SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport

First Published: February 27, 2006
Last Updated: February 27, 2006

This feature module describes the SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport feature which implements the Transport Layer Security (TLS) protocol on the Transmission Control Protocol (TCP) transport for Cisco IOS SIP Gateways. The feature leverages the existing SIP gateway's support of the public-key infrastructure (PKI) (for certificate management) and utilizes TLS functionality to provide SIP signaling over TLS transport. The use of PKI on the Cisco IOS software requires that the clock on the session initiation protocol (SIP) gateway be synchronized with the network time to ensure proper validation of certificates.

Note The SIP: Cisco IOS SIP Gateway Signaling Over TLS Transport feature provides security only to the device authentication and data encryption of SIP signaling information at the transport layer of the Open System Interconnection (OSI) model. The authentication of the SIP user itself at the application level is done using the Digest Mechanism Implemented by the SIP Gateway Authentication feature.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport, page 52.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Prerequisites for SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport

Before configuring peers for certificate enrollment, you should have an understanding of the following subtasks using information from the following guides: Cisco IOS Security Configuration Guide, Release 12.4 and Cisco IOS SIP Security Application Guide, Release 12.3:

- Enter user EXEC or privileged EXEC mode
- Enter global configuration mode
- Generate the keypair
- Configure the PKI trustpoint
- Authenticate the trustpoint
- Enroll the trustpoint with the CA

The use of PKI on Cisco IOS software requires that the clock on the SIP gateway be synchronized with the network time to ensure proper validation of certificates.

Information About SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport

In order to use the SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport feature, you should understand the following concepts:

Security Benefits of SIP over TLS Signaling

The SIP: Cisco IOS SIP Gateway Signaling Over TLS Transport feature provides the following security for SIP gateway calls;

- Mutual Authentication—To overcome the identity theft whereby the intruder gains illegitimate access by posing as a trusted SIP endpoint or the server, a two way device authentication (by both client and the server) by exchange of SIP gateway's certificate signed by the trusted CA is performed.
- Signaling Data Encryption—To overcome the eavesdropping (intruder sniffing) and man-in-the-middle attacks (intruder interrupting the dialog or modifying the signaling data), the following is performed.
  - Negotiation of a dynamically generated symmetric key and cipher algorithms through TLS handshake,
  - SIP signaling data encryption or decryption using the exchanged symmetric key.

Cisco IOS software has a simplified security infracture deployment and management. The PKI component on Cisco IOS software supports hierarchical framework for managing the key pairs, certificates and authorities. It helps securely distribute public keys. The following functions provided by the infrastructure are leveraged for the SIP over TLS signaling.

- Authentication of issuing certification authority (CA) server —For obtaining the CA certificate chain,
- Enrollment with the CA server—For obtaining its own certificate (aka SIP gateway's identity) for the generated key pair.
- Revocation—Efficient rejection of bad public key that was sent by the negotiating router.

When the SIP gateway is interworking with another SIP entity that supports Simple Certification Enrollment Protocol (SCEP) based enrollment process sharing the common root, the auto-enrollment procedure is employed. Otherwise, the support for manual and Trivial File Transfer Protocol (TFTP) enrollment on Cisco IOS SIP Gateway ensure at least the ability to interoperate with the elements such as Cisco CallManager (CCM) and Cisco SIP Proxy Server (CSPS), which does not support SCEP or auto enrollment.

How to Configure SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport

This section contains the following procedures:

- Configuring SIP Gateways to Communicate with SIP Endpoints over TLS That Share the Same CA, page 3
- Configuring SIP Gateways to Communicate With SIP Endpoint Over TLS That Uses Different CA, page 9
- Displaying TLS Over TCP Transport Connection Information, page 18 (optional)
- Clearing TLS Over TCP Transport Connection Information, page 19 (optional)

Configuring SIP Gateways to Communicate with SIP Endpoints over TLS That Share the Same CA

This procedure allows the SIP gateway to communicate with SIP endpoints over TLS that share the same CA. It consists of the following subtasks:

- Enter user EXEC or privileged EXEC mode

- Enter global configuration mode
- Generate the keypair
- Configure the PKI trustpoint
- Authenticate the trustpoint
- Enroll the trustpoint with the CA
- Have SIP use this trustpoint for TLS connections
- Configure SIP to use TLS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** {**general-keys** | **usage-keys**} **label** *key-label*][**exportable**][**modulus** *modulus-size*][**storage** *device***:**]
4. **crypto pki trustpoint** *name*
5. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
6. **serial-number** [**none**]
7. **ip-address** {*ip-address* | *interface* | **none**}
8. **subject-name** [*x.500-name*]
9. **enrollment** [**mode**][**retry period** *minutes*][**retry count** *number*] **url** *url* [**pem**]
10. **crl optional** or **revocation-check** *method1* [*method2*[*method3*]]
11. **password** *string*
12. **exit**
13. **crypto ca authenticate** *name* or **crypto pki authenticate** *name*
14. **crypto ca enroll** *name* or **crypto pki enroll** *name*
15. **sip-ua**
16. **crypto signaling** [(**remote-addr** {*ip address* | *subnet mask*}) | **default**] **trustpoint** *trustpoint-name* [**strict-cipher**]
17. **voice service** {**pots** | **voatm** | **vofr** | **voip**}
18. **sip**
19. **url** {**sip** | **sips** | **tel**}
20. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto key generate rsa** {**general-keys** | **usage-keys**} [**label** *key-label*[]**exportable**][**modulus** *modulus-size*][**storage** *device***:**] **Example:** `Router(config)# crypto key generate rsa general-keys label kp1 exportable`	Generates RSA key pairs. Arguments and keywords are as follows: • **general-keys**—Specifies that the general-purpose key pair should be generated. • **usage-keys**—Specifies that two RSA special-usage key pairs should be generated (that is, one encryption pair and one signature pair) instead of one general-purpose key pair. • **label** *key-label*—(Optional) Name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used. • **exportable**—(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router. • **modulus** *modulus-size*—(Optional) IP size of the key modulus in a range from 350 to 2048. If you do not enter the modulus keyword and specify a size, you will be prompted. • storage *device***:**—(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:). **Note** kp1 is a label name that you select.
Step 4	**crypto pki trustpoint** *name* **Example:** `Router(config)# crypto pki trustpoint user1`	Declares the trustpoint that your router should use. Argument is as follows: • *name*—Creates a name for the trustpoint. (If you previously declared the trustpoint and just want to update its characteristics, specify the name you previously created.) **Note** user1 represents the trustpoint name that the user specifies.

	Command or Action	Purpose
Step 5	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **Example:** `Router(config)# rsakeypair kp1`	Specifies which key pair to associate with the certificate. Arguments are as follows: • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exists or if the **auto-enroll regenerate** command is configured. • *key-size*—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • *encryption-key-size*—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.
Step 6	**serial-number** [**none**] **Example:** `Router(ca-trustpoint)# serial-number`	Specifies whether the router serial number should be included in the certificate request. Keywords is as follows: • **none**—(Optional) Specifies that a serial number will not be included in the certificate request.
Step 7	**ip-address** [*ip-address* | *interface* | **none**] **Example:** `Router(ca-trustpoint)# ip-address 172.18.197.154`	Specifies a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request. Arguments and keyword are as follows: • *ip-address*—Specifies a dotted IP address that will be included as "unstructuredAddress" in the certificate request. • *interface*—Specifies an interface, from which the router can get an IP address, that will be included as "unstructureAddress" in the certificate request. • **none**—Specifies that an IP address is not to be included in the certificate request. **Note** This is the IP address of this router.
Step 8	**subject-name** [*x.500-name*] **Example:** `Router(ca-trustpoint)# subject-name CN=172.18.197.154`	Specifies the subject name in the certificate request. Argument is as follows: • *x.500-name*—(Optional) Specifies the subject name used in the certificate request. **Note** This is the IP address of this router.

