Understanding Session Initiation Protocol (SIP)

Understanding Session Initiation Protocol (SIP) describes SIP and the interaction between SIP and Cisco Unified CallManager.

This section covers the following topics:

SIP Networks

A SIP network uses the following components:

- SIP Proxy Server—The proxy server works as an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
- Redirect Server—The redirect server provides the client with information about the next hop or hops that a message should take, and the client then contacts the next hop server or user agent server directly.
- Registrar Server—The registrar server processes requests from user agent clients for registration of their current location. Redirect or proxy servers often contain registrar servers.
- User Agent (UA)— UA comprises a combination of user agent client (UAC) and user agent server (UAS) that initiates and receives calls. A UAC initiates a SIP request. A UAS, a server application, contacts the user when it receives a SIP request. The UAS then responds on behalf of the user. Cisco Unified CallManager can act as both a server and a client (a back-to-back user agent).

SIP uses a request/response method to establish communications between various components in the network and to ultimately establish a call or session between two or more endpoints. A single session may involve several clients and servers.

Identification of users in a SIP network works through

- A unique phone or extension number.
- A unique SIP address that appears similar to an e-mail address and uses the format `sip:<userID>@<domain>`. The user ID can be either a user name or an E.164 address. Cisco Unified CallManager only supports E.164 addresses; it does not support email addresses.
- An email address format (employee@company.com) that is supported on Cisco Unified CallManager with SIP route patterns.

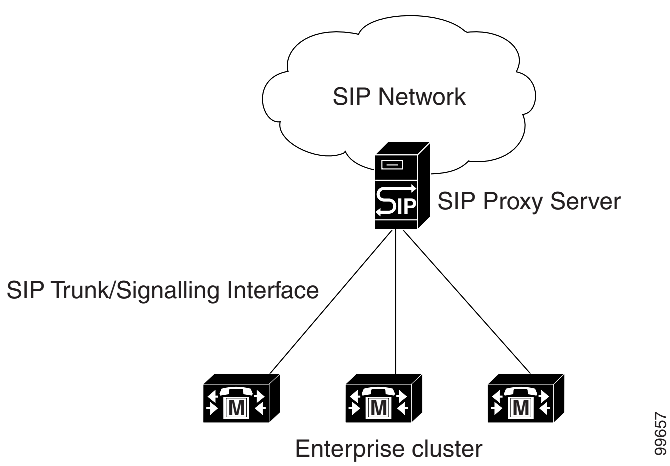
SIP and Cisco Unified CallManager

All protocols require that either a signaling interface (trunk) or a gateway be created to accept and originate calls. For SIP, the user must configure a SIP trunk. For more information, refer to Trunk Configuration in the *Cisco Unified CallManager Administration Guide*.

SIP trunks connect Cisco Unified CallManager networks and SIP networks that are served by a SIP proxy server. As with other protocols, SIP components fit under the device layer of Cisco Unified CallManager architecture. As is true for the H.323 protocol, multiple logical SIP trunks can be configured in the Cisco Unified CallManager database and associated with route groups, route lists, and route patterns. To provide redundancy, in the event of failure of one logical SIP interface, other logical SIP interfaces provide services in the same route group list. Assigning multiple Cisco Unified CallManager nodes under SIP trunk device pools also achieves redundancy.

SIP trunks support multiple port-based routing. Multiple SIP trunks on Cisco Unified CallManager can use port 5060, the default, which is configurable from the SIP Trunk Security Profile Configuration window. For TCP/UDP, SIP trunks use the remote host and local listening port to do the routing (the remote host can be IP, FQDN, or SRV). For TLS, SIP trunks use X.509 Subject Name to do the routing. For SIP trunks, Cisco Unified CallManager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk.

