Cisco Unified SIP Proxy SIP Commands

Last Updated: November 1, 2020

sip network

To create a logical SIP network and to enter SIP network configuration mode, use the **sip network** command in Cisco Unified SIP Proxy configuration mode. There is not a **no** form of this command.

sip network *network* [**icmp** | **nat** | **noicmp** | **standard**]

Syntax Description

network	Specifies the name of the SIP network interface.
standard	(Optional) Configures the network interface to use standard SIP. The network has full UDP support. The network interface supports ICMP and different sockets can be used for each endpoint. This is the default setting.
nat	(Optional) Configures the network interface to use Network Address Translation (NAT).
icmp	(Optional) Configures the network interface to use Internet Control Message Protocol (ICMP).
noicmp	(Optional) Specifies that the network interface does not use a separate socket for each endpoint. With this configuration, no ICMP errors are supported.

Command Default

Standard

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The type of socket used for the network interface has different characteristics:

- Standard
  - The network interface has full UDP support.
  - The network interface supports ICMP.
  - Different sockets can be used for each endpoint.
- ICMP
  - The network interface supports ICMP.
- No ICMP
  - No ICMP errors are supported.
  - The network does not use a separate socket for each endpoint.
- NAT
  - The network interface supports NAT.

Caution After a SIP network is created, it cannot be removed.

Examples

The following example configures a standard network and enters SIP network configuration mode:

```
se-10-0-0-0(cusp-config)> sip network internal
se-10-0-0-0(cusp-config-network)>
```

The following example configures a SIP network to support ICMP:

```
se-10-0-0-0(cusp-config)> sip network external icmp
```

The following example configures the SIP network interface so that ICMP errors are not supported:

```
se-10-0-0-0(cusp-config)> sip network external noicmp
```

Related Commands

Command	Description
allow-connections	Configures the SIP network to allow TCP/TLS client connections.
header-hide	Configures the SIP network to mask the header.
non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests,
retransmit-count	Configures the retransmit count for a SIP network.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
show configuration active sip network	Displays the configured SIP network.

allow-connections

To configure the SIP network to allow TCP/TLS client connections, use the **allow-connections** command in Cisco Unified SIP Proxy SIP network configuration mode. To prevent the SIP network from allowing TCP/TLS connections, use the **no** form of this command.

allow-connections

no allow-connections

Syntax Description

This command has no arguments or keywords.

Command Default

TCP/TLS client connections on the SIP network are enabled by default.

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example allows TCP/TLS connections on a standard SIP network named “internal”:

```
se-10-0-0-0(cusp-config)> sip network internal standard
se-10-0-0-0(cusp-config-network)> allow-connections
```

The following example disables TCP/TLS connections on a standard SIP network named “internal”:

```
se-10-0-0-0(cusp-config)> sip network internal standard
se-10-0-0-0(cusp-config-network)> no allow-connections
```

Related Commands

Command	Description
header-hide	Configures the SIP network to mask the header.
non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests,
retransmit-count	Configures the retransmit count for a SIP network.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
sip network	Creates a logical SIP network and enters SIP network configuration mode.

header-hide

To configure the SIP network to mask the header value, use the **header-hide** command in Cisco Unified SIP Proxy SIP network configuration mode. To configure the SIP network to not mask the header value, use the **no** form of this command.

header-hide *header-name*

no header-hide *header-name*

Syntax Description

header-name	Specifies the header name that is masked for the network.

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Command Default

The header value is not masked.

Usage Guidelines

The only valid header name in Cisco Unified SIP Proxy version 1.0 is **via**.

Examples

The following example configures the SIP network to mask the Via header:

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> header-hide via
```

The following example configures the SIP network to not mask the Via header:

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no header-hide via
```

Related Commands

Command	Description
non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests,
retransmit-count	Configures the retransmit count for a SIP network.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
sip network	Creates a logical SIP network and enters SIP network configuration mode

udp max-datagram-size

To configure the maximum size of a UDP datagram for this network, use the **udp max-datagram-size** command in Cisco Unified SIP Proxy SIP network configuration mode. To set the default value of the UDP maximum datagram size, use the **no** form of this command.

udp max-datagram-size *size*

no udp max-datagram-size

Syntax Description

size	Specifies the maximum size of a UDP datagram in bytes for the network.

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
1.1.4	This command was introduced.

Command Default

udp max-datagram-size: 1500

Usage Guidelines

If a packet on the network is larger than this specified size, the message is upgraded to TCP if there exists a TCP listening point configured for the network.

Examples

The following example configures the maximum size of a UDP datagram to 2000 bytes for this network:

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> udp max-datagram-size 2000
```

Related Commands

Command	Description
non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests,
retransmit-count	Configures the retransmit count for a SIP network.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
sip network	Creates a logical SIP network and enters SIP network configuration mode

non-invite-provisional

To enable the sending of 100 responses to nonINVITE requests, use the **non-invite-provisional** command in Cisco Unified SIP Proxy SIP network configuration mode. To disable the sending of 100 responses to non-INVITE requests, use the **no** form of this command.

non-invite-provisional {*TU3-timer-value*}

no non-invite-provisional

Syntax Description

TU3-timer-value	Specifies the TU3 timer to be used.

Command Default

The sending of 100 responses to non-INVITE requests is disabled.

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure SIP networks with TU3 transmission type only. If you enable the sending of 100 responses to nonINVITE requests, you must specify a TU3 timer.

Examples

The following example enables the sending of 100 responses to non-INVITE requests, and sets the TU3 timer value to 200:

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> non-invite-provisional 200
```