	Command or Action	Purpose
Step 9	**enrollment** [**mode**][**retry period** *minutes*][**retry count** *number*] **url** *url* [**pem**] **Example:** `Router (ca-trustpoint)# enrollment url http://172.18.193.103`	Specifies the enrollment parameters of a certificate authority (CA). Arguments and keywords are as follows: • **mode**—(Optional) Registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled. • **retry period** *minutes*—(Optional) Specifies the period in which the router will wait before sending the CA another certificate request. The default is 1 minute between retries. (Specify from 1 through 60 minutes.) • **retry count** *number*—(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 through 100 retries.) • **url** *url*—URL of the file system where your router should send certificate requests. For enrollment method options, see the **enrollment url** command. • **pem**—(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request. **Note** This IP address is the CA's IP.
Step 10	**crl optional** or **revocation-check** *method1* [*method2* [*method3*]] **Example:** `Router(ca-trustpoint)# crl optional` `or` `Router(ca-trustpoint)# revocation-check none`	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL or Checks the revocation status of a certificate. Arguments are as follows: • *method1* [*method2* [*method3*]]—Method used by the router to check the revocation status of the certificate. Available methods are as follows: – **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. – **none**—Certificate checking is not required. – **ocsp**—Certificate checking is performed by an online certificate status protocol (OCSP). If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.
Step 11	**password** *string* **Example:** `Router(ca-trustpoint)# password password`	Specifies the revocation password for the certificate. Argument is as follows: • *string*—Name of the password

	Command or Action	Purpose
Step 12	**exit** **Example:** `Router# exit`	Exists the current mode.
Step 13	**crypto ca authenticate** *name* or **crypto pki authenticate** *name* **Example:** `Router(config)# crypto ca authenticate user1` `or` `Router(config)# crypto pki authenticate user1`	Authenticates the CA (by getting the certificate of the CA). Argument is as follows: • *name*—Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command. **Note** This is where you paste the remote root CA certificate (PEM file format).
Step 14	**crypto ca enroll** *name* or **crypto pki enroll** *name* **Example:** `Router(config)# crypto ca name user1` `or` `Router(config)# crypto pki name user1`	Obtains the certificates of your router from the certificate authority. Argument is as follows: • *name*—Specifies the name of the CA. Use the same name when you declared the CA using the **crypto pki trustpoint** command.
Step 15	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 16	**cypto signaling** [(**remote-addr** {*ip address* | *subnet mask*) **default**] **trustpoint** *trustpoint-name* [**strict-cipher**] **Example:** `Router(config-sip-ua)# crypto signaling default trustpoint user1`	Configures the SIP gateway to use its trustpoint when it establishes or accepts TLS connection with a remote device with an IP address. Keywords and arguments are as follows: • **remote-addr** *address*—Associates an IP address to a trustpoint. • **remote-addr** *subnet mask*—Associates a subnet mask to a trustpoint. • **default**—Configures a default trustpoint. • **trustpoint** *string*—Refers to the SIP gateways certificate generated as part of the enrollment process using Cisco IOS PKI commands. • **strict-cipher**—Supports only TLS_RSA_WITH_AES_128_CBC_SHA. **Note** The cipher suite used during the TLS transport handshake is set to TLS_RSA_WITH_AES_128_CBC_SHA.

	Command or Action	Purpose
Step 17	**voice service** {**pots** | **voatm** | **vofr** | **voip**} **Example:** `Router(config)# voice service voip`	Specifies a voice encapsulation type and enters voice service VoIP configuration mode.
Step 18	**sip** **Example:** `Router(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 19	**url** {**sip** | **sips** | **tel**} **Example:** `Router(config-serv-sip)# url sips`	Configures URLs to either the SIP, SIPS, or TEL format for your VoIP SIP calls. Keywords are as follows: • **sip**—Generate URLs in SIP format for VoIP calls. This is the default. • **sips**—Generate URLs in SIPS format for VoIP calls. • **tel**—Generate URLs in TEL format for VoIP calls. **Note** This SIP gateway is now configured to use TLS with endpoints sharing the same CA.
Step 20	**end** **Example:** `Router(conf-serv-sip)# end`	Ends the current mode.

Configuring SIP Gateways to Communicate With SIP Endpoint Over TLS That Uses Different CA

This procedure allows the SIP gateway to communicate with SIP endpoints over TLS that uses a different CA. It consists of the following subtasks:

- Enter user EXEC or privileged EXEC mode
- Enter global configuration mode
- Generate the keypair
- Configure the PKI trustpoint
- Authenticate the trustpoint
- Enroll the trustpoint with the CA
- Have SIP use this trustpoint for TLS connections
- Configure SIP to use TLS
- Import root signed certificate from endpoint using a different CA
- Export our root CA certificate so that it can be imported on the other SIP endpoint

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto key generate rsa** {**general-keys** | **usage-keys**} **label** *key-label*][**exportable**][**modulus** *modulus-size*][**storage** *device***:**]
4. **crypto pki trustpoint** *name*
5. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
6. **serial-number** [**none**]
7. **ip-address** {*ip-address* | *interface* | **none**}
8. **subject-name** [*x.500-name*]
9. **enrollment** [**mode**][**retry period** *minutes*][**retry count** *number*] **url** *url* [**pem**]
10. **crl optional** or **revocation-check** *method1* [*method2*[*method3*]]
11. **password** *string*
12. **exit**
13. **crypto ca authenticate** *name* or **crypto pki authenticate** *name*
14. **crypto ca enroll** *name* or **crypto pki enroll** *name*
15. **sip-ua**
16. **crypto signaling** [(**remote-addr** {*ip address* | *subnet mask*}) | **default**] **trustpoint** *trustpoint-name* [**strict-cipher**]
17. **voice service** {**pots** | **voatm** | **vofr** | **voip**}
18. **sip**
19. **url** {**sip** | **sips** | **tel**}
20. **end**
21. **crypto ca trustpoint** *name* or **crypto pki trustpoint** *name*
22. **enrollment terminal** [**pem**]
23. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
24. **ip-address** {*ip-address* | *interface* | **none**}
25. **password** *string*
26. **crl optional** or **revocation-check** *method1* [*method2* [*method3*]]
27. **serial-number** [**none**]
28. **subject-name** [*x.500-name*]
29. **end**
30. **configure terminal**
31. **crypto ca authenticate** *name* or **crypto pki authenticate** *name*
32. **crypto ca export** *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase* or **crypto pki export** *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*
33. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto key generate rsa** {**general-keys** | **usage-keys**} [**label** *key-label*[]**exportable**][**modulus** *modulus-size*][**storage** *device***:**] **Example:** `Router(config)# crypto key generate rsa general-keys label kp1 exportable`	Generates RSA key pairs. Arguments and keywords are as follows: • **general-keys**—Specifies that the general-purpose key pair should be generated. • **usage-keys**—Specifies that two RSA special-usage key pairs should be generated (that is, one encryption pair and one signature pair) instead of one general-purpose key pair. • **label** *key-label*—(Optional) Name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used. • **exportable**—(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router. • **modulus** *modulus-size*—(Optional) IP size of the key modulus in a range from 350 to 2048. If you do not enter the modulus keyword and specify a size, you will be prompted. • storage *device***:**—(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:). **Note** kp1 is a label name that you select.
Step 4	**crypto pki trustpoint** *name* **Example:** `Router(config)# crypto pki trustpoint user1`	Declares the trustpoint that your router should use. Argument is as follows: • *name*—Creates a name for the trustpoint. (If you previously declared the trustpoint and just want to update its characteristics, specify the name you previously created.) **Note** user1 represents the trustpoint name that the user specifies.