Figure 41-1 SIP and Cisco Unified CallManager Interaction



Media Termination Point (MTP) Devices

You can configure Cisco Unified CallManager SIP devices (lines and trunks) to always use an MTP. If the configuration parameters are set to not use an MTP (default case), Cisco Unified CallManager will attempt to dynamically allocate an MTP if the DTMF methods for the call are not compatible. For example, SCCP phones support only out-of-band DTMF, and Cisco SIP phones (model 7905, 7912, 7940, 7960) support only RFC2833. Because the DTMF methods are not identical, Cisco Unified CallManager will dynamically allocate an MTP. If, however, a SCCP phone that supports RFC2833 and out-of-band, such as Cisco Unified IP Phone 7971, calls a Cisco SIP IP phone 7940, Cisco Unified CallManager will not allocate an MTP because both phones support RFC2833. By having the same type of DTMF method supported on each phone, no need for an MTP exists.

Note While Cisco Unified CallManager provides an MTP Required check box for SIP IP phones, this check box should not be checked for Cisco SIP IP phones. (Only generic third-party SIP IP phones use this check box.) Checking this box can cause problems with Cisco Unified CallManager features such as shared lines. When this check box is not checked, Cisco Unified CallManager will still insert MTPs dynamically as needed. Thus, there is little or no benefit in checking the MTP Required check box for Cisco SIP IP phones.

Configuring Regions (Region Relationship) for SIP Devices with the MTP Required Option Enabled

When you configure a region relationship, you must ensure that you choose an audio codec that has sufficient bandwidth for all the devices that will be used in a call. This includes configuring the codec for devices that will be in the same region as well as devices that are in different regions. When you configure a trunk or third-party phone to use the SIP protocol and Media Termination Point Required is enabled, Cisco Unified CallManager Administration only allows you to choose a G.711 codec in the MTP Preferred Originating Codec field. When you assign the SIP trunk or third-party SIP phone with the MTP Required option enabled to the device pool for that region, you must verify that the region relationship between the SIP device and the MTP device is configured to use a codec with equal or greater bandwidth (G.711 or Wideband codec).

SIP Service Parameters

You can individually configure SIP timers and counters for functionality on different servers. Refer to Service Parameters Configuration in the *Cisco Unified CallManager Administration Guide* for full information on how to configure service parameters.

SIP Timers and Counters

SIP timers and counters act as configurable service parameters. The following tables describe the various SIP timers and counters and give their default values and range values:

Table 41-1 SIP Timers That Are Supported in Cisco Unified CallManager

Timer	Default Value	Default Range	Definition
Trying	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait for a 100 response before retransmitting the INVITE.
Connect	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait for an ACK before retransmitting the 2xx response to the INVITE.
Disconnect	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait for a 2xx response before retransmitting the BYE request.
Expires	180000 milliseconds	60000 to 300000	Valid time that is allowed for an INVITE request.
rel1xx	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait before retransmitting the reliable1xx responses.
PRACK	500 milliseconds	100 to 1000	Time that Cisco Unified CallManager should wait before retransmitting the PRACK request.

Note When using TCP transport and a timer times out, the SIP device does not retransmit. The device relies on TCP to retry.

Table 41-2 SIP Retry Counters That Are Supported in Cisco Unified CallManager

Retry Counter	Default Value	Default Range	Definition
INVITE	6	1 to 10	Number of INVITE retries
Response	6	1 to 10	Number of RESPONSE retries
BYE	10	1 to 10	Number of BYE retries
Cancel	10	1 to 10	Number of Cancel retries
PRACK	6	1 to 10	Number of PRACK retries
Rel1xx	10	1 to 10	Number of Reliable 1xx response retries

Supported Audio Media Types

The following table describes the various supported audio media types:

Table 41-3 Supported Audio Media Types

Type	Encoding Name	Payload Type	Comments
G.711 u-law	PCMU	0	
GSM Full-rate	GSM	3	
G.723.1	G723	4	
G.711 A-law	PCMA	8	
G.722	G722	9	
G.728	G728	15	
G.729	G729	18	Support all combinations of annex A and B
RFC2833 DTMF	Telephony-event	Dynamically Assigned	Acceptable range is 96 - 127

Supported Video Media Types

The following table describes the various supported video media types:

Table 41-4 Supported Video Media Types

Type	Encoding Name	Payload Type
H.261	H261	31
H.263	H263	34
H.263+	H263-1998	Acceptable range is 96 - 127
H.263++	H263-2000	Acceptable range is 96 - 127
H.264	H264	Acceptable range is 96 - 127

Supported Application Media Type

The following table describes the supported application media types:

