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm1/0 pvc 1/100
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between local and remote routers via the packet network.
session target	Configures a network-specific address for a dial peer.
session target loopback	Tests the voice transmission path of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoFR dial peer)

To specify a network-specific address for a specified VoFR dial peer, use the **session target** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 2600 Series and Cisco 3600 Series Routers
session target *interface dlci* [*cid*]
no session target

Cisco 7200 Series Routers
session target interface dlci
no session target

Syntax Description

interface	Serial interface and interface number (slot number and port number) associated with this dial peer. For the range of valid interface numbers for the selected interface type, enter a **?** character after the interface type.
dlci	Data link connection identifier for this dial peer. Range is from 16 to 1007.
cid	(Optional) DLCI subchannel to be used for data on FRF.11 calls. A CID must be specified only when the session protocol is **frf11-trunk**. When the session protocol is **cisco-switched**, the CID is dynamically allocated. Range is from 4 to 255. **Note** By default, CID 4 is used for data; CID 5 is used for call-control. We recommend that you select CID values between 6 and 63 for voice traffic. If the CID is greater than 63, the FRF.11 header contains an extra byte of data.

Command Default

The default for this command is enabled with no IP address or domain name defined.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was implemented for VoFR, VoHDLC, and POTS dial peers on the Cisco MC3810.
12.0(3)XG	This command was implemented for VoFR dial peers on the Cisco 2600 series and Cisco 3600 series. The *cid* option was added.
12.0(4)T	This command was integrated into Cisco IOS Release12.0(4)T and implemented for VoFR and POTS dial peers on the Cisco 7200 series.

Usage Guidelines

Use the **session target**command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

For VoFR dial peers, the *cid* option is not allowed when the **cisco-switched**option for the **session protocol** command is used.

Examples

The following example configures serial interface 1/0, DLCI 100 as the session target for Voice over Frame Relay dial peer 200 (an FRF.11 dial peer) using the FRF.11 session protocol:

```
dial-peer voice 200 vofr
 destination-pattern 13102221111
 called-number 5552150
 session protocol frf11-trunk
 session target serial 1/0 100 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between the local and the remote routers via the packet network.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoIP dial peer)

To designate a network-specific address to receive calls from a VoIP or VoIPv6 dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1751, Cisco 3725, Cisco 3745, and Cisco AS5300
session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **sip-server** | **registrar**} [**:***port*]
no session target

Cisco 2600 Series, Cisco 3600 Series, Cisco AS5350, Cisco AS5400, and Cisco AS5850
session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **settlement** *provider-number* | **sip-server** | **registrar**} [**:***port*]
no session target

Syntax Description

dhcp	Configures the router to obtain the session target via DHCP. **Note** The **dhcp** option can be made available only if the Session Initiation Protocol (SIP) is used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.
ipv4: *destination -address*	Configures the IP address of the dial peer to receive calls. The colon is required.
ipv6: [*destination-address*]	Configures the IPv6 address of the dial peer to receive calls. Square brackets must be entered around the IPv6 address. The colon is required.
dns:[s] *hostname*	Configures the host device housing the domain name system (DNS) server that resolves the name of the dial peer to receive calls. The colon is required. Use one of the following macros with this keyword when defining the session target for VoIP peers: • **s.** --(Optional) Source destination pattern is used as part of the domain name. • **d.** --(Optional) Destination number is used as part of the domain name. • **e.** --(Optional) Digits in the called number are reversed and periods are added between the digits of the called number. The resulting string is used as part of the domain name. • **u.** --(Optional) Unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name. • *hostname* --String that contains the complete hostname to be associated with the target address; for example, serverA.example1.com.
enum: *table -num*	Configures ENUM search table number. Range is from 1 to 15. The colon is required.

loopback:rtp	Configures all voice data to loop back to the source. The colon is required.
ras	Configures the registration, admission, and status (RAS) signaling function protocol. A gatekeeper is consulted to translate the E.164 address into an IP address.
sip -server	Configures the global SIP server is the destination for calls from the dial peer.
: *port*	(Optional) Port number for the dial-peer address. The colon is required.
settlement *provider -number*	Configures the settlement server as the target to resolve the terminating gateway address. • The *provider-number* argument specifies the provider IP address.
registrar	Specifies to route the call to the registrar end point. • The **registrar** keyword is available only for SIP dial peers.

Command Default

No IP address or domain name is defined.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was modified. This command was implemented on the Cisco AS5300. The **ras** keyword was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **settlement** and **sip-server** keywords were added.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **enum** keyword was added.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **dhcp** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Release	Modification
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **session target** command to specify a network-specific destination for a dial peer to receive calls from the current dial peer. You can select an option to define a network-specific address or domain name as a target, or you can select one of several methods to automatically determine the destination for calls from the current dial peer.

Use the **session target dns** command with or without the specified macros. Using the optional macros can reduce the number of VoIP dial-peer session targets that you must configure if you have groups of numbers associated with a particular router.

The **session target enum** command instructs the dial peer to use a table of translation rules to convert the dialed number identification service (DNIS) number into a number in E.164 format. This translated number is sent to a DNS server that contains a collection of URLs. These URLs identify each user as a destination for a call and may represent various access services, such as SIP, H.323, telephone, fax, e-mail, instant messaging, and personal web pages. Before assigning the session target to the dial peer, configure an ENUM match table with the translation rules using the **voice enum-match-table**command in global configuration mode. The table is identified in the **session target enum** command with the *table-num* argument.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin.

Use the **session target dhcp** command to specify that the session target host is obtained via DHCP. The **dhcp** option can be made available only if the SIP is being used as the session protocol. To enable SIP, use the **session protocol**(dial peer) command.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command.

For the **session target settlement** *provider-number* command, when the VoIP dial peers are configured for a settlement server, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Use the **session target sip-server** command to name the global SIP server interface as the destination for calls from the dial peer. You must first define the SIP server interface by using the **sip-server** command in SIP user-agent (UA) configuration mode. Then you can enter the **session target sip-server** option for each dial peer instead of having to enter the entire IP address for the SIP server interface under each dial peer.

After the SIP endpoints are registered with the SIP registrar in the hosted unified communications (UC), you can use the **session target registrar** command to route the call automatically to the registrar end point. You must configure the **session target** command on a dial pointing towards the end point.

Examples

The following example shows how to create a session target using DNS for a host named "voicerouter" in the domain example.com:

```
dial-peer voice 10 voip
 session target dns:voicerouter.example.com
```

The following example shows how to create a session target using DNS with the optional **u**. macro. In this example, the destination pattern ends with four periods (.) to allow for any four-digit extension that has the leading number 1310555. The optional **u**. macro directs the gateway to use the

unmatched portion of the dialed number--in this case, the four-digit extension--to identify a dial peer. The domain is "example.com."

```
dial-peer voice 10 voip
 destination-pattern 1310555....
 session target dns:$u$.example.com
```

The following example shows how to create a session target using DNS, with the optional **d**. macro. In this example, the destination pattern has been configured to 13105551111. The optional macro **d**. directs the gateway to use the destination pattern to identify a dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 13105551111
 session target dns:$d$.example.com
```

The following example shows how to create a session target using DNS, with the optional **e**. macro. In this example, the destination pattern has been configured to 12345. The optional macro **e**. directs the gateway to do the following: reverse the digits in the destination pattern, add periods between the digits, and use this reverse-exploded destination pattern to identify the dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.example.com
```

The following example shows how to create a session target using an ENUM match table. It indicates that calls made using dial peer 101 should use the preferential order of rules in enum match table 3:

```
dial-peer voice 101 voip
 session target enum:3
```

The following example shows how to create a session target using DHCP:

```
dial-peer voice 1 voip
session protocol sipv2
voice-class sip outbound-proxy dhcp
session target dhcp
```

The following example shows how to create a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13105551111
 session target ras
```

The following example shows how to create a session target using settlement:

```
dial-peer voice 24 voip
 session target settlement:0
```

The following example shows how to create a session target using IPv6 for a host at 2001:10:10:10:10:10:10:230a:5090:

```
dial-peer voice 4 voip
destination-pattern 5000110011
session protocol sipv2
```

```
session target ipv6:[2001:0DB8:10:10:10:10:10:230a]:5090
codec g711ulaw
```

The following example shows how to configure Cisco Unified Border Element (UBE) to route a call to the registering end point:

```
dial-peer voice 4 voip
session target registrar
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dial -peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.
session protocol (dial peer)	Specifies a session protocol for calls between local and remote routers using the packet network dial peer configuration mode.
settle -call	Specifies that settlement is to be used for the specified dial peer, regardless of the session target type.
sip -server	Defines a network address for the SIP server interface.
voice enum -match-table	Initiates the ENUM match table definition.

session target

To configure the Session Initiation Protocol (SIP) Uniform Resource Locator (URI) as the session target for a dial peer, use the **session target sip-uri** command in dial peer voice configuration mode. To disable this configuration, use the **no** form of the command.

session target
no session target

Command Default

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure the SIP URI as the session target for a dial peer using the **session target sip-uri** command:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# destination uri mydesturi
Device(config-dial-peer)# session target sip-uri
Device(config-dial-peer)# end
```

session transport

To configure a VoIP dial peer to use TCP or User Datagram Protocol (UDP) as the underlying transport layer protocol for Session Initiation Protocol (SIP) messages, use the **session transport** command in dial-peer configuration mode. To reset to the **system** default keyword, use the **no** form of this command.