	Command or Action	Purpose
Step 5	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **Example:** `Router(config)# rsakeypair kp1`	Specifies which key pair to associate with the certificate. Arguments are as follows: • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exists or if the **auto-enroll regenerate** command is configured. • *key-size*—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • *encryption-key-size*—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.
Step 6	**serial-number** [**none**] **Example:** `Router(ca-trustpoint)# serial-number`	Specifies whether the router serial number should be included in the certificate request. Keywords is as follows: • **none**—(Optional) Specifies that a serial number will not be included in the certificate request.
Step 7	**ip-address** [*ip-address* | *interface* | **none**] **Example:** `Router(ca-trustpoint)# ip-address 172.18.197.154`	Specifies a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request. Arguments and keyword are as follows: • *ip-address*—Specifies a dotted IP address that will be included as "unstructuredAddress" in the certificate request. • *interface*—Specifies an interface, from which the router can get an IP address, that will be included as "unstructureAddress" in the certificate request. • **none**—Specifies that an IP address is not to be included in the certificate request. **Note** This is the IP address of this router.
Step 8	**subject-name** [*x.500-name*] **Example:** `Router(ca-trustpoint)# subject-name CN=172.18.197.154`	Specifies the subject name in the certificate request. Argument is as follows: • *x.500-name*—(Optional) Specifies the subject name used in the certificate request. **Note** This is the IP address of this router.

	Command or Action	Purpose
Step 9	**enrollment** [**mode**][**retry period** *minutes*][**retry count** *number*] **url** *url* [**pem**] **Example:** `Router (ca-trustpoint)# enrollment url http://172.18.193.103`	Specifies the enrollment parameters of a certificate authority (CA). Arguments and keywords are as follows: • **mode**—(Optional) Registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled. • **retry period** *minutes*—(Optional) Specifies the period in which the router will wait before sending the CA another certificate request. The default is 1 minute between retries. (Specify from 1 through 60 minutes.) • **retry count** *number*—(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 through 100 retries.) • **url** *url*—URL of the file system where your router should send certificate requests. For enrollment method options, see the **enrollment url** command. • **pem**—(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request. **Note** This IP address is the CA's IP.
Step 10	**crl optional** or **revocation-check** *method1* [*method2* [*method3*]] **Example:** `Router(ca-trustpoint)# crl optional` `or` `Router(ca-trustpoint)# revocation-check none`	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL or Checks the revocation status of a certificate. Arguments are as follows: • *method1* [*method2* [*method3*]]—Method used by the router to check the revocation status of the certificate. Available methods are as follows: – **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. – **none**—Certificate checking is not required. – **ocsp**—Certificate checking is performed by an online certificate status protocol (OCSP). If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.
Step 11	**password** *string* **Example:** `Router(ca-trustpoint)# password password`	Specifies the revocation password for the certificate. Argument is as follows: • *string*—Name of the password

	Command or Action	Purpose
Step 12	**exit** **Example:** `Router# exit`	Exists the current mode.
Step 13	**crypto ca authenticate** *name* or **crypto pki authenticate** *name* **Example:** `Router(config)# crypto ca authenticate user1` `or` `Router(config)# crypto pki authenticate user1`	Authenticates the CA (by getting the certificate of the CA). Argument is as follows: • *name*—Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command. **Note** This is where you paste the remote root CA certificate (PEM file format).
Step 14	**crypto ca enroll** *name* or **crypto pki enroll** *name* **Example:** `Router(config)# crypto ca name user1` `or` `Router(config)# crypto pki name user1`	Obtains the certificates of your router from the certificate authority. Argument is as follows: • *name*—Specifies the name of the CA. Use the same name when you declared the CA using the **crypto pki trustpoint** command.
Step 15	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 16	**cypto signaling** [(**remote-addr** {*ip address* | *subnet mask*) **default**] **trustpoint** *trustpoint-name* [**strict-cipher**] **Example:** `Router(config-sip-ua)# crypto signaling default trustpoint user1`	Configures the SIP gateway to use its trustpoint when it establishes or accepts TLS connection with a remote device with an IP address. Keywords and arguments are as follows: • **remote-addr** *address*—Associates an IP address to a trustpoint. • **remote-addr** *subnet mask*—Associates a subnet mask to a trustpoint. • **default**—Configures a default trustpoint. • **trustpoint** *string*—Refers to the SIP gateways certificate generated as part of the enrollment process using Cisco IOS PKI commands. • **strict-cipher**—Supports only TLS_RSA_WITH_AES_128_CBC_SHA. **Note** The cipher suite used during the TLS transport handshake is set to TLS_RSA_WITH_AES_128_CBC_SHA.

	Command or Action	Purpose
Step 17	**voice service** {**pots** | **voatm** | **vofr** | **voip**} **Example:** `Router(config)# voice service voip`	Specifies a voice encapsulation type and enters voice service VoIP configuration mode.
Step 18	**sip** **Example:** `Router(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 19	**url** {**sip** | **sips** | **tel**} **Example:** `Router(config-serv-sip)# url sips`	Configures URLs to either the SIP, SIPS, or TEL format for your VoIP SIP calls. Keywords are as follows: • **sip**—Generate URLs in SIP format for VoIP calls. This is the default. • **sips**—Generate URLs in SIPS format for VoIP calls. • **tel**—Generate URLs in TEL format for VoIP calls. **Note** This SIP gateway is now configured to use TLS with endpoints sharing the same CA.
Step 20	**end** **Example:** `Router(conf-serv-sip)# end`	Ends the current mode.
Step 21	**crypto ca trustpoint** *name* or **crypto pki trustpoint** *name* **Example:** `Router(conf)# crypto ca trustpoint x` or `Router(conf)# crypto pki trustpoint x`	Declares the CA that your router should use. Argument is as follows: • *name*—Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.) **Note** x represents the remote trustpoint being imported.
Step 22	**enrollment terminal** [**pem**] **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual cut-and-paste certificate enrollment. Keyword is as follows: • **pem**—(Optional) Add privacy-enhanced mail (PEM) boundaries to the certificate request. **Note** This means that the enrolled certificate will be cut-and-pasted.