Table 41-5 Supported Application Media Types

Type	Encoding Name	Payload Type
H.224 FECC	H224	Acceptable range is 96 - 127

Supported T38fax Payload Type

The following table describes the various supported application media types:

Table 41-6 Supported T38fax Payload type

Type	Encoding Name	Payload Type
T38fax	Not applied	Not applicable

SIP Profiles for Trunks

SIP trunks and SIP endpoints use SIP profiles. SIP trunks use SIP profiles to define the Default Telephony Event Payload Type and the Disable Early media on 180. For more information on SIP profiles, see the "SIP Profiles for Endpoints" section on page 41-20 and SIP Profile Configuration in the *Cisco Unified CallManager Administration Guide*.

SIP Functions That Are Supported in Cisco Unified CallManager

Cisco Unified CallManager supports the following functions and features for SIP calls:

Basic Calls Between SIP Endpoints and Cisco Unified CallManager

This section includes three basic calling scenarios. Two scenarios describe incoming and outgoing calls, while the other one describes the use of early media which is a media connection prior to the connection or answer of a call.

Basic Outgoing Call

You can initiate outgoing calls to a SIP device from any Cisco Unified CallManager device. A Cisco Unified CallManager device includes SCCP or SIP IP phones or fax devices that are connected to Foreign Exchange Station (FXS) gateways. For example, an SCCP IP phone can place a call to a SIP endpoint. The SIP device answering the call triggers media establishment.

Basic Incoming Call

Any device on the SIP network, including SIP IP Phones or fax devices that are connected to FXS gateways can initiate incoming calls. For example, a SIP endpoint can initiate a call to an SCCP IP Phone. The SCCP IP phone that answers the call triggers media establishment.

Use of Early Media

While the PSTN provides inband progress information to signal early media (such as a ring tone or a busy signal), the same does not occur for SIP. The originating party includes Session Description Protocol (SDP) information, such as codec usage, IP address, and port number, in the outgoing INVITE message. In response, the terminating party sends its codec, IP address, and port number in a 183 Session Progress message to indicate possible early media.

The 183 Session Progress response indicates that the message body contains information about the media session. Both 180 Alerting and 183 Session Progress messages may contain SDP, which allows an early media session to be established prior to the call being answered.

When early media needs to be delivered to SIP endpoints prior to connection, Cisco Unified CallManager always sends a 183 Session Progress message with SDP. Although Cisco Unified CallManager does not generate a 180 Alerting message with SDP, it does support the 180 Alerting message with SDP when it receives one.

The SIP Profile Configuration window contains a Disable Early Media on 180 check box. Check the check box to play local ringback on the called phone and connect the media upon receipt of the 200OK response. See the "SIP Profile Configuration Settings" section on page 79-2.

DTMF Relay Calls Between SIP Endpoints and Cisco Unified CallManager

MTPs are now dynamically allocated, if needed, based on the DTMF methods used on each endpoint.

Forwarding DTMF Digits from SIP Devices to Gateways or Interactive Voice Response (IVR) Systems for Dissimilar DTMF methods

The following example (Figure 41-2) shows the MTP software device processing inband DTMF digits from the SIP phone to communicate with the Primary Rate Interface (PRI) gateway. The RTP stream carries RFC 2833 DTMF, as indicated by a dynamic payload type.

Figure 41-2 Forwarding DTMF Digits

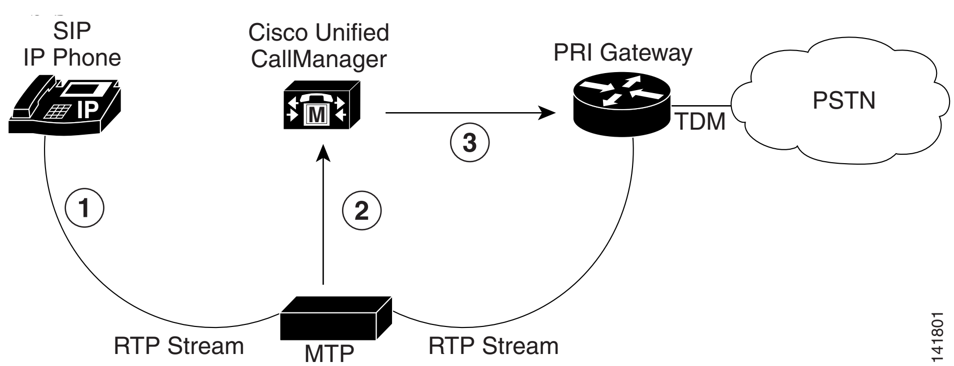


Figure 41-2 begins with media streaming, and the MTP device has been informed of the DTMF dynamic payload type:

1. The SIP phone initiates a payload type response when the user enters a number on the keypad. The SIP phone transfers the DTMF in-band digit (per RFC 2833) to the MTP device.
2. The MTP device extracts the in-band DTMF digit and passes the digit out of band to Cisco Unified CallManager.
3. Cisco Unified CallManager then relays the DTMF digit out of band to the gateway or IVR system.

Generating DTMF Digits for Dissimilar DTMF Methods

As discussed in DTMF Relay Calls Between SIP Endpoints and Cisco Unified CallManager, page 41-7, SIP sends DTMF in-band digits, while Cisco Unified CallManager only supports out-of-band digits. The software MTP device receives the DTMF out-of-band tones and generates DTMF in-band tones to the SIP client.

Figure 41-3 Generating DTMF Digits

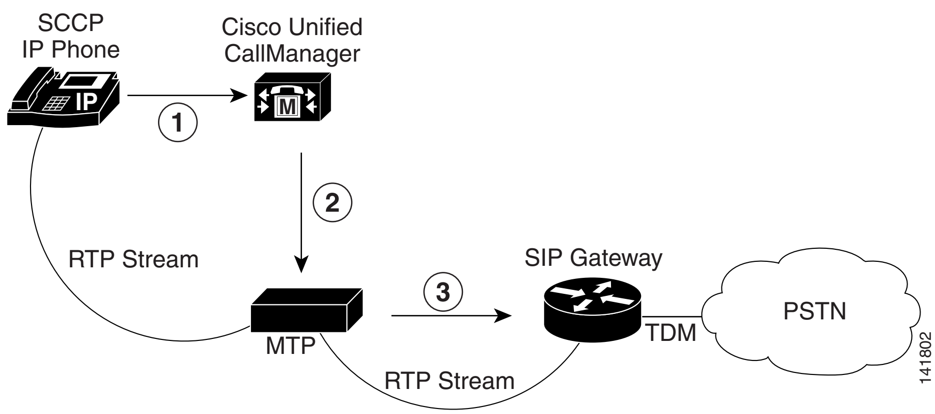


Figure 41-3 begins with media streaming, and the MTP device has been informed of the dynamic DTMF payload type.

1. The SCCP IP phone user presses buttons on the keypad. Cisco Unified CallManager collects the out-of-band digits from the SCCP IP phone.
2. Cisco Unified CallManager passes the out-of-band digits to the MTP device.
3. The MTP device converts the digits to RFC 2833 RTP compliant in-band digits and forwards them to the SIP client.

Supplementary Services That Are Initiated If an MTP Is Allocated

The system supports all supplementary services that the SCCP endpoint initiates during a SIP call. Cisco Unified CallManager internally manages SCCP endpoints without affecting the connecting SIP device. Any changes to the original connecting information get updated with re-INVITE or UPDATE messages that use the Remote-Party-ID header. See *SIP Extensions for Caller Identity and Privacy* for more information on the Remote-Party-ID header.

The section, Ringback Tone During Blind Transfer, page 41-9, describes a blind transfer, which is unique as a supplementary service because it requires Cisco Unified CallManager to provide a media announcement.

Ringback Tone During Blind Transfer

For SCCP initiated blind transfers, Cisco Unified CallManager needs to generate tones or ringback after a call has already connected. In other words, Cisco Unified CallManager provides a media announcement for blind transfers.

A blind transfer works when the transferring phone connects the caller to a destination line before the target of the transfer answers the call. A blind transfer differs from a consultative, or attended transfer, in which one transferring party either connects the caller to a ringing phone (ringback received) or speaks with the third party before connecting the caller to the third party

Blind transfers that are initiated from an SCCP IP phone allow ringback to the original, connected SIP device user. To accomplish ringback, Cisco Unified CallManager uses an annunciator software device that is often located with an MTP device.