session transport {**system** | **tcp** [**tls**] | **udp**}
no session transport {**system** | **tcp** [**tls**] | **udp**}

Syntax Description

system	The SIP dial peer defers to the voice service VoIP session transport.
tcp	The SIP dial peer uses the TCP transport layer protocol.
tls	(Optional) The SIP dial peer uses Transport Layer Security (TLS) over the TCP transport layer protocol.
udp	The SIP dial peer uses the UDP transport layer protocol. This is the default.

Command Default

UDP

Note The transport protocol specified with the **transport**command **must match**the one specified with this command.

Command Modes

Dial-peer configuration.

Voice class tenant.

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(6)T	The optional tls keyword was added to the command.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the show **sip-ua** status command to ensure that the transport protocol that you set using this command matches the protocol set using the **transport** command. The **transport** command is used in dial-peer configuration mode to specify the SIP transport method, either UDP, TCP, or TLS over TCP.

Examples

The following example shows a VoIP dial peer configured to use TCP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport tcp
```

The following example shows a VoIP dial peer configured to use TLS over TCP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport tcp tls
```

The following example shows a VoIP dial peer configured to use UDP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport udp
```

Related Commands

Command	Description
show sip-ua status	Displays the status of SIP call service on a SIP gateway.
transport	Configures the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

session transport (H.323 voice-service)

To configure the underlying transport layer protocol for H.323 messages to be used across all VoIP dial peers, use the **session transport** command in H.323 voice service configuration mode. To reset the default value, use the **no** form of this command.

session transport {**udp** | **tcp** [**calls-per-connection** *value*]}
no session transport

Syntax Description

udp	Configures the H.323 dial peer to use the UDP transport layer protocol.
tcp	Configures the H.323 dial peer to use the TCP transport layer protocol. This is the default.
calls-per-connection	Configures the number of calls multiplexed into a single TCP connection.
value	The number of calls. The range is from 1 to 9999. The default is 5.

Command Default

TCP is the default session transport protocol; the default **calls-per-connection** value is 5.

Command Modes

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

Command History

Release	Modification
12.2(1)T	This command was introduced for session initiation protocol (SIP) dial peers.
12.2(2)XA	This command was modified to include support for H323 dial peers and to include the **calls-per-connection** keyword.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows a dial peer configured to use the UDP transport layer protocol.

```
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# session transport udp
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

session transport (SIP)

To configure the underlying transport layer protocol for SIP messages to TCP, transport layer security over TCP (TLS over TCP), or User Datagram Protocol (UDP), use the session transport command in SIP configuration mode. To reset the value of this command to the default, use the **no** form of this command.

session transport {**udp** | **tcp** [**tls**]}
no session transport {**udp** | **tcp** [**tls**]}

Syntax Description

udp	Configure SIP messages to use the UDP transport layer protocol. This is the default.
tcp	Configure SIP messages to use the TCP transport layer protocol.
tls	(Optional) Configure SIP messages to use the TLS over TCP transport layer protocol.

Command Default

The default for the command is UDP.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(2)XB	This command was introduced in SIP configuration mode.
12.2(2)XB2	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco 3700 series. Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms were not supported in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.
12.4(6)T	The optional tls keyword was added to the command.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **show sip-ua status** command to verify that the transport protocol set with the **session transport**command matches the protocol set using the **transport** command in SIP user agent configuration mode.

Examples

The following example configures the underlying transport layer protocol for SIP messages to UDP:

```
voice service voip
 sip
 session transport udp
```

The following example configures the underlying transport layer protocol for SIP messages to TCP:

```
voice service voip
 sip
 session transport tcp
```

The following example configures the underlying transport layer protocol for SIP messages to TLS over TCP:

```
voice service voip
 sip
 session transport tcp tls
```

Related Commands

Command	Description
show sip-ua status	Displays the status of SIP call service on a SIP gateway.
transport	Configures the SIP gateway for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

session-set

To create a Signlaing System 7 (SS7)-link-to-SS7-session-set association or to associate an SS7 link with an SS7 session set on the Cisco 2600-based Signaling Link Terminal (SLT), enter the session-set command in global configuration mode. To remove the link from its current SS7 session set and to add it to SS7 session set 0 (the default), use the no form of this command.

session-set *session-set-id*
no session-set

Syntax Description

session -set-id	SS7 session ID. Valid values are 0 and 1. Default is 0.