	Command or Action	Purpose
Step 23	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **Example:** `Router(ca-trustpoint)# rsakeypair kp1`	Specifies which key pair to associate with the certificate. Arguments are as follows: • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exists or if the **auto-enroll regenerate** command is configured. • *key-size*—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • *encryption-key-size*—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.
Step 24	**ip-address** [*ip-address* | *interface* | **none**] **Example:** `Router(ca-trustpoint)# ip-address 172.18.197.154`	Specifies a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request. Arguments and keyword are as follows: • *ip-address*—Specifies a dotted IP address that will be included as "unstructuredAddress" in the certificate request. • *interface*—Specifies an interface, from which the router can get an IP address, that will be included as "unstructureAddress" in the certificate request. • **none**—Specifies that an IP address is not to be included in the certificate request. **Note** This is our gateway's IP address.
Step 25	**password** *string* **Example:** `Router(ca-trustpoint)# password password`	Specifies the revocation password for the certificate. Argument is as follows: • *string*—Name of the password
Step 26	**crl optional** or **revocation-check** *method1* [*method2* [*method3*]] **Example:** `Router(ca-trustpoint)# crl optional` or `Router(ca-trustpoint)# revocation-check none`	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL or Checks the revocation status of a certificate. Arguments are as follows: • *method1* [*method2* [*method3*]]—Method used by the router to check the revocation status of the certificate. Available methods are as follows: – **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. – **none**—Certificate checking is not required. – **ocsp**—Certificate checking is performed by an online certificate status protocol (OCSP). If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

	Command or Action	Purpose
Step 27	**serial-number** [**none**] **Example:** `Router(ca-trustpoint)# serial-number`	Specifies whether the router serial number should be included in the certificate request. Keywords is as follows: • **none**—(Optional) Specifies that a serial number will not be included in the certificate request.
Step 28	**subject-name** [*x.500-name*] **Example:** `Router(ca-trustpoint)# subject-name CN=172.18.197.154`	Specifies the subject name in the certificate request. Argument is as follows: • *x.500-name*—(Optional) Specifies the subject name used in the certificate request.
Step 29	**end** **Example:** `Router(ca-trustpoint)# end`	Ends the current mode.
Step 30	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 31	**crypto ca authenticate** *name* or **crypto pki authenticate** *name* **Example:** `Router(config)# crypto ca authenticate x` `or` `Router(config)# crypto pki authenticate x`	Authenticates the CA (by getting the certificate of the CA). Argument is as follows: • *name*—Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command. or Authenticates the CA (by getting the certificate of the CA). Argument is as follows: • *name*—Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command. **Note** This is where you paste the remote root CA certificate (PEM file format).

	Command or Action	Purpose
Step 32	**crypto ca export** *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase* or **crypto pki export** *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase* **Example:** `Router(config)# crypto ca export user1 pem terminal` or `Router(config)# crypto pki export user1 pem terminal`	Exports certificates and RSA keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file. Arguments and keywords are as follows: • *trustpoint*—Name of the trustpoint that the associated certificate and RSA key pair will export. The trustpoint argument must match the name that was specified via the crypto pki trustpoint command. • **terminal**—Certificate and RSA key pair that will be displayed in PEM format on the console terminal. • **url** *url*—URL of the file system where your router should export the certificate and RSA key pairs. • **3des**—Export the trustpoint using the Triple Data Encryption Standard (3DES) encryption algorithm. • ***des***—Export the trustpoint using the DES encryption algorithm. • *passphrase*—Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser. **Note** The CA certificate (first one) is the one which needs to be placed on the remote endpoint. The general purpose certificate must not be exported.
Step 33	**end** **Example:** `Router(config)# end`	Ends the current mode.

Displaying TLS Over TCP Transport Connection Information

This procedure provides a method for observing the details of the TLS over TCP connections owned by SIP on the Cisco IOS SIP gateway.

SUMMARY STEPS

1. **enable**
2. **show sip-ua connections tcp tls brief**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
Step 2	**show sip-ua connections tcp tls brief** **Example:** `Router# show sip-ua connections tcp tls brief`	Displays connection details after a call is made. The following sample output shows multiple calls to multiple destinations. This example show a brief detail example using TLS over TCP (see Examples, page 19).
Step 3	**end** **Example:** `Router(conf-sip-ua)# end`	Ends the current mode.

Examples

The following sample output shows multiple calls to multiple destinations. This example show a brief detail example using TLS over TCP:

```
Router# show sip-ua connections tcp tls brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tls  send msg queue size of 0, recorded for 0.0.0.0:0
```

Clearing TLS Over TCP Transport Connection Information

This procedure provides a method for tearing down existing TLS over TCP connections on the SIP gateway.

Note The established TLS over TCP connections on the SIP gateway are not normally torn down or aged out by the SIP gateway. The TLS over TCP connections on the SIP gateway are normally connected until either the remote end closes the connection or the connection is closed down due to an error or by implementing this procedure.

SUMMARY STEPS

1. **enable**
2. **clear sip-ua tcp tls connection** {**id** *value* [**target** *ip-address*] | [**id** *value*] **target** *ip-address*}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
Step 2	**clear sip-ua tcp tls connection** {**id** *value* [**target** *ip-address*] | [**id** *value*] **target** *ip-address*} **Example:** `Router# clear sip-ua tcp tls connection id 3`	Clears the SIP user-agent TLS over TCP connection. Keywords and arguments are as follows: • **id** *value*—Specifies the ID of the connection that needs to be closed in the SIP TCP process. The *value* argument represents the connection ID. The range is from 1 to 2048. • **target** *ip-address*—Specifies the target address for the connection that needs to be closed in the SIP transport layer. The *ip-address* argument is the target address in the form of **ipv4:***address***:***port*.
Step 3	**end** **Example:** `Router# end`	Ends the current mode.

Configuration Examples for SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport

This section provides the following configuration example:

- SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport: Example, page 20

SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport: Example

The following shows examples of the SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport feature when enabled.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname user1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
```