With an annunciator, Cisco Unified CallManager can play predefined tones and announcements to SCCP IP phones, gateways, and other IP telephony devices. These predefined tones and announcements provide users with specific information on the status of the call.

Supplementary Services That Are Initiated by SIP Endpoint

The following sections describe supplementary services that a SIP endpoint can initiate.

- SIP–Initiated Call Transfer, page 41-9
- Call Hold, page 41-9
- Call Forward, page 41-9

SIP–Initiated Call Transfer

Cisco Unified CallManager does support SIP-initiated call transfer and does accept REFER requests or INVITE messages that include a Replaces header.

Call Hold

Cisco Unified CallManager supports call hold and retrieve that a SIP device initiates or that a Cisco Unified CallManager device initiates. For example, when a SCCP IP phone user retrieves a call another user placed on hold, Cisco Unified CallManager sends a re-INVITE message to the SIP proxy. The re-INVITE message contains updated Remote-Party-ID information to reflect the current connected party. If Cisco Unified CallManager originally initiated the call, the Party field in the Remote-Party-ID header gets set to calling; otherwise, it gets set to called. For more information on the Party field parameter, see Enhanced Call Identification Services, page 41-10.

Call Forward

Cisco Unified CallManager supports call forward that a SIP device initiates or that a Cisco Unified CallManager device initiates. With call forwarding redirection requests from SIP devices, Cisco Unified CallManager processes the requests. For call forwarding that is initiated by Cisco Unified CallManager, the system uses no SIP redirection messages. Cisco Unified CallManager handles redirection internally and then conveys the connected party information to the originating SIP endpoint through the Remote-Party-ID header.

Enhanced Call Identification Services

This section describes the following SIP identification services in Cisco Unified CallManager and how Cisco Unified CallManager conveys these identification services in the SIP:

- Line Identification Services
  - Calling Line Presentation (CLIP) and Restriction (CLIR)
  - Connected Line Presentation (COLP) and Restriction (COLR)
- Name Identification Services
  - Calling Name Presentation (CNIP) and Restriction (CNIR)
  - Connected Name Presentation (CONP) and Restriction (CONR)

Cisco Unified CallManager provides flexible configuration options to provide these identification services either on a call-by-call, or a statically preconfigured for each SIP signaling interface, basis.

Calling Line and Name Identification Presentation

Cisco Unified CallManager includes the calling line (or number) and name presentation information in the From and Remote-Party-ID headers of the initial INVITE message from Cisco Unified CallManager. The From header field indicates the initiator of the request. Cisco Unified CallManager uses Remote-Party-ID headers in 18x, 200 and re-INVITE messages to convey connected name and identification information. The Remote-Party-ID header also gives detailed descriptions of caller identity and privacy. Cisco Unified CallManager sets the Party field of the Remote-Party-ID header to calling for calling ID services.

Note See the *Cisco IOS SIP Configuration Guide* for more general information on Remote-Party-ID header.

Example

Bob Jones (with external phone number=8005550100) dials out to a SIP signaling interface; the From and Remote-Party-ID headers contain

```
From: "Bob Jones" <sip:8005550100@localhost>
Remote-Party-ID: "Bob Jones"<8005550100@localhost; user=phone>;
party=calling;screen=no;privacy=off
```

Calling Line and Name Identification Restriction

Calling line (or number) and name restrictions configuration occurs on the SIP signaling interface level or on a call-by-call basis. The SIP trunk level configuration takes precedence over the call-by-call configuration. To configure on a call-by-call basis, refer to the Route Group Configuration in the *Cisco Unified CallManager Administration Guide.*

Calling line and name restrictions configuration also occurs independently of each other. For example, you may choose to restrict only numbers and allow names to be presented.