The following example disables the sending of 100 responses to non-INVITE requests

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no non-invite-provisional
```

Related Commands

Command	Description
allow-connections	Configures the SIP network to allow TCP/TLS client connections.
header-hide	Configures the SIP network to mask the header.
retransmit-count	Configures the retransmit count for a SIP network.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
sip network	Creates a logical SIP network and enters SIP network configuration mode

retransmit-count (SIP network)

To configure the retransmission count for a SIP network, use the **retransmit-count** command in Cisco Unified SIP Proxy SIP network configuration mode. To restore the default retransmit count value, use the **no** or **default** form of this command.

retransmit-count {**invite-client-transaction** | **invite-server-transaction** | **non-invite-client-transaction**} *count_value*

no retransmit-count {**invite-client-transaction** | **invite-server-transaction** | **non-invite-client-transaction**}

default retransmit-count {**invite-client-transaction** | **invite-server-transaction** | **non-invite-client-transaction**}

Syntax Description

invite-client-transaction	Specifies the retransmit count for the INVITE request. The default is 5.
invite-server-transaction	Specifies the retransmit counts for final responses of INVITE requests. The default is 9.
non-invite-client-transaction	Specifies the retransmit count for requests other than INVITE. The default is 9.
count_value	Specifies the retransmission count value. The valid range is from 0 to 127. The default depends on the retransmit count selected.

Command Default

The default value for each retransmit count type is as follows:

- **invite-client-transaction**—3
- **invite-server-transaction**—3
- **non-invite-client-transaction**—3

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The retransmission count values specify the maximum number of allowable SIP retransmissions. The value of a specific count can be set different for different networks if a network has different transmission latency characteristics. For more information about retransmission counts using SIP, see RFC 3261.

Examples

The following example configures the invite-client retransmit count to 5:

```
se-10-0-0-0(cusp-config)> sip network external standard
```

```
se-10-0-0-0(cusp-config-network)> retransmit-count invite-client-transaction 5
```

The following example configures the client retransmit count to 18:

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> retransmit-count non-invite-client-transaction 18
```

The following example restores the default value of the invite-client count.

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no retransmit-count invite-client-transaction
```

Related Commands

Command	Description
allow-connections	Configures the SIP network to allow TCP/TLS client connections.
header-hide	Configures the SIP network to mask the header.
non-invite-provisional	Enables the sending of 100 responses to nonINVITE requests.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
sip network	Creates a logical SIP network and enters SIP network configuration mode.

retransmit-timer (SIP network)

To configure the SIP retransmission timer values for a SIP network, use the **retransmit-timer** command in Cisco Unified SIP Proxy SIP network configuration mode. To change a retransmission timer value back to the default value, use the **no** or **default** forms of this command.

retransmit-timer {**T1** | **T2** | **T4** | **serverTn** | **clientTn** | **TU1** | **TU2** } *timer_value*

no retransmit-timer {**T1** | **T2** | **T4** | **serverTn** | **clientTn** | **TU1** | **TU2** }

default retransmit-timer {**T1** | **T2** | **T4** | **serverTn** | **clientTn** | **TU1** | **TU2**}

Syntax Description

T1	Sets the initial request retransmission interval. The default is 500 milliseconds.
T2	Sets the maximum request retransmission value. The default is 4,000 milliseconds.
T4	Sets the amount of time a NONINVITE client transaction or INVITE server transaction remains active after completion to handle request or response retransmissions. The default is 5,000 milliseconds.
serverTn	Sets the maximum lifetime of a server transaction. The default is 64,000 milliseconds.
clientTn	Sets the maximum lifetime of a client transaction. The default is 64,000 milliseconds.
TU1	Sets the amount of time an INVITE transaction remains active after completion with a 2xx response to handle response retransmissions. The default is 5,000 milliseconds.
TU2	Sets the amount of time the server waits for a provisional or final response for an INVITE client transaction or NONINVITE server transaction after which the transaction is considered timed out. The default is 32,000 milliseconds.
timer_value	Specifies the retransmission timer value. The default value depends on the retransmission timer selected.

Command Default

The default value for each retransmit timer is as follows:

- **T1**—500 milliseconds
- **T2**—4,000 milliseconds
- **T4**—5,000 milliseconds
- **serverTn**—64,000 milliseconds
- **clientTn**—64,000 milliseconds
- **TU1**—5,000 milliseconds
- **TU2**—32,000 milliseconds

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The retransmission timer values define the duration of SIP retransmissions. The value of a specific timer can be set differently for different networks if a network has different transmission latency characteristics. For more information about retransmission timers using SIP, see RFC 3261.

Examples

The following example configures the T1 retransmission timer to 1,000 milliseconds.

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> retransmit-timer T1 1000
```

The following example restores the default value of the TU1 retransmission timer.