```
ip subnet-zero
!
!
ip cef
!
!
ip host liotta.com 172.18.201.173
ip name-server 172.18.197.154
!
!
voice-card 0
no dspfarm
!
!
voice service voip
sip
! SIP: Cisco IOS SIP gateway signaling support over TLS transport information
session transport tcp tls
!
! SIP: Cisco IOS SIP gateway signaling support over TLS transport information
crypto pki trustpoint user1
enrollment url http://172.18.193.103:80
serial-number
ip-address 172.18.197.154
password 7 011E0305481F0B0E2F
subject-name CN=172.18.197.154
revocation-check none
rsakeypair kp1
!
! SIP: Cisco IOS SIP gateway signaling support over TLS transport information
crypto pki certificate chain user1
certificate 66
30820233 3082019C A0030201 02020166 300D0609 2A864886 F70D0101 04050030
0F310D30 0B060355 04031304 6D796373 301E170D 30363031 31323135 30383533
5A170D30 36303231 35323232 3634315A 305F3117 30150603 55040313 0E313732
2E31382E 3139372E 31353431 44300F06 03550405 13083336 45384230 42333014
06092A86 4886F70D 01090216 0773696E 6973652E 301B0609 2A864886 F70D0109
08130E31 37322E31 382E3139 372E3135 3430819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C5A4 9A53D8B8 55B2892D 6CE8B7BD D570C78D
433837C9 5AC3CD7E 1BE0BC52 373F0435 2E87F976 ACFBBABA 2E168EBE 52D175B6
44BDFBC3 5A27CE12 E0C09A42 ABC8F5FD EDF27AAC 0E7F545B 0967E0DA 7FBE7151
8ED5E5F7 B3C714F4 B713984A 2E3595DB 57EB3A33 ED00C3F8 156A9D6A CE694492
8C4B973D E9519856 C4249686 53DD0203 010001A3 4F304D30 0B060355 1D0F0404
030205A0 301F0603 551D2304 18301680 14DB2346 8CFF6FC6 DD378A43 9B45B8E2
DF133EC9 6A301D06 03551D0E 04160414 BFD1C42A D70C4DF5 EDA6F2AE EE2CA16F
04120DC4 300D0609 2A864886 F70D0101 04050003 81810066 DB4B7A09 D70DF56C
79FAC2D6 C218D1A3 5AFAC906 B01BE4A0 DBF6A29A 7EF80525 DFC25A06 00AB6BC8
A58F2667 DED82D4F 300A1CCE FD3AB9E4 91C94B83 ABF2E5E9 AA8FAD46 C36EC168
7A5144D5 CC97C9C9 927C3217 AFAA03FD CA2D9575 F2D81807 22540260 3B928CB0
83864CFB 95F0AF92 EF4E41DE D090B4E7 BDB10441 27305C
quit
certificate ca 01
308201F7 30820160 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
0F310D30 0B060355 04031304 6D796373 301E170D 30353032 31353232 31373136
5A170D30 36303231 35323231 3731365A 300F310D 300B0603 55040313 046D7963
7330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100CC60
4C61464C F446D6FF 2DE642CB 9F4AD24F 469F5D7C 875D7EEB C2BCAAEB B4C799FD
DCCCC4EB C4D9FC9E F97B2AB6 F4A1ABFE 4E20DE31 3C147490 D3D1779B 2BD950CA
A62C10AB BB9FD62E 495ECDC3 8A4B9468 3F8B59EB EAC0EEDB AFA5826B 60777D79
91FE7D87 22CA6B28 B09C1FE0 E5ACE916 2AD229B7 A727FDD5 85DC55E2 A0D50203
010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
01FF0404 03020186 301F0603 551D2304 18301680 14DB2346 8CFF6FC6 DD378A43
9B45B8E2 DF133EC9 6A301D06 03551D0E 04160414 DB23468C FF6FC6DD 378A439B
45B8E2DF 133EC96A 300D0609 2A864886 F70D0101 04050003 818100AE 27D9B69A
```

```
8E1D01AF 5CFAAB3C 1DC8866A BEAA832A 1D773B47 09828762 58A83C7A FC0C2ED5
1886267B 56299BDA 998DB834 3CED9495 E57EC757 A91FF38C FCBE288B 250E66BB
24A709CB DE2FB443 55233FCA DCA3397B 25B1086A 141B1649 603D3DCA E7095248
C224C3E6 CE14C91D 07585BF5 5082E3FC C380D1ED 58432D73 DE0EB8
quit
!
application
service blind tftp://172.18.207.15/gw-tcl-scripts/ovaltine/app-h450-transfer.2.0.0.9.tcl
paramspace english index 0
paramspace english language en
paramspace english location tftp://172.18.207.15/gw-tcl-scripts/ovaltine/prompts/en
paramspace english prefix en
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 172.18.197.154 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.197.1
!
!
ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
voice-port 0/3/0
caller-id enable
!
voice-port 0/3/1
caller-id enable type 1
!
!
mgcp behavior rsip-range all
!
!
!
dial-peer voice 1 pots
destination-pattern 777
port 0/3/1
!
dial-peer voice 2 voip
destination-pattern 111
```

```
session protocol sipv2
session target ipv4:172.18.201.177
incoming called-number 9001
dtmf-relay rtp-nte
codec g711ulaw
!
dial-peer voice 5 voip
destination-pattern 9001
session protocol sipv2
session target ipv4:172.18.195.49
incoming called-number 777
dtmf-relay rtp-nte
codec g711ulaw
!
dial-peer voice 333 voip
destination-pattern 333
session protocol sipv2
session target dns:liotta.com
incoming called-number 5550100
codec g711ulaw
!
dial-peer voice 555 voip
destination-pattern 5550101
!SIP: Cisco IOS SIP gateway signaling support over TLS transport information
voice-class sip url sips
session protocol sipv2
session target ipv4:172.18.193.97
codec g711ulaw
!
dial-peer voice 111 voip
destination-pattern 111
session protocol sipv2
session target ipv4:172.18.201.177
codec g711ulaw
!
dial-peer voice 911 voip
destination-pattern 1234
session protocol sipv2
session target ipv4:172.18.197.182
incoming called-number 911
codec g711ulaw
!
sip-ua
! IP: Cisco IOS SIP gateway signaling support over TLS transport information
registrar ipv4:172.18.193.97 expires 3600 tcp tls
! SIP: Cisco IOS SIP gateway signaling support over TLS transport information
crypto signaling default trustpoint user1
!
!
!
!
line con 0
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
!
end
```

Additional References

The following sections provide references related to SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport feature.

Related Documents

Related Topic	Document Title
Cisco IOS Documentation	*Cisco IOS Security Configuration Guide, Release 12.4T*
SIP	*Cisco IOS SIP Configuration Guide*
	Cisco IOS SIP Security Application Guide
	Cisco IOS Voice Configuration Library

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2246	*The TLS Protocol Version 1.0*
RFC 3261	*Session Initiation Protocol*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new, modified, obsolete, and replaced commands only.

clear sip-ua

To clear a SIP UDP, TCP, or TLS over TCP connection, use the **clear sip-ua** command in privileged EXEC mode.

clear sip-ua {**udp** | **tcp** [**tls**]} **connection** {**id** *connection-id* [**target ipv4:***address***:***port*]] | [**id** *connection-id*] **target ipv4:***address***:***port*}

Syntax Description

udp connection	UDP transport layer protocol.
tcp connection	TCP transport layer protocol.
tcp tls connection	(Optional) TLS over TCP transport layer protocol.
id *connection-id*	Specifies the ID of the connection that needs to be closed in the SIP UDP process. The range is from 1 to 2048.
target ipv4:*address***:***port*	Specifies the target address for the connection that needs to be closed in the SIP transport layer.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introducted to replace the **clear sip-ua tcp connection**, **clear sip-ua tcp** [**tls**] **connection**, and **clear sip-ua udp connection** command.

Usage Guidelines

Inappropriate usage of the **clear sip-ua** command without understanding the issue or the implications can lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

Examples

To purge the connection entry only at the upper transport layer, assign the target IP address and port.

```
Router# clear sip-ua udp connection target ipv4:172.18.194.183:5060
```

To purge the connection entry only at the lower TCP/UDP layer, assign the connection ID.

```
Router# clear sip-ua udp connection id 1
```

Note Inappropriate usage of the **clear** command without understanding the issue or the implications would lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

To completely purge a valid connection to target 172.18.194.183, port 5060, consider the following example.

Before executing the **clear sip-ua udp connection** command, running the **show sip-ua connections** command gave the following output.