Command Default

SS7 session set 0

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced on the Cisco 2600-based SLT.

Usage Guidelines

On Cisco AS5350 and Cisco AS5400 platforms, the **channel-id** command is used to create an SS7-link-to-SS7-session-set association on the Cisco SLT. The Cisco 26xx platforms do not support the **channel-id** command, so channel IDs on the Cisco 26xx-based SLT are implicitly assigned on the basis of the slot location of the WAN interface card (WIC) and the channel group ID used to create the SS7 link.

If this command is omitted, the link is implicitly added to the SS7 session set 0, which is the default.

Examples

The following example shows how the **session-set** command is used to add the associated SS7 link to an SS7 session set:

```
session-set 1
```

The following example shows how the no session-set command is used to remove the link from its current SS7 session set and add it to SS7 session set 0, which is the default:

```
no session-set
```

Related Commands

Command	Description
channel-id	Assigns a session channel ID to a Signaling System 7 (SS7) serial link or assign an SS7 link to an SS7 session set on a Cisco AS5350 or Cisco AS5400.

session-timeout

To specify the maximum amount of time for which a TFTP session can remain open, use the **session-timeout** command in phone proxy configuration mode. To remove the timeout period of a TFTP session, use the **no** form of the command.

session-timeout *seconds*
no session-timeout

Syntax Description

seconds	Maximum length of a TFTP session in seconds. The range is from 60 to 6000. The default is 180 seconds.

Command Default

The session timeout is 180 seconds.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

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

Usage Guidelines

Example

The following example shows how to specify a timeout period for a TFTP session of 200 seconds:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# session-timeout 200
```

set

To create a fault-tolerant or nonfault-tolerant session set with the client or server option, use the **set** command in backhaul session-manager configuration mode. To delete the set, use the **no** form of this command.

set *set-name* {**client** | **server**} {**ft** | **nft**}
no set *set-name* {**client** | **server**} {**ft** | **nft**}

Syntax Description

set-name	Session-set name.
client	The session set operates as a client. Select this option for signaling backhaul.
server	The session set operates as a server.
ft	Fault-tolerant operation. Select fault-tolerant if this session set can contain more than one session group, with each session group connecting the gateway to a different Cisco VSC3000. Fault-tolerance allows the system to operate properly if a session group in the session set fails.
nft	Non-fault-tolerant operation. Select non-fault-tolerant if this session set contains only one session group (which connects the gateway to a single Cisco VSC3000).

Command Default

No default behavior or values

Command Modes

Backhaul session manager configuration (config-bsm)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Multiple session groups can be associated with a session set.

For signaling backhaul, session sets should be configured to operate as clients.

A session set cannot be deleted unless all session groups associated with the session set are deleted first.

Examples

The following example sets the client set named "set1" as fault-tolerant:

```
Router(config-bsm)# set set1 client ft
```

set http client cache stale

To set the status of all entries in the HTTP client cache to stale, use the **set http client cache stale** command in global configuration mode.

set http client cache stale

Syntax Description

This command has no arguments or keywords.

Command Default

Entries in the HTTP client cache are not marked stale manually.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	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 force the HTTP client to check with the server to see if an updated version of the file exists when any cached entries are requested by the VoiceXML application. If the router is in nonstreaming mode, a conditional reload is sent to the HTTP server. If the router is in streaming mode, an unconditional reload is sent for the refresh. Regardless of which mode the router is in, the VoiceXML application is guaranteed to receive the most up-to-date file when you use the **set http client cache stale** command.

The **show http client cache** command shows a pound sign (#) next to the age of entries that are marked stale manually.

Examples

The following example sets the status of all entries in the HTTP client cache to stale:

```
Router# set http client cache stale
```

Related Commands

Command	Description
show http client cache	Displays information about the entries contained in the HTTP client cache.

set pstn-cause

To map an incoming PSTN cause code to a Session Initiation Protocol (SIP) error status code, use the **set pstn-cause**command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

set pstn-cause *value* **sip-status** *value*
no set pstn-cause

Syntax Description

pstn -cause *value*	PSTN cause code. Range is from 1 to 127
sip -status *value*	SIP status code that is to correspond with the PSTN cause code. Range is from 400 to 699.

Command Default

The default mappings defined in the following table are used:

Table 1: Default PSTN Cause Codes Mapped to SIP Events

PSTN Cause Code	Description	SIP Event
1	Unallocated number	404 Not found
2	No route to specified transit network	404 Not found
3	No route to destination	404 Not found
17	User busy	486 Busy here
18	No user responding	480 Temporarily unavailable
19	No answer from the user	
20	Subscriber absent	
21	Call rejected	403 Forbidden
22	Number changed	410 Gone
26	Non-selected user clearing	404 Not found
27	Destination out of order	404 Not found
28	Address incomplete	484 Address incomplete
29	Facility rejected	501 Not implemented
31	Normal, unspecified	404 Not found
34	No circuit available	503 Service unavailable
38	Network out of order	503 Service unavailable
41	Temporary failure	503 Service unavailable

PSTN Cause Code	Description	SIP Event
42	Switching equipment congestion	503 Service unavailable
47	Resource unavailable	503 Service unavailable
55	Incoming class barred within the Closed User Group (CUG)	403 Forbidden
57	Bearer capability not authorized	403 Forbidden
58	Bearer capability not currently available	501 Not implemented
65	Bearer capability not implemented	501 Not implemented
79	Service or option not implemented	501 Not implemented
87	User not member of the Closed User Group (CUG)	503 Service unavailable
88	Incompatible destination	400 Bad request
95	Invalid message	400 Bad request
102	Recover on Expires timeout	408 Request timeout
111	Protocol error	400 Bad request
Any code other than those listed above	500 Internal server error	

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for on the Cisco AS5300 Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

A PSTN cause code can be mapped only to one SIP status code at a time.

Examples

The following example maps a SIP status code to correspond to a PSTN cause code:

```
Router(config)# sip-ua
Router(config-sip-ua)# set pstn-cause 111 sip-status 400
Router(config-sip-ua)# exit
```

Related Commands

Command	Description
set sip -status	Sets an incoming SIP error status code to a PSTN release cause code.

set sip-status

To map an incoming Session Initiation Protocol (SIP) error status code to a PSTN cause code, use the **set sip-status**command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

set sip-status *value* **pstn-cause** *value*
no set sip-status

Syntax Description

sip -status *value*	SIP status code. Range is from 400 to 699.
pstn -cause *value*	PSTN cause code that is to correspond with the SIP status code. Range is from 1 to 127.

Command Default

The default mappings defined in the table below are used:

Table 2: Default SIP Events Mapped to PSTN Cause Codes

SIP Event	PSTN Cause Code	Description
400 Bad request	127	Interworking, unspecified
401 Unauthorized	57	Bearer capability not authorized
402 Payment required	21	Call rejected
403 Forbidden	57	Bearer capability not authorized
404 Not found	1	Unallocated number
405 Method not allowed	127	Interworking, unspecified
406 Not acceptable		
407 Proxy authentication required	21	Call rejected
408 Request timeout	102	Recover on Expires timeout
409 Conflict	41	Temporary failure
410 Gone	1	Unallocated number
411 Length required	127	Interworking, unspecified
413 Request entity too long		
414 Request URI (URL) too long		
415 Unsupported media type	79	Service or option not available
420 Bad extension	127	Interworking, unspecified
480 Temporarily unavailable	18	No user response

SIP Event	PSTN Cause Code	Description
481 Call leg does not exist	127	Interworking, unspecified
482 Loop detected		
483 Too many hops		
484 Address incomplete	28	Address incomplete
485 Address ambiguous	1	Unallocated number
486 Busy here	17	User busy
487 Request canceled	127	Interworking, unspecified
488 Not acceptable here	127	Interworking, unspecified
500 Internal server error	41	Temporary failure
501 Not implemented	79	Service or option not implemented
502 Bad gateway	38	Network out of order
503 Service unavailable	63	Service or option unavailable
504 Gateway timeout	102	Recover on Expires timeout
505 Version not implemented	127	Interworking, unspecified
580 Precondition failed	47	Resource unavailable, unspecified
600 Busy everywhere	17	User busy
603 Decline	21	Call rejected
604 Does not exist anywhere	1	Unallocated number
606 Not acceptable	58	Bearer capability not currently available

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

A SIP status code can be mapped to many PSTN cause codes. For example, 503 can be mapped to 34, 38, and 58.

Examples

The following example maps a PSTN cause code to correspond to a SIP status code:

```
Router(config)# sip-ua
Router(config-sip-ua)# set sip-status 400 pstn-cause 16
```

Related Commands

Command	Description
set pstn -cause	Sets an incoming PSTN cause code to a SIP error status code.

settle-call

To force a call to be authorized with a settlement server that uses the address resolution method specified in the **session target** command, use the **settle-call**command in dial-peer configuration mode. To ensure that no authorization is performed by a settlement server, use the **no** form of this command.

settle-call *provider-number*
no settle-call *provider-number*

Syntax Description

provider -number	Digit defining the ID of a particular settlement server. The only valid entry is 0. **Note** If **session target** *type* is **settlement**, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Command Default

No default behavior or values.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

With the **session target** command, a dial peer can determine the address of the terminating gateway through the **ipv4**, **dns**, **ras,** and **settlement** keywords.

If the session target is not **settlement,** and the **settle-call** *provider-number* argument is set, the gateway resolves address of the terminating gateway using the specified method and then requests the settlement server to authorize that address and create a settlement token for that particular address. If the server cannot authorize the terminating gateway address suggested by the gateway, the call fails.

Do not combine the session target types **ras** and **settle-call**. Combination of session target types is not supported.

Examples

The following example sets a call to be authorized with a settlement server that uses the address resolution method specified in the **session target**:

```
dial-peer voice 10 voip
 destination-pattern 1408.......
 session target ipv4:172.22.95.14
 settle-call 0
```

Related Commands

Command	Description
session target	Specifies a network-specific address for a specified dial peer.

settlement

To enter settlement configuration mode and specify the attributes specific to a settlement provider, use the **settlement** command in global configuration mode. To disable the settlement provider, use the **no** form of this command.

settlement *provider-number*
no settlement *provider-number*

Syntax Description

provider -number	Digit that defines a particular settlement server. The only valid entry is 0.

Command Default

0

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The variable *provider-number* defines a particular settlement provider. For Cisco IOS Release 12.1, only one clearinghouse per system is allowed, and the only valid value for *provider-number* is 0.

Examples

This example enters settlement configuration mode:

```
settlement 0
```

Related Commands

Command	Description
connection -timeout	Configures the length of time for which a connection is maintained after a communication exchange is completed.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -delay	Sets the time between attempts to connect with the settlement provider.
retry -limit	Sets the connection retry limit.

Command	Description
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

settlement roam-pattern

To configure a pattern that must be matched to determine if a user is roaming, use the **settlement roam-pattern**command in global configuration mode. To delete a particular pattern, use the **no** form of this command.

settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **noroaming**}
no settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **noroaming**}

Syntax Description

provider -number	Digit defining the ID of particular settlement server. The only valid entry is 0.
pattern	User account pattern.
roaming	Specifies that a user is roaming.
noroaming	Specifies that a user is not roaming.

Command Default

No default pattern is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

Multiple roam patterns can be entered on one gateway.

Examples

The following example shows how to configure a pattern that determines if a user is roaming:

```
settlement 0 roam-pattern 1222 roaming
settlement 0 roam-pattern 1333 noroaming
settlement 0 roam-pattern 1444 roaming
settlement 0 roam-pattern 1555 noroaming
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settlement	Enters settlement configuration mode.

sgcp

To start and allocate resources for the Simple Gateway Control Protocol (SGCP) daemon, use the **sgcp** command in global configuration mode. To terminate all calls, release all allocated resources, and kill the SGCP daemon, use the **no** form of this command.

sgcp
no sgcp

Syntax Description

This command has no arguments or keywords.

Command Default

The SGCP daemon is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

When the SGCP daemon is not active, all SGCP messages are ignored.

When you enter the **no sgcp** command, the SGCP process is removed.



Note After you enter the **no sgcp** command, you must save the configuration and reboot the router for the disabling of SGCP to take effect.

Examples

The following example enables the SGCP daemon:

```
sgcp
```

The following example disables the SGCP daemon:

```
no sgcp
```

Related Commands

Command	Description
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp call-agent

To define the IP address of the default Simple Gateway Control Protocol (SGCP) call agent in the router configuration file, use the **sgcp call-agent** command in global configuration mode. To remove the IP address of the default SGCP call agent from the router configuration, use the **no** form of this command.

sgcp call-agent *ipaddress* [**:** *udp port*]
no sgcp call-agent *ipaddress*

Syntax Description

ipaddress	IP address or hostname of the call agent.
:udp port	(Optional) UDP port of the call agent.

Command Default

No IP address is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

This command defines the IP address of the default SGCP call agent to which the router sends an initial RSIP (Restart In Progress) packet when the router boots up. This is used for initial bootup only before the SGCP call agent contacts the router acting as the gateway.