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no retransmit-timer TU1
```

Related Commands

Command	Description
allow-connections	Configures the SIP network to allow TCP/TLS client connections.
header-hide	Configures the SIP network to mask the header.
non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests.
retransmit-count	Configures the retransmit count for a SIP network.
sip network	Creates a logical SIP network and enters SIP network configuration mode.

tls verify

To selectively enable client or server certificate validation on tls connection, use the **tls verify** command in Cisco Unified SIP Proxy configuration mode. To disable the certificate verification, use the **no** form of this command.

tls verify type [client-auth| server-auth]

no tls verify type [client-auth| server-auth]

Syntax Description

client-auth	Verifies the client authentication certificate for TLS connections
server-auth	Verifies the server authentication certificate for TLS connections.

By default, the TLS Verify command is enabled.

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.8	This command was introduced.

Usage Guidelines

Use this command to enable the following certificate type validation:

- tls verify type client-auth—This enables the client certificate authentication for TLS connections. The client certificate validation is applicable for incoming TLS connections to cusp.
- tls verify type server-auth—This enables the server certificate authentication for TLS connections. The server certificate validation is applicable for outgoing TLS connections from cusp.

Examples

The following example enables the both server and client certificate authentication:

```
se-10-104-45-238(cusp-config-network)# tls verify
type type of authentication
<cr>
```

The following example enables the server certificate authentication and client certificate authentication is disabled:

```
se-10-104-45-238(cusp-config-network)# tls verify type server-auth
client-auth client authentication
<cr>
```

The following example enables the client certificate authentication and server certificate authentication is disabled:

```
se-10-104-45-238(cusp-config-network)# tls verify type client-auth
```

```
server-auth server authentication
<cr>
```

The following example disables certificate verification:

```
se-10-104-45-238(cusp-config-network)# no tls verify
```

Related Commands

Command	Description
sip tls	Enables the use of a SIP TLS connections with other SIP entities.
sip record-route	Enables record-routing for a SIP network.

sip listen

To create a listener that listens for SIP traffic on a specific SIP network, host and port, use the **sip listen** command in Cisco Unified SIP Proxy configuration mode. To remove the listener from the SIP network, use the **no** form of this command.

sip listen *network_name* {**tcp** | **tls** | **udp**} *ip_address port*

no sip listen *network_name* {**tcp** | **tls** | **udp**} *ip_address port*

Syntax Description

network_name	Specifies the SIP network name.
tcp	Specifies that TCP is used as the transport protocol of the listener.
tls	Specifies that TLS is used as the transport protocol of the listener.
udp	Specifies that UDP is used as the transport protocol of the listener. This is the default.
ip_address	The interface IP address that accepts incoming requests.
port	The port the server listens on for incoming messages. The valid range is from 1024 to 65535. The default value is 5060.

Command Default

The listener on the SIP network is not enabled.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

A listener is an interface, port, and transport tuple that the server listens on for incoming packets. Multiple listeners can be configured for a single server; however, at least one **must** be established for the server to accept SIP traffic. A network can have multiple listeners. You do not have to disable listeners on the network when you make configuration changes to the network.

Caution You cannot run TCP and TLS listeners on the same port.

Caution Do not enable the **sip listen** command until you complete all of the other configuration tasks. After you enable the command, the system starts receiving incoming requests from the specified SIP network.

Examples

The following example configures the listener on a SIP network named “external” that uses the TCP:

```
se-10-0-0-0(cusp-config)> sip listen external tcp 10.2.3.4 5060
```

The following example configures the listener on a SIP network named “internal” that uses the UDP:

```
se-10-0-0-0(cusp-config)> sip listen internal udp 192.168.1.3 5061
```

The following example disables a listener on a SIP network:

```
se-10-0-0-0(cusp-config)> no sip listen external tcp 10.2.3.4 5060
```

Related Commands

Command	Description
sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip record-route

To enable record-routing for a SIP network, use the **sip record-route** command in Cisco Unified SIP Proxy configuration mode. To disable record-routing for a SIP network, use the **no** form of this command.

sip record-route *network_name* {**tcp** | **tls** | **udp**} *ip_address* [*port*]

no sip record-route *network_name*

Syntax Description

network_name	Specifies the SIP network name (as configured using the **sip network** command) that is logically associated with a Record-Route configuration.
tcp	Specifies that TCP populates the Record-Route header field.
tls	Specifies that TLS populates the Record-Route header field.
udp	Specifies that UDP populates the Record-Route header field. This is the default.
ip_address	Specifies the interface hostname or IP address that populates the Record-Route header field.
port	(Optional) Specifies the port that populates the Record-Route header field. If not specified, 5060 is populated. The valid range is from 1024 to 65535.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Record-routing ensures that all SIP messages within a dialog traverse the same route. The SIP Record-Route header field contains configurable interface, port, and transport values, which forces messages to pass through the desired SIP entity. The Record-Route feature is critical for directing messages to a load balancer that is managing SIP traffic for a group of servers.

Examples

The following example enables record-routing for a SIP network named “internal”:

```
se-10-0-0-0(cusp-config)> sip record-route internal udp cusp1.example.com
```

The following example enables record-routing for a SIP network named “external”:

```
se-10-0-0-0(cusp-config)> sip record-route external tcp 192.168.1.3 5061
```

The following example disables record-routing for a SIP network named “external”:

```
se-10-0-0-0(cusp-config)> no sip record-route external
```

Related Commands

Command	Description
show configuration active sip record-route	Displays SIP record-route configuration.

sip max-forwards

To configure the value of the SIP Max-Forwards header field, use the **sip max-forwards** command in Cisco Unified SIP Proxy configuration mode. To remove the value from the SIP Max-Forwards header field and restore the default value, use the **no** form of this command.

sip max-forwards *max_forward_value*

no sip max-forwards *max_forward_value*

Syntax Description

max_forward_value	Specifies the value of the Max-Forwards header field. The allowed values are 0 to 255. The default value is 70.

Command Default

70

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The Max-Forwards header field of a SIP request specifies the maximum number of times the request can be forwarded to another server. Each time a request is received by a server, this value is decremented by one. (If the request does not have a Max-Forwards header, one is added.) When the value reaches zero, the server responds with a 483 (Too Many Hops) response and terminates the transaction.

You can use the Max-Forwards header field to detect forwarding loops within a network.

Note We recommend that you set this command to a value greater than or equal to 10, and less than or equal to 100.

Examples

The following example configures the value of the SIP Max-Forwards header field to 100:

```
se-10-0-0-0(cusp-config)> sip max-forwards 100
```

Related Commands

Command	Description
sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip header-compaction

To enable SIP header compaction, use the **sip header-compaction** command in Cisco Unified SIP Proxy configuration mode. To disable SIP header compaction, use the **no** form of this command.

sip header-compaction

no sip header-compaction

Syntax Description

This command has no arguments or keywords.

Command Default

SIP header compaction is disabled.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When enabled, compact header forms are used for the following SIP headers:

- Call-ID
- Contact
- Content-Encoding
- Content-Length
- Content-Type
- From
- Subject
- To
- Via

When header compaction is disabled, complete SIP headers are used in all outgoing messages, regardless of the header format.

Examples

The following example enables SIP header compaction:

```
se-10-0-0-0(cusp-config)> sip header-compaction
```

The following example disables SIP header compaction:

```
se-10-0-0-0(cusp-config)> no sip header-compaction
```

Related Commands

Command	Description
sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip overload redirect

To configure the server to send a 300 (Redirect) response when the server is overloaded, use the **sip overload redirect** command in Cisco Unified SIP Proxy configuration mode. To disable the server from sending a redirect response when the server is overloaded, use the **no** from of this command.

sip overload redirect *redirect_ip* [**port** *redirect_port*] [**transport** {**tcp | tls | udp**}]

no sip overload redirect *redirect_ip* [**port** *redirect_port*] [**transport** {**tcp | tls | udp**}]

Syntax Description

redirect_ip	The redirect interface host name or IP address sent in the SIP Contact header field. Subsequent requests will be redirected to the server at this address.
port *redirect_port*	(Optional) The port of the redirect host. The valid range is from 1024 to 65535. The default is 5060.
transport	(Optional) The transport protocol used by the redirect host.
tcp	Uses TCP as the transport.
tls	Uses TLS as the transport.
udp	Uses UDP as the transport. UDP is the default value if a transport protocol is not chosen.

Command Default

The default port is 5060, and the default transport protocol is UDP.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command configures the behavior of the server when it is overloaded. There are two behavior modes: reject and redirect. Use the **sip overload redirect** command to configure redirect mode and the **sip overload reject** command to configure reject mode. Only one mode can be configured at a time.

If reject mode is configured, the proxy rejects messages and responds with a 503 (Server Unavailable) response when overloaded.

If redirect mode is cconfigured, the proxy redirects messages and responds with a 300 (Redirect) response when overloaded.

Examples

The following example configures the server to send a 300 (Redirect) response when the server is overloaded:

```
se-10-0-0-0(cusp-config)> sip overload redirect 192.168.20.5 transport udp
```

The following example disables the server from sending a 300 (Redirect) response when the server is overloaded:

```
se-10-0-0-0(cusp-config)> no sip overload redirect 192.168.20.5
```

Related Commands

Command	Description
sip overload reject	Configures the server to send a 503 (Server Unavailable) response when the server is overloaded.

sip overload reject

To configure the server to send a 503 (Server Unavailable) response when the server is overloaded, use the **sip overload reject** command in Cisco Unified SIP Proxy configuration mode. To disable the server from sending a reject response when the server is overloaded, use the **no** from of this command.

sip overload reject [**retry-after** *retry_after_time*]

no sip overload reject [**retry-after** *retry_after_time*]

Syntax Description

retry-after *retry_after_time*	(Optional) The number of seconds sent in the SIP Retry-After header field of the 503 (Server Unavailable) response, which indicates when the sender can attempt the transaction again. If not specified, the 503 (Server Unavailable) response does not contain a Retry-After header field. The minimum value allowed is 0. The default value is 0.

Command Default

The default value is 0.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command configures the behavior of the server when it is overloaded. There are two behavior modes: reject and redirect. Use the **sip overload redirect** command to configure redirect mode and the **sip overload reject** command to configure reject mode. Only one mode can be configured at a time.

If reject mode is configured, the proxy rejects messages and responds with a 503 (Server Unavailable) response when overloaded.

If redirect mode is cconfigured, the proxy redirects messages and responds with a 300 (Redirect) response when overloaded.

Examples

The following example configures the server to send a 503 (Server Unavailable) response when the server is overloaded:

```
se-10-0-0-0(cusp-config)> sip overload-reject
```

The following example configures the server to send a 503 (Server Unavailable) response when the server is overloaded and sets the retry-after-time to 60 seconds:

```
se-10-0-0-0(cusp-config)> sip overload-reject 60
```

The following example disables the server from sending a 503 (Server Unavailable) response when the server is overloaded:

```
se-10-0-0-0(cusp-config)> no sip overload-reject
```

Related Commands

Command	Description
sip overload redirect	Configures the server to send a 300 (Redirect) response when the server is overloaded.

sip tcp connection-timeout

To configure the time in minutes that the server keeps the SIP TCP connections open, use the **sip tcp connection-timeout** command in Cisco Unified SIP Proxy configuration mode. To reset the SIP TCP connection timeout value to its default value, use the **no** form of this command.

sip tcp connection-timeout *timeout_value*

no sip tcp connection-timeout

Syntax Description

timeout_value	Specifies the time, in minutes, before an idle TCP/TLS connection is gracefully closed. The accepted values start at 0. The default value is 30 minutes.

Command Default

30 minutes

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the SIP TCP connection timeout value to 120 minutes:

```
se-10-0-0-0(cusp-config)> sip tcp connection-timeout 120
```

Related Commands

Command	Description
sip tcp max-connections	Configures the maximum number of TCP/TLS connections.

sip tcp max-connections

To configure the maximum number of TCP/TLS connections, use the **sip tcp max-connections** command in Cisco Unified SIP Proxy configuration mode. To reset the system to the default value, use the **no** form of this command.

sip tcp max-connections *value*

no sip tcp max-connections *value*

Syntax Description

value	Maximum number of TCP/TLS connections allowed. The default is 256 and the minimum is 1.

Command Default

The maximum number of TCP/TLS connections allowed is 256.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When the maximum number of TCP/TLS connections is reached, passive (incoming) connections are not accepted, and additional active (outgoing) connections can be made.

Examples

The following example configures the maximum number of TCP/TLS connections to 512:

```
se-10-0-0-0(cusp-config)> sip tcp max-connections 512
```

Related Commands

Command	Description
sip tcp connection-timeout	Configures the time in minutes that the server keeps the SIP TCP connections open.

sip queue

To configure the properties of a SIP queue and enter SIP queue configuration mode, use the **sip queue** command in Cisco Unified SIP Proxy configuration mode. To set all the properties in the SIP queue configuration submode back to the default, use the **no** or **default** forms of this command.

sip queue {**message** | **request** | **st-callback** | **ct-callbackresponse** | **timer** | **xcl** | **radius**}

no sip queue {**message** | **request** | **st-callback** | **ct-callbackresponse** | **timer** | **xcl** | **radius**}

default sip queue {**message** | **request** | **st-callback** | **ct-callbackresponse** | **timer** | **xcl** | **radius**}

Syntax Description

message	Enters SIP queue configuration mode to configure the properties of the message queue. The message queue manages incoming SIP messages received from the transport layer.
request	Enters SIP queue configuration mode to configure the properties of the request queue. The request queue manages incoming SIP requests that cannot be immediately processed by the server.
st-callback	Enters SIP queue configuration mode to configure the properties of the st-callback queue. The st-callback queue manages ACK and CANCEL callbacks to server transactions.
ct-callbackresponse	Enters SIP queue configuration mode to configure the properties of the ct-callback queue. The ct-callbackresponse queue manages callbacks to client transmissions.
timer	Enters SIP queue configuration mode to configure the properties of the timer queue. The timer queue manages SIP timer events.
xcl	Enters SIP queue configuration mode to configure the properties of the XCL queue. The xcl queue manages XCL requests.
radius	Enters SIP queue configuration mode to configure the properties of the RADIUS queue. The radius queue manages RADIUS accounting requests.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The SIP queues are created by the proxy during runtime. The queue gets created by the proxy with the default values as the service gets activated. The command fails if the queue does not yet exist. To verify what SIP queues have been created, use the **show status queue** command.

Examples

The following example enters SIP queue configuration mode to configure the timer queue:

```
se-10-0-0-0(cusp-config)> sip queue timer
se-10-0-0-0(cusp-config-queue)>
```

The following example enters SIP queue configuration mode to configure the st-callback queue:

```
se-10-0-0-0(cusp-config)> sip queue st-callback
se-10-0-0-0(cusp-config-queue)>
```

The following example sets all the SIP RADIUS queue parameters back to their default values:

```
se-10-0-0-0(cusp-config)> no sip queue radius
```

Related Commands

Command	Description
drop-policy	Configures the drop policy for a SIP queue.
low-threshold	Configures the low-water-mark for a SIP queue.
show status queue	Displays the statistics for active SIP queues.
size	Configures the maximum number of messages that can be held by a specified queue.
thread-count	Configures the thread count for a specific SIP queue.

drop-policy

To configure the drop policy for a SIP queue, use the **drop-policy** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the configured drop policy and return to the default value, use the **no or default** form of this command.

drop-policy {**head** | **tail** | **none**}

no drop-policy {**head** | **tail** | **none**}

default drop-policy {**head** | **tail** | **none**}

Syntax Description

head	Instructs the transport layer to drop the oldest events from the head of the queue when the maximum queue size is reached. This is the default value.
tail	Instructs the transport layer to drop the newest events from the tail of the queue when the maximum queue size is reached.
none	Instructs the transport layer to ignore the maximum queue size limit and store all events.

Command Default

The head drop policy is used.

Command Modes

Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the drop policy in the SIP message queue to the head setting:

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> drop-policy head
```

The following example configures the drop policy in the SIP st-callback queue to the tail setting:

```
se-10-0-0-0(cusp-config)> sip queue st-callback
se-10-0-0-0(cusp-config-queue)> drop-policy tail
```

The following example configures the drop policy in the radius queue to the unbounded setting:

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> drop-policy none
```

The following example returns the drop-policy for the RADIUS queue to the default value:

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> no drop-policy
```

Related Commands

Command	Description
low-threshold	Configures the low-water-mark for a SIP queue.
sip queue	Creates a SIP queue and enters SIP queue configuration mode.
size	Configures the maximum number of messages that can be held by a specified queue.
thread-count	Configures the thread count for a specific SIP queue.

low-threshold

To configure the low-water-mark for a SIP queue, use the **low-threshold** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the low-water-mark value from the SIP queue and return to the default value, use the **no** or **default** form of this command.

low-threshold *low-water-mark*

no low-threshold

default low-threshold

Syntax Description

low-water-mark	Specifies the percentage of the maximum queue size. The valid range is from 1 to 100. The default is 80 percent.

Command Default

80 percent

Command Modes

Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The low-water mark value specifies the capacity at which the server is no longer considered overloaded, and starts accepting new events.