```
Router# show sip-ua connections udp detail

Total active connections : 1
No. of send failures : 0
```

```
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. udp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

Then execute the **clear sip-ua udp connection** command:

```
Router# clear sip-ua udp connection id 1 target ipv4:172.18.194.183:5060

Purging the entry from sip udp process
Purging the entry from reusable global connection table
```

The final result is that all connections are cleared after executing the **clear sip-ua udp connection** command:

```
Router# show sip-ua connections udp detail

Total active connections : 0
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. udp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:0
```

Related Commands

Command	Description
show sip-ua connections	Displays SIP UA transport connections.
timers connection aging	Sets the time before the SIP UA ages out a TCP and UDP connection.

clear sip-ua tcp connection

To clear a session initiation protocol (SIP) TCP connection, use the **clear sip-ua tcp connection** command in privileged EXEC mode.

clear sip-ua tcp connection {**id** *connection-id* [**target ipv4:***address***:***port*] | [**id** *connection-id*] **target ipv4:***address***:***port*}

Syntax Description

id *connection-id*	Specifies the ID of the connection that needs to be closed in the SIP TCP process. The *connection-id* argument represents the connection ID. The range is from 1 to 2048.
target ipv4:*address***:***port*	Specifies the target address for the connection that needs to be closed in the SIP transport layer.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	This command was replaced by the **clear sip-ua** command.

Usage Guidelines

Inappropriate usage of the **clear sip-ua tcp connection** command can lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

Examples

To cear the connection entry only at the upper transport layer, assign the target IP address and port:

```
Router# clear sip-ua tcp connection target ipv4:172.18.194.183:5060
```

To clear the connection entry only at the lower TCP or User Datagram Protocol (UDP) layer, specify the connection:

```
Router# clear sip-ua tcp connection id 1
```

To completely clear a valid connection to target 172.18.194.183, port 5060, consider the following output example from the **show sip-ua connections** command:

```
Router# show sip-ua connections tcp detail

Total active connections : 1
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
```

```
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

Then execute the **clear sip-ua tcp connection** command:

```
Router# clear sip-ua tcp connection id 1 target ipv4:172.18.194.183:5060

Purging the entry from sip tcp process
Purging the entry from reusable global connection table
```

The result is that all connections are cleared after inputting the **clear sip-ua tcp connection** command:

```
Router# show sip-ua connections tcp detail

Total active connections : 0
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:0
```

Related Commands

Command	Description
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua connections	Displays SIP UA transport connection tabless.
timers connection aging	Sets the time before the SIP UA ages out a TCP and UDP connection.

clear sip-ua tcp tls connection

To clear a session initiation protocol (SIP) TCP connection, use the **clear sip-ua tcp tls connection** command in privileged EXEC mode.

clear sip-ua tcp tls connection {**id** *connection-id* [**target ipv4:***address***:***port*] | [**id** *connection-id*] **target ipv4:***address***:***port*}

Syntax Description

id *connection-id*	Specifies the ID of the connection that needs to be closed in the SIP TCP process. The *connection-id* argument represents the connection ID. The range is from 1 to 2048.
target ipv4:*address***:***port*	Specifies the target address for the connection that needs to be closed in the SIP transport layer.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was replaced by the **clear sip-ua** command.

Usage Guidelines

Inappropriate usage of the **clear sip-ua tcp tls connection** command can lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

Examples

To cear the connection entry only at the upper transport layer, assign the target IP address and port:

```
Router# clear sip-ua tcp tls connection target ipv4:172.18.194.183:5060
```

To clear the connection entry only at the lower TCP or User Datagram Protocol (UDP) layer, specify the connection:

```
Router# clear sip-ua tcp tls connection id 1
```

To completely clear a valid connection to target 172.18.194.183, port 5060, consider the following output example from the **show sip-ua connections** command:

```
Router# show sip-ua connections tcp tls detail

Total active connections : 1
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
```

```
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

Then execute the **clear sip-ua tcp connection** command:

```
Router# clear sip-ua tcp tls connection id 1 target ipv4:172.18.194.183:5060

Purging the entry from sip tcp process
Purging the entry from reusable global connection table
```

The result is that all connections are cleared after inputting the **clear sip-ua tcp connection** command:

```
Router# show sip-ua connections tcp tls detail

Total active connections : 0
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:0
```

Related Commands

Command	Description
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua connections	Displays SIP UA transport connection tabless.
timers connection aging	Sets the time before the SIP UA ages out a TCP and UDP connection.

clear sip-ua udp connection

To clear a SIP UDP connection, use the **clear sip-ua udp connection** command in privileged EXEC mode.

clear sip-ua udp connection {**id** *value* [**target** *ip-address*] | [**id** *value*] **target** *ip-address*}

Syntax Description

id *value*	Specifies the ID of the connection that needs to be closed in the SIP UDP process. The *value* argument represents the value of the connection ID. The range is from 1 to 2048.
target *ip-address*	Specifies the target address for the connection that needs to be closed in the SIP transport layer. The *ip-address* argument is the target address in the form of **ipv4:***address***:***port*.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	This command was replaced by the **clear sip-ua** command.

Usage Guidelines

Inappropriate usage of the **clear sip-ua udp connection** command without understanding the issue or the implications can lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

Examples

To purge the connection entry only at the upper transport layer, assign the target IP address and port.

```
Router# clear sip-ua udp connection target ipv4:172.18.194.183:5060
```

To purge the connection entry only at the lower TCP/UDP layer, assign the connection ID.

```
Router# clear sip-ua udp connection id 1
```

Note Inappropriate usage of the **clear** command without understanding the issue or the implications would lead to erroneous call behavior, inappropriate usage of connections, and failure of calls.

To completely purge a valid connection to target 172.18.194.183, port 5060, consider the following example.

Before executing the **clear sip-ua udp connection** command, running the **show sip-ua connections** command gave the following output.

```
Router# show sip-ua connections udp detail

Total active connections : 1
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
```

```
No. of inactive conn. ageouts : 0
Max. udp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

Then execute the **clear sip-ua udp connection** command:

```
Router# clear sip-ua udp connection id 1 target ipv4:172.18.194.183:5060

Purging the entry from sip udp process
Purging the entry from reusable global connection table
```

The final result is that all connections are cleared after executing the **clear sip-ua udp connection** command:

```
Router# show sip-ua connections udp detail

Total active connections : 0
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
Max. udp send msg queue size of 1, recorded for 172.18.194.183:5060
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:0
```

Related Commands

Command	Description
clear sip-ua tcp connection	Clears a SIP TCP connection.
show sip-ua connections	Displays SIP UA transport connections.
timers connection aging	Sets the time before the SIP UA ages out a TCP and UDP connection.

crypto signaling

To identify the **trustpoint** *trustpoint-name* keyword and argument used during the Transport Layer Security (TLS) handshake that correspond to the remote device address, use the **crypto signaling** command in SIP user agent (UA) configuration mode. To reset to the default **trustpoint** *string*, use the **no** form of this command.

crypto signaling [(**remote-addr** {*ip address* | *subnet mask*}) | **default**] **trustpoint** *trustpoint-name* [**strict-cipher**]

no crypto signaling [(**remote-addr** {*ip address* | *subnet mask*}) | **default**] **trustpoint** *trustpoint-name* [**strict-cipher**]

Syntax Description

remote-addr *ip address*	(Optional) Associates an Internet Protocol (IP) address to a trustpoint.
remote-addr *subnet mask*	(Optional) Associates the subnet mask to a trustpoint.
default	(Optional) Configures the default trustpoint.
trustpoint *trustpoint-name*	Trustpoint trustpoint name refers to the gateways certificate generated as part of the enrollment process using Cisco IOS public-key infrastructure (PKI) commands.
strict-cipher	(Optional) The **strict-cipher** keyword supports only the TLS Rivest, Shamir, and Adelman (RSA) encryption with the Advanced Encryption Standard-128 (AES-128) cipher-block-chaining (CBC) Secure Hash Algorithm (SHA) (TLS_RSA_WITH_AES_128_CBC_SHA) cipher suite. **Note** When the **strict-cipher** keyword is not specified, the SIP TLS process uses the larger set of ciphers depending on the support at the Secure Socket Layer (SSL).

Command Default

The **crypto signaling** command defaults to the SIP URLs.

Command Modes

SIP user agent configuration

Command History

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

Usage Guidelines

The **trustpoint** *trustpoint-name* keyword and argument refer to the gateway's certificate generated as part of the enrollment process using the Cisco IOS PKI commands.

When the gateway has a single certificate, it is used by all the remote devices and is configured by the **default** keyword.

When the gateway has multiple certificates, the default and specific certificates are based on the remote endpoints and are associated to the appropriate **trustpoint** *trustpoint-name* keyword and argument.

Note The cipher suite in this case is the overall set that is supported by the SSL layer on the Cisco IOS gateway.

Examples

The following example configures the gateway to use the **trustpoint** *trustpoint-name* keyword and argument when it establishes or accepts the TLS connection with a remote device with IP address 172.16.0.0:

```
configure terminal
sip-ua
 crypto signaling remote-addr 172.16.0.0 trustpoint user1
```

The following example configures the gateway to use **trustpoint** *trustpoint-name* keyword and argument when it establishes or accepts the TLS connection with any remote devices:

```
configure terminal
sip-ua
 crypto signaling default trustpoint user2
```

The following example configures the gateway to use its **trustpoint** *trustpoint-name* keyword and argument when it establishes or accepts the TLS connection with any remote devices with IP address 172.16.0.0:

```
configure terminal
sip-ua
 crypto signaling remote-addr 172.16.0.0 trustpoint user3 strict-cipher
```

Note The cipher suite used during the TLS handshake in this case is limited to TLS_RSA_WITH_AES_128_CBC_SHA.

Related Commands

Command	Description
sip-ua	Enables the SIP user agent configuration commands.

registrar

To enable Session Initiation Protocol (SIP) gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar, use the **registrar** command in SIP user-agent configuration mode. To disable registration of E.164 numbers, use the **no** form of this command.

registrar {**dns:***address* | **ipv4:***destination-address*} **aor-domain expires** *seconds* [**tcp [tls]**] **type** [**secondary**] [**scheme** *string*]

no registrar [**secondary**]

Syntax Description

dns:*address*	DNS address of the primary SIP registrar server.
ipv4:*destination-address*	IP address of the primary SIP registrar server.
aor-domain	Use address-of-record (AOR) domain name in To/From headers of the outgoing register.
expires *seconds*	Default registration time, in seconds. Range is 60 to 65535. Default is 3600.
tcp	TCP transport layer protocol. When the **tcp** keyword is not selected, UDP is the default.
tls	(Optional) TLS over TCP transport layer protocol. When the **tcp tls** keyword is not selected, UDP is the default.
type	Registration type.
secondary	(Optional) Registration with a secondary SIP proxy or registrar to provide redundancy if the primary registrar fails.
scheme *string*	URL scheme. *String* set to either sip or sips. Default is sip.

Defaults

Registration is disabled.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(6)T	Added the following optional **tls** keyword and keyword and argument: **scheme** *string*.

Usage Guidelines

This command enables the gateway to register E.164 telephone numbers with primary and secondary external SIP registrars.

By default, SIP gateways do not generate SIP register messages.

Examples

The following example specifies registration with a primary and secondary registrar server.

```
.
sip-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar ipv4:10.8.17.40 expires 3600 secondary
.
```

The following example specifies an IP address with TCP.

```
.
sip-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar ipv4:10.8.17.40 tcp
.
```

The following example specifies an IP address with TLS over TCP.

```
.
sip-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar ipv4:10.8.17.40 tcp tls
.
```

The following example specifies a URL scheme with SIP security (SIPS).

```
.
sip-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar ipv4:10.8.17.40 scheme sips
.
```

Related Commands

Command	Description
retry register	Sets the total number of SIP Register messages to send.
show sip-ua register status	Displays the status of E.164 numbers that a SIP gateway has registered with an external primary or secondary SIP registrar.
timers register	Sets how long the SIP UA waits before sending register requests.

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.

Defaults

UDP

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

Command Modes

Dial-peer configuration

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.

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 (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.

Defaults

The default for the command is UDP.

Command Modes

SIP configuration

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.

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.

show sip-ua connections

To display Session Initiation Protocol (SIP) user-agent (UA) transport connection tables, use the **show sip-ua connections** command in privileged EXEC mode.

show sip-ua connections {**tcp [tls]** | **udp**} {**brief** | **detail**}

Syntax Description

tcp	Displays all TCP connection information.
tls	(Optional) Displays all TLS over TCP connection information.
udp	Displays all UDP connection information.
brief	Shows a summary of connections.
detail	Show detailed connection information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced
12.4(6)T	Added the optional **tls** keyword.

Usage Guidelines

The **show sip-ua connections** command should be executed only after a call is made. Use this command to learn the connection details.

Examples

The following is sample output from this command. Table 1 describes significant fields shown in this output.

The example below shows multiple calls to multiple destinations. While this example shows UDP details, the command output looks identical for TCP calls.

```
Router# show sip-ua connections udp detail

Total active connections : 2
No. of send failures : 0
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition
Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060 1 Established 0
```

```
Remote-Agent:172.19.154.18, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060        2       Established   0

Router# show sip-ua connections udp brief

Total active connections      : 0
No. of send failures          : 2
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 5

Router# show sip-ua connections tcp detail

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:172.18.194.183, Connections-Count:1
Remote-Port Conn-Id Conn-State WriteQ-Size
=========== ======= =========== ===========
5060         1      Established   0

Router# show sip-ua connections tcp brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0