When you enter the **no sgcp call-agent** command, only the IP address of the default SGCP call agent is removed.

Examples

The following example enables SGCP and specifies the IP address of the call agent:

```
sgcp
sgcp call-agent 209.165.200.225
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.

Command	Description
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp graceful-shutdown

To block all new calls and gracefully terminate all existing calls (wait for the caller to end the call), use the **sgcp graceful-shutdown**command in global configuration mode. To unblock all calls and allow new calls to go through, use the **no** form of this command.

sgcp graceful-shutdown
no sgcp graceful-shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until users terminate them, or until you enter the **no sgcp**command. When the last active call is terminated, the SGCP daemon is terminated, and all resources allocated to it are released.

Examples

The following example blocks all new calls and terminates existing calls:

```
sgcp graceful-shutdown
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.

Command	Description
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp max-waiting-delay

To set the Simple Gateway Control Protocol (SGCP) maximum waiting delay to prevent restart avalanches, use the **sgcp max-waiting-delay**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp max-waiting-delay *delay*
no sgcp max-waiting-delay *delay*

Syntax Description

delay	Maximum waiting delay (MWD), in milliseconds. Range is from 0 to 600000. Default is 3000.

Command Default

3,000 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300, and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Examples

The following example sets the maximum wait delay value to 40 ms:

```
sgcp max-waiting-delay 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp modem passthru

To enable Simple Gateway Control Protocol (SGCP) modem or fax pass-through, use the **sgcp modem passthru** command in global configuration mode. To disable SGCP modem or fax pass-through, use the **no** form of this command.

sgcp modem passthru {**ca** | **cisco** | **nse**}
no sgcp modem passthru {**ca** | **cisco** | **nse**}

Syntax Description

ca	Call-agent-controlled modem upspeed-method violation message.
cisco	Cisco-proprietary upspeed method based on the protocol.
nse	NSE-based modem upspeed method.

Command Default

SGCP modem or fax pass-through is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

You can use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions.

If you use the **nse** option, you must also configure the **sgcp tse payload** command.

Examples

The following example configures SGCP modem pass-through using the call-agent upspeed method:

```
sgcp modem passthru ca
```

The following example configures SGCP modem pass-through using the proprietary Cisco upspeed method:

```
sgcp modem passthru cisco
```

The following example configures SGCP modem pass-through using the NSE-based modem upspeed:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp quarantine-buffer disable

To disable the Simple Gateway Control Protocol (SGCP) quarantine buffer, use the **sgcp quarantine-buffer disable**command in global configuration mode. To reenable the SGCP quarantine buffer, use the **no** form of this command.

sgcp quarantine-buffer disable
no sgcp quarantine-buffer disable

Syntax Description

This command has no arguments or keywords.

Command Default

The SGCP quarantine buffer is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The SGCP quarantine buffer is the mechanism for buffering the SGCP events between two notification-request (RQNT) messages.

Examples

The following example disables the SGCP quarantine buffer:

```
sgcp quarantine-buffer disable
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp request retries

To specify the number of times to retry sending notify and delete messages to the Simple Gateway Control Protocol (SGCP) call agent, use the **sgcp request retries**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp request retries *count*
no sgcp request retries

Syntax Description

count	Number of times that a notify and delete message is retransmitted to the SGCP call agent before it is dropped. Range is from 1 to 100. Default is 3.

Command Default

3 times

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The actual retry count may be different from the value you enter for this command. The retry count is also limited by the call agent. If there is no response from the call agent after 30 seconds, the gateway does not retry anymore, even though the number set using the **sgcp request retries**command has not been reached.

The router stops sending retries after 30 seconds, regardless of the setting for this command.

Examples

The following example configures the system to send the **sgcp** command 10 times before dropping the request:

```
sgcp request retries 10
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.

Command	Description
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp request timeout

To specify how long the system should wait for a response to a request, use the **sgcp request timeout**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp request timeout *timeout*
no sgcp request timeout

Syntax Description

timeout	Time to wait for a response to a request, in milliseconds. Range is from 1 to 10000. Default is 500.

Command Default

500 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

This command is used for "notify" and "delete" messages, which are sent to the SGCP call agent.

Examples

The following example configures the system to wait 40 ms for a reply to a request:

```
sgcp request timeout 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp restart

To trigger the router to send a Restart in Progress (RSIP) message to the Simple Gateway Control Protocol (SGCP) call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller, use the **sgcp restart**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp restart {**delay** *delay* | **notify**}
no sgcp restart {**delay** *delay* | **notify**}

Syntax Description

delay *delay*	Restart delay, in milliseconds. Range is from 0 to 600. Default is 0.
notify	Restarts notification upon the SGCP/digital interface state transition.