Examples

The following example configures the low-water mark for the SIP message queue to 100 percent:

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> low-threshold 100
```

The following example configures the low-water mark for the RADIUS queue to 50 percent:

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> low-threshold 50
```

The following example returns the low-water mark for the ct-callback queue to the default value:

```
se-10-0-0-0(cusp-config)> sip queue ct-callback
se-10-0-0-0(cusp-config-queue)> no low-threshold
```

Related Commands

Command	Description
drop-policy	Configures the drop policy for a SIP queue.
sip queue	Creates a SIP queue and enters SIP queue configuration mode.

Command	Description
size	Configures the maximum number of messages that can be held by a specified queue.
thread-count	Configures the thread count for a specific SIP queue.

size

To configure the maximum number of messages that can be held by a specified queue, use the **size** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the configured SIP queue size and return to the default value, use the **no** or **default** form of this command.

size *queue-size*

no size *queue-size*

default size *queue-size*

Syntax Description

queue-size	The maximum number of messages that can be held by the specified queue. The valid range is from 10 to 50,000. The default is 2,000.

Command Default

2,000

Command Modes

Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Caution Setting this parameter to a large value must be carefully evaluated because the memory consumed is directly proportional to this queue size.

Examples

The following example configures the message queue size to 10,000:

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> size 10000
```

The following example configures the radius queue size to 5,000:

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> size 5000
```

The following example returns the radius queue size to the default value:

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> no size 5000
```

Related Commands

Command	Description
drop-policy	Configures the drop policy for a SIP queue.
low-threshold	Configures the low-water-mark for a SIP queue.
sip queue	Creates a SIP queue and enters SIP queue configuration mode.
thread-count	Configures the thread count for a specific SIP queue.

thread-count

To configure the maximum number of threads allocated to a specified SIP queue, use the **thread-count** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the thread count value from the SIP queue and return to the default value, use the **no** or **default** form of this command.

thread-count *thread_count*

no thread-count *thread_count*

default thread-count *thread_count*

Syntax Description

thread_count	The maximum number of threads allocated to the specified queue. The minimum value allowed is 1. The default is 20.

Command Default

20 threads are allocated to the SIP queue.

Command Modes

Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the thread count for the SIP message queue to 40:

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> thread-count 40
```

The following example returns the message queue thread count to the default value:

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> no thread-count 40
```

Related Commands

Command	Description
drop-policy	Configures the drop policy for a SIP queue.
low-threshold	Configures the low-water-mark for a SIP queue.
sip queue	Creates a SIP queue and enters SIP queue configuration mode.

sip dns-srv

To configure SIP DNS SRV lookup commands and enter SIP DNS SRV configuration mode, use the **sip dns-srv** command in Cisco Unified SIP Proxy configuration mode. To return all of the DNS SRV configuration submode parameters to the default values, use the **no** form of this command.

sip dns-srv

no sip dns-srv

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When there is no server-group configured for a given hostname, the system first attempts the DSN resolution using /etc/hosts. If this fails, then the system uses DNS lookup. Commands in the SIP DNS SRV configuration submode configure the DNS NAPTR/SRV lookup related information.

Examples

The following example enters SIP DNS SRV configuration mode:

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)>
```

Related Commands

Command	Description
enable (SIP DNS server)	Enables the use of DNS server NAPTR or SRV query records for doman name/IP address mapping.
sip network	Creates a logical SIP network and enters SIP network configuration mode.
use-naptr	Enables the use of DNS NAPTR for domain name/IP address mapping.

enable (SIP DNS server)

To enable the use of DNS server NAPTR or SRV query records for doman name/IP address mapping, use the **enable** command in SIP DNS server configuration mode. To disable the use of DNS server NAPTR or SRV query records, use the **no** form of this command.

enable

no enable

SyntaxDescription

This command has no arguments or keywords.

Command Default

Using DNS server SRV query records is disabled.

Command Modes

SIP DNS server configuration (cusp-config-dns)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When this command is disabled, the use of DNS servers NAPTR/SRV records is disabled and only simple naming resolution is performed using the operating system's DNS configuration. DNS SRV (RFC 3263) is used for Cisco Unified SIP Proxy load balancing.

Examples

The following example enables the use of DNS server SRV query records:

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> enable
```

The following example disables the use of DNS server SRV query records:

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> no enable
```

Related Commands

Command	Description
sip dns-srv	Enters SIP DNS SRV configuration mode.
sip network	Creates a logical SIP network and enters SIP network configuration mode.
use-naptr	Enables the use of DNS NAPTR for domain name/IP address mapping.

use-naptr

To enable the use of DNS NAPTR for hostname/IP address mapping, use the **use-naptr** command in SIP DNS server configuration mode. To disable the use of DNS NAPTR for domain name/IP address mapping, use the **no** form of this command.

use-naptr

no use-naptr

SyntaxDescription

This command has no arguments or keywords.

Command Default

The use of DNS NAPTR for domain name/IP address mapping is disabled.