Router# show sip-ua connections tcp tls brief

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
No. of handshake errors       : 0
Max. tls send msg queue size of 0, recorded for 0.0.0.0:0
```

Table 1 show sip-ua connections Field Descriptions

Field	Description
Total active connections	Indicates all the connections that the gateway holds for various targets. Statistics are broken down within individual fields.
No. of send failures	Indicates the number of TCP or UDP messages dropped by the transport layer. Messages are dropped if there were network issues and the connection was frequently torn down.
No. of remote closures	Indicates the number of times a remote gateway tore down the connection. A higher value indicates a problem with the network or that the remote gateway does not support reusing the connections (thus it is not RFC 3261 compliant). The remote closure number can also contribute to the number of send failures.
No. of conn. failures	Indicates the number of times that the transport layer was unsuccessful in establishing the connection to the remote agent. The field can also indicate that the address or port configured under the dial peer might be incorrect or that the remote gateway does not support that mode of transport.
No. of inactive conn. ageouts	Indicates the number of times that the connections were torn down or timed out because of signaling inactivity. During call traffic, this number should ideally be zero. If not, it is recommended to tune the inactivity timer to optimize performance by using the **timers** command.
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0	Indicates the number of messages waiting in the queue to be sent out on the TCP connection when the congestion was at its peak. A higher queue number indicates that more messages are waiting to be sent on the network. The growth of this queue size cannot be controlled directly by the administrator.
Tuples with no matching socket entry	Any tuples for the connection entry that are marked with "**" at the end of the line indicate an upper transport layer error condition; specifically, that the upper transport layer is out of sync with the lower connection layer. Cisco IOS software should automatically overcome this condition. If the error continues to persist, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** commands and report the problem to your support team.
Tuples with mismatched address/port entry	Any tuples for the connection entry that is marked with "++" at the end of the line indicate an upper transport layer error condition, where the socket is probably readable, but is hanging and not being used. If the error continues to persist, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection** commands and report the problem to your support team.
Remote-Agent Connections-Count	Connections to the same target address. This field indicates how many connections are established to the same host.
Remote-Port Conn-Id Conn-State WriteQ-Size	Connections to the same target address. This field indicates how many connections are established to the same host. The WriteQ-Size field is relevant only to TCP connections and is a good indicator of network congestion and if there is a need to tune the TCP parameters.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

transport

To configure the Session Initiation Protocol (SIP) user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP, Transport Layer Security (TLS) over TCP, or User Datagram Protocol (UDP) socket, use the **transport** command in SIP user agent configuration mode. To block reception of SIP signaling messages on a particular socket, use the **no** form of this command.

transport {**tcp** [**tls**] | **udp**}

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

Syntax Description

tcp	SIP user agent receives SIP messages on TCP port 5060.
tls	(Optional) SIP user agent receives SIP messages on TLS over TCP port 5060.
udp	SIP user agent receives SIP messages on UDP port 5060.

Defaults

TCP, TLS over TCP, and UDP transport protocols are enabled.

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300 platforms.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XA	This command was implemented on Cisco AS5400 and Cisco AS5350 platforms.
12.2(2)XB1	This command was implemented on Cisco AS5850 platforms.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms were not included in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms in this release.
12.4(6)T	The optional **tls** keyword was added to the command.

Usage Guidelines

This command controls whether messages reach the SIP service provider interface (SPI). Setting **tcp**, **tls** over **tcp**, or **udp** as the protocol causes this to be the protocol for which SIP user agents listen on port 5060.

To block reception of SIP signaling messages on a specific socket, use the **no** form of this command.

To reset this command to the default value, use the **default** command.

Examples

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the UDP socket:

```
sip-ua
 transport udp
```

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the TCP socket:

```
sip-ua
 transport tcp
```

The following example sets the SIP user agent to allow the reception of SIP signaling messages on the TLS over TCP socket:

```
sip-ua
 transport tcp tls
```

Related Commands

Command	Description
sip-ua	Enables the SIP user agent configuration commands.

url (SIP)

To configure URLs to either the Session Initiation Protocol (SIP), SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls, use the **url** command in SIP configuration mode. To reset to the default, use the **no** form of this command.

url {**sip** | **sips** | **tel**}

no url

Syntax Description

sip	Generates URLs in SIP format for VoIP calls.
sips	Generates URLs in SIPS format for VoIP calls.
tel	Generates URLs in TEL format for VoIP calls.

Defaults

SIP URLs

Command Modes

SIP configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
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 Cisco AS5300, Cisco AS5350, and Cisco AS5400 patforms.
12.4(6)T	The **sips** keyword was added to the command.

Usage Guidelines

This command affects only user-agent clients (UACs), because it causes the use of a SIP, SIPS, or TEL URL in the request line of outgoing SIP INVITE requests. SIP URLs indicate the originator, recipient, and destination of the SIP request; TEL URLs indicate voice call connections.

The **voice-class sip url** command, in dial-peer configuration mode, takes precedence over the **url** command in SIP global configuration mode. However, if the **voice-class sip url** command is configured with the **system** keyword, the gateway uses what was globally configured under the **url** command.

Enter SIP configuration mode after entering voice-service VoIP configuration mode, as shown in the Examples section.

Examples

The following example generates URLs in SIP format:

```
voice service voip
sip
 url sip
```

The following example generates URLs in SIPS format:

```
voice service voip
sip
 url sips
```

The following example generates URLs in TEL format:

```
voice service voip
sip
 url tel
```

Related Commands

Command	Description
sip	Enters SIP configuration mode from voice-service VoIP configuration mode.
voice-class sip url	Generates URLs in the SIP, SIPS, or TEL format.

voice-class sip url

To configure URLs to either the Session Initiation Protocol (SIP), SIP security (SIPS), or telephone (TEL) format for your dial-peer SIP calls, use the **voice-class sip url** command in dial-peer configuration mode. To reset to the default value (**system**), use the **no** form of this command.

voice-class sip url {**sip** | **sips** | **system** | **tel**}

no voice-class sip url

Syntax Description

sip	Generates URLs in the SIP format for calls on a dial-peer basis.
sips	Generates URLs in the SIPS format for calls on a dial-peer basis.
system	Uses the system value. This is the default.
tel	Generates URLs in the TEL format for calls on a dial-peer basis.

Defaults

system

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on 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, and Cisco AS5400 platforms.
12.4(6)T	The **sips** keyword was added to the command.

Usage Guidelines

This command affects only user-agent clients (UACs), because it causes the use of a SIP, SIPS, or TEL URL in the request line of outgoing SIP INVITE requests. SIP URLs indicate the originator, recipient, and destination of the SIP request; TEL URLs indicate voice-call connections.

The **voice-class sip url** command, in dial-peer configuration mode, takes precedence over the **url** command in SIP global-configuration mode. However, if the **voice-class sip url** command is used with the **system** keyword, the gateway uses what was globally configured under the **url** command.

Examples

The following example shows how to set up the **voice-class sip url** command to generate URLs in the SIP format:

```
dial-peer voice 102 voip
 voice-class sip url sip
```

The following example shows how to set up the **voice-class sip url** command to generate URLs in the SIPS format:

```
dial-peer voice 102 voip
 voice-class sip url sips
```

The following example shows how to set up the **voice-class sip url** command to generate URLs in the TEL format:

```
dial-peer voice 102 voip
 voice-class sip url tel
```

Related Commands

Command	Description
sip url	Generates URLs in the SIP, SIPS, or TEL format.
url	Configures URLs to either session initiation protocol (SIP), SIP secure (SIPS), or telephone (TEL) format.

Feature Information for SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for <Phrase Based on Module Title>

Feature Name	Releases	Feature Information
SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport	12.4(6)T	This feature module describes the SIP: Cisco IOS SIP Gateway Signaling Support Over TLS Transport feature which implements the Transport Layer Security (TLS) protocol on the Transmission Control Protocol (TCP) transport for Cisco IOS SIP gateways. The feature leverages the existing SIP gateway's support of the public-key infrastructure (PKI) (for certificate management) and utilizes TLS functionality to provide SIP signaling over TLS transport. The use of PKI on the Cisco IOS software requires that the clock on the session initiation protocol (SIP) gateway be synchronized with the network time to ensure proper validation of certificates. The following sections provide information about this feature: • Security Benefits of SIP over TLS Signaling, page 2 • Configuring SIP Gateways to Communicate with SIP Endpoints over TLS That Share the Same CA, page 3 • Configuring SIP Gateways to Communicate With SIP Endpoint Over TLS That Uses Different CA, page 9 • Displaying TLS Over TCP Transport Connection Information, page 18 • Clearing TLS Over TCP Transport Connection Information, page 19 The following commands were introduced or modified by this feature:clear sip-ua, clear sip-ua tcp connection, clear sip-ua tcp tls connection, clear sip-ua udp connection, crypto signaling, registrar, session transport, session transport (SIP), show sip-ua connections, transport, url (SIP), and voice-class sip url.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.