Command Default

0 ms

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Use this command to send RSIP messages from the router to the SGCP call agent. RSIP messages are used to synchronize the router and the call agent. RSIP messages are also sent when the **sgcp** command is entered to enable the SGCP daemon.

You must enter the **notify** option to enable RSIP messages to be sent.

Examples

The following example configures the system to wait 40 ms before restarting SGCP:

```
sgcp restart delay 40
```

The following example configures the system to send an RSIP notification to the SGCP call agent when the T1 controller state changes:

```
sgcp restart notify
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp retransmit timer

To configure the Simple Gateway Control Protocol (SGCP) retransmission timer to use a random algorithm, use the **sgcp retransmit timer**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp retransmit timer random
no sgcp retransmit timer random

Syntax Description

random	SGCP retransmission timer uses a random algorithm.

Command Default

The SGCP retransmission timer does not use a random algorithm.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 3600 series and the Cisco MC3810 in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Use this command to enable the random algorithm component of the retransmission timer. For example, if the retransmission timer is set to 200 ms, the first retransmission timer is 200 ms, but the second retransmission timer picks up a timer value randomly between either 200 or 400. The third retransmission timer picks up a timer value randomly of 200, 400, or 800 as shown below:

- First retransmission timer: 200
- Second retransmission timer: 200 or 400
- Third retransmission timer: 200, 400, or 800
- Fourth retransmission timer: 200, 400, 800, or 1600
- Fifth retransmission timer: 200, 400, 800, 1600, or 3200 and so on.

After 30 seconds, the retransmission timer no longer retries.

Examples

The following example sets the retransmission timer to use a random algorithm:

```
sgcp retransmit timer random
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

Command	Description
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp timer

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

sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}
no sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}

Syntax Description

receive -rtcp *timer*	RTP Control Protocol (RTCP) transmission interval, in milliseconds. Range is from 1 to 100. Default is 5.
rtp -nse *timer*	RTP named signaling event (NSE) timeout, in milliseconds. Range is from 100 to 3000. Default is 200.

Command Default

receive -rtcp: 5 ms

rtp -nse: 200 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The RTP NSE timer is used for proxy ringing (the ringback tone is provided at the originating gateway).

Examples

The following example sets the RTPCP transmission interval to 100 ms:

```
sgcp timer receive-rtcp 100
```

The following example sets the NSE timeout to 1000 ms:

```
sgcp timer rtp-nse 1000
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp tse payload

To enable Inband Telephony Signaling Events (TSE) for fax and modem operation, use the **sgcp tse payload**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp tse payload *type*
no sgcp tse payload *type*

Syntax Description

type	TSE payload type. Range is from 96 to 119. Default is 0, meaning that the command is disabled.

Command Default

0 (disabled)

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Because this command is disabled by default, you must specify a TSE payload type.

If you set the **sgcp modem passthru** command to the **nse** value, then you must configure this command.

Examples

The following example sets Simple Gateway Control Protocol (SGCP) modem pass-through using the NSE-based modem upspeed and the Inband Telephony Signaling Events payload value set to 110:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.

Command	Description
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.up or down so that the call agent can synchronize
sgcp timer	Configures how the gateway detects the RTP stream host.

source filter

To filter Real-time Transport Protocol (RTP) packets with a source IP address and port number that are different from the one negotiated through Session Initiation Protocol (SIP) signaling, use the **source filter** command in voice service SIP configuration mode. To disable filtering, use the **no** form of this command.

source filter
no source filter

Command Default

RTP source filtering is disabled.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

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

Usage Guidelines

Public Switched Telephone Network (PSTN) callers may experience crosstalk when the SIP IOS gateway receives an invalid RTP stream destined to the same IP address and port of an active call. The invalid stream has a different source IP address and port than the one negotiated using SIP Session Description Protocol (SDP). The Digital Signal Processor (DSP) within the gateway mixes both the valid and invalid RTP streams and plays it to the PSTN caller. Use the **source filter** command when you want to filter RTP packets with a source IP address and port number that are different from the one negotiated through SIP signaling.

Examples

The following example shows how to filter RTP packets:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# source filter
```

Related Commands

Command	Description
sip	Enters SIP configuration mode.
voice service voip	Specifies the voice-encapsulation type and enters voice service configuration mode.