Command Modes

SIP DNS server configuration mode (cusp-config-dns)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example enables the use of DNS NAPTR for hostname/IP address mapping:

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> use-naptr
```

The following example disables the use of DNS NAPTR for hostname/IP address mapping:

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> no use-naptr
```

Related Commands

Command	Description
enable (SIP DNS server)	Enables the use of DNS server NAPTR or SRV query records for doman name/IP address mapping.
sip dns-srv	Enters SIP DNS SRV configuration mode.
sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip alias

To configure the hostname of this instance, use the **sip alias** command in Cisco Unified SIP Proxy configuration mode. To remove the hostname from the DNS server list, use the **no** form of this command.

sip alias {*hostname*}

no sip alias {*hostname*}

Syntax Description

hostname	Specifies the globally reachable host name of the system and adds it to the server's hostname list.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example adds cusp.example.com to the hostname list:

```
se-10-0-0-0(cusp-config)> sip alias cusp.example.com
```

The following example removes cusp.example.com from the server's hostname list:

```
se-10-0-0-0(cusp-config)> no sip alias cusp.example.com
```

Related Commands

Command	Description
sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip logging

To enable the logging of all incoming and outgoing SIP messages, use the **sip logging** command in Cisco Unified SIP Proxy configuration mode. To disable the logging of incoming and outgoing SIP messages, use the **no** form of this command.

sip logging

no sip logging

Syntax Description

This command has no arguments or keywords.

Command Default

SIP logging is disabled.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Turning on SIP logging has a significant performance impact on Cisco Unified SIP Proxy.

Examples

The following example enables the logging of all incoming and outgoing SIP messages:

```
se-10-0-0-0(cusp-config)> sip logging
```

The following example disables the logging of all incoming and outgoing SIP messages:

```
se-10-0-0-0(cusp-config)> no sip logging
```

Related Commands

Command	Description
sip network	Creates a logical SIP network and enters SIP network configuration mode.
sip queue	Creates a SIP queue and enters SIP queue configuration mode.

sip peg-counting

To enable SIP transaction peg counting for all incoming and outgoing SIP messages, use the **sip peg-counting** command in Cisco Unified SIP Proxy configuration mode. To disable SIP transaction peg counting, use the **no** form of this command.

sip peg-counting *interval*

no sip peg-counting

Syntax Description

interval	Peg count collection interval in seconds.

Command Default

SIP peg counting is disabled.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Enabling SIP peg counting has a noticeable performance impact on Cisco Unified SIP Proxy, although not as much of an impact as enabling SIP logging.

Examples

The following example enables SIP transaction peg counting every 60 seconds:

```
se-10-0-0-0(cusp-config)> sip peg-counting 60
```

The following example disables SIP transaction peg counting:

```
se-10-0-0-0(cusp-config)> no sip peg-counting
```

Related Commands

Command	Description
sip logging	Enables the logging of all incoming and outgoing SIP messages.

sip privacy trusted-destination

To configure where to assert the privacy, which determines if the requested privacy service can be provided or not, use the **sip privacy trusted-destination** command in Cisco Unified SIP Proxy configuration mode. To remove the assert privacy configuration, use the **no** form of the command.

sip privacy trusted-destination sequence *sequence_number* [**condition** *condition*]

no sip privacy trusted-destination sequence *sequence_number* [**condition** *condition*]

Syntax Description

sequence *sequence_number*	Specifies the sequence number that denotes the order of conditions to be checked.
condition *condition*	(Optional) Specifies the trigger condition name (configured with the **trigger condition** command) to which the privacy assertion support applies. If the **condition** keyword is not specified, then the privacy assertion is unconditional.

Command Default

All peers are untrusted.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure the conditions for trusted-peers for "id" privacy service. Cisco Unified SIP Proxy removes P-Asserted-Identity headers from the request if the request is from a untrusted peer; and it removes P-Asserted-Identity from the request if the request it to be sent to a untrusted peer. Privacy service is provided for Diversion headers as well, following draft-levi-sip-diversion-08.txt

Examples

The following example configures the destination as a trusted peer if the in-network condition is met:

```
se-10-0-0-0(cusp-config)> sip privacy trusted-destination sequence 1 condition in-network
```

The following example configures all destinations as untrusted unconditionally:

```
se-10-0-0-0(cusp-config)> no sip privacy trusted-destination sequence 1
```

Related Commands

Command	Description
sip privacy trusted-source	Configures where to assert the privacy, which determines if the requested privacy service can be provided or not.

sip privacy trusted-source

To configure where to assert the privacy, which determines if the requested privacy service can be provided or not, use the **sip privacy trusted-source** command in Cisco Unified SIP Proxy configuration mode. To remove the assert privacy configuration, use the **no** form of this command.

sip privacy trusted-source sequence *sequence_number* [**condition** *condition*]

no sip privacy trusted-source sequence *sequence_number* [**condition** *condition*]

Syntax Description

sequence *sequence_number*	Specifies the sequence number that denotes the order of conditions to be checked.
condition *condition*	(Optional) Specifies the trigger condition name (configured with the **trigger condition** command) to which the privacy assertion support applies. If the **condition** keyword is not specified, then the privacy assertion is unconditional.

Command Default

All peers are untrusted.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure the conditions for trusted-peers for "id" privacy service. CUSP removes P-Asserted-Identity headers from the request if the request is from a untrusted peer; and it removes P-Asserted-Identity from the request if the request it to be sent to a untrusted peer. Privacy service is provided for Diversion headers as well, following draft-levi-sip-diversion-08.txt

Examples

The following example configures all sources as trusted unconditionally and assigns the value to sequence 1:

```
se-10-0-0-0(cusp-config)> sip privacy trusted-source sequence 1
```

The following example configures all sources as untrusted unconditionally:

```
se-10-0-0-0(cusp-config)> no sip privacy trusted-source sequence 1
```

Related Commands

Command	Description
sip privacy trusted-destination	Configures where to assert the privacy, which determines if the requested privacy service can be provided or not.
trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

sip privacy service

To enable SIP privacy service, use the **sip privacy service** command in Cisco Unified SIP Proxy configuration mode. To disable SIP privacy service, use the **no** form of this command.

sip privacy service

no sip privacy service

Syntax Description

This command has no arguments or keywords.

Command Default

SIP privacy service is enabled.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Since the Cisco Unified SIP Proxy implements "id" privacy (RFC 3325) only, if privacy values contain any one of "session", "user" or "header", and it also contains "critical", Cisco Unified SIP Proxy returns 500 response following RFC 3323 if the SIP privacy service is enabled.

Examples

The following example enables SIP privacy service:

```
se-10-0-0-0(cusp-config)> sip privacy service
```

sip tls

To enable the use of SIP Transport Layer Security (TLS) connections with other SIP entities, providing secure communication over the Internet, use the **sip tls** command in Cisco Unified SIP Proxy configuration mode. To disable the SIP TLS transport, use the **no** form of this command.

sip tls

no sip tls

Syntax Description

This command has no arguments or keywords.

Command Default

SIP TLS is not enabled.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command before configuring a SIP listener that uses the TLS transport.

Use this command to enable the use of SIP TLS connections with any other SIP entities, providing secure communications over the network. By default, TLS connections are accepted from all requesting clients with whom the Cisco Unified SIP Proxy has a trusted certificate. This is useful only when data encryption is desired and trust relationships are not required.

TLS encryption requires the two participating parties to specify a keystore and a corresponding trust certificate. When TLS is enabled, the system reads the key store files. As a result, before enabling the **sip tls** command, the keystore must first be created using the **cypto key generate** command.

Cisco Unified SIP Proxy supports both one-way and two-way TLS.

Note If there are active SIP listeners with the TLS transport enabled, then this command cannot be disabled.

Examples

The following example enables the use of SIP TLS connections:

```
se-10-0-0-0(cusp-config)> sip tls
```

The following example disables the use of SIP TLS connections:

```
se-10-0-0-0(cusp-config)> no sip tls
```

Related Commands

Command	Description
crypto key generate	Generates a certificate-private key pair.
sip network	Creates a logical SIP network and enters SIP network configuration mode.
sip tls trusted-peer	Configures a SIP TLS trusted peer.
tls verify	Enables client or server certificate validation.

sip tls trusted-peer

To configure a SIP TLS trusted peer, use the **sip tls trusted-peer** command in Cisco Unified SIP Proxy configuration mode. To remove the SIP TLS trusted peer, use the **no** form of this command.

sip tls trusted-peer {*peer's-hostname*}

no sip tls trusted-peer {*peer's-hostname*}

Syntax Description

peer's-hostname	Specifies the peer's hostname.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The establishment of TLS connections fails unless the identity of the remote side matches the identifier of a configured trusted peer. If there are no trusted peers configured, the connection is accepted as long as the TLS handshake succeeds.

Examples

The following example configures example.com as a TLS trusted peer:

```
se-10-0-0-0(cusp-config)> sip tls trusted-peer example.com
```

The following example removes example.com as a TLS trusted peer:

```
se-10-0-0-0(cusp-config)> no sip tls trusted-peer example.com
```

Related Commands

Command	Description
sip-tls	Enable the use of SIP Transport Layer Security (TLS) connections with other SIP entities.

sip tls connection-setup-timeout

To configure a SIP TLS connections setup timeout with other SIP entities, use the **sip tls connection-setup-timeout** command in Cisco Unified SIP Proxy configuration mode. To disable the SIP TLS connections setup timeouts, use the **no** form of this command.

sip tls connection-setup-timeout {*seconds*}

no sip tls

Syntax Description

connection-setup-timeout *seconds*	Displays the time specified in Cisco Unified SIP Proxy by the user to establish connection with the trusted peer in seconds. The default value is 1 second. Range is 1 to 60 seconds.

Command Default

1 second

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.5	This command was introduced.

Usage Guidelines

Use this command to setup the timeout intervals between SIP entities that uses the TLS transport.

Examples

The following example enables the use of SIP TLS with connection-setup-timeout connections:

```
se-10-0-0-0(cusp-config)> sip tls connection-setup-timeout 10
```

Related Commands

Command	Description
crypto key generate	Generates a certificate-private key pair.
sip network	Creates a logical SIP network and enters SIP network configuration mode.
sip tls trusted-peer	Configures a SIP TLS trusted peer.
tls verify	Enables client or server certificate validation.

route recursion

To enable SIP route recursion system-wide for the Cisco Unified SIP Proxy when a redirect response is issued, use the **route recursion** command in Cisco Unified SIP Proxy configuration mode. To disable SIP route recursion, use the **no** form of this command.

route recursion

no route recursion

Syntax Description

This command has no arguments or keywords.

Command Default

Route recursion is enabled by default.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When the Cisco Unified SIP Proxy receives a redirect response (that is, any 3xx response), it can be configured to recursively perform its routing logic on the received Contacts. A received Contact is placed into the Request URI of the prenormalized incoming request, and the server's routing and postnormalization logic is executed based on the new destination. If multiple Contacts are received, they are processed sequentially based on their configured q-values. If more than one contacts have the same q-value, they are processed sequentially in order of the appearance. Use the command **no route recursion** in global configuration mode to turn off redirect processing in Cisco Unified SIP Proxy.

Examples

The following example enables route recursion on the Cisco Unified SIP Proxy:

```
se-10-0-0-0(cusp-config)> route recursion
```

The following example disables route recursion on the Cisco Unified SIP Proxy:

```
se-10-0-0-0(cusp-config)> no route recursion
```

Related Commands

Command	Description
route group	Creates a route group and enters route group configuration mode.
route table	Creates a route table and enters route table configuration mode.