Example 1

With a restricted calling name, Cisco Unified CallManager sets the calling name in the From header to a configurable string. Cisco Unified CallManager sets the display field in the Remote-Party-ID header to include the actual name but sets the Privacy field to name:

```
From: "Anonymous" <sip:8005550100@localhost>
```

```
Remote-Party-ID: "Bob Jones"<sip:9728135001@localhost;user=phone>;
party=calling;screen=no;privacy=name
```

Example 2

With a restricted calling number, Cisco Unified CallManager leaves out the calling line in the From header; however, Cisco Unified CallManager still includes the calling line in the Remote-Party-ID header but sets the Privacy field to privacy=uri:

```
From: "Bob Jones" <sip:@localhost>
Remote-Party-ID: "Bob Jones"<sip:8005550100@localhost;user=phone>;
party=calling;screen=no;privacy=uri
```

Example 3

With a restricted calling name and number, Cisco Unified CallManager sets the Privacy field to privacy=full in the Remote-Party-ID header:

```
From: "Anonymous" <sip:localhost>
Remote-Party-ID: "Bob Jones"<sip:8005550100@localhost;user=phone>;
party=calling;screen=no;privacy=full
```

Connected Line and Name Identification Presentation

Cisco Unified CallManager uses connected line and name identification as a supplementary service to provide the calling party with the connected party's number and name. The From header field indicates the initiator of the request. Cisco Unified CallManager uses Remote-Party-ID headers in 18x, 200 and re-INVITE messages to convey connected information. Cisco Unified CallManager sets the Party field of Remote-Party-ID header to called.

Example 1

Cisco Unified CallManager receives an INVITE message with a destination address of 800555. Cisco Unified CallManager includes the connected party name in 18x and 200 messages as follows:

```
Remote-Party-ID: "Bob Jones"<98005550100@localhost; user=phone>;
party=called;screen=no;privacy=off
```

Connected Line and Name Identification Restriction

You can configure connected line (or number) and name restrictions on the SIP trunk level or on a call-by-call basis. The SIP trunk level configuration takes precedence over the call-by-call configuration. To configure on a call-by-call basis, refer to the Route Group Configuration in the *Cisco Unified CallManager Administration Guide.*

Similar to Calling ID services, users can restrict connected number and name independently of each other.

Example 1

Cisco Unified CallManager sets the display field in the Remote-Party-ID header to include the actual name, but sets the Privacy field to privacy=name:

```
Remote-Party-ID: "Bob Jones"<8005550100@localhost; user=phone>;
party=called;screen=no;privacy=name
```

Example 2

With a restricted connected number, Cisco Unified CallManager still includes the connected number in the Remote-Party-ID header but sets the Privacy field to privacy=uri:

```
Remote-Party-ID: "Bob Jones"<8005550100@localhost; user=phone>;
party=called;screen=no;privacy=uri
```

Example 3

With a restricted connected name and number, Cisco Unified CallManager sets the Privacy field to privacy=full in the Remote-Party-ID header:

```
Remote-Party-ID: "Bob Jones"<8005550100@localhost; user=phone>;
party=called;screen=no;privacy=full
```

Redirecting Dial Number Identification Service (RDNIS)

Cisco Unified CallManager uses the SIP Diversion header in the initial INVITE message to carry available RDNIS information.

Redirection

Previously, the redirection from the SIP network got handled at the SIP stack level, and the system accepted and forwarded all redirection requests to the contacts in the redirection response out to the same trunk on which the redirection response was received. No consulting or applying of any additional logic to handle or restrict how the call is redirected occurred. For example, if the redirection contact in a 3xx response to an outgoing INVITE was a Cisco Unified CallManager registered phone and the stack is handling redirection, the call gets redirected back out over the same trunk instead of being routed directly to the Cisco Unified CallManager phone. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at the stack level will cause the call to be routed instead of being blocked. This represents the behavior you will get if the Redirect by Application check box on the SIP Profile Configuration window is unchecked.

Checking the Redirect by Application check box that is on the SIP Profile Configuration window and configuring this option on the SIP trunk allows the Cisco Unified CallManager administrator to

- Apply a specific calling search space to redirected contacts that are received in the 3xx response.
- Apply digit analysis to the redirected contacts to make sure that the call gets routed correctly.
- Prevent DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set.
- Allow other features to be invoked while the redirection is taking place.

For more information, see the "SIP Profile Configuration Settings" section on page 79-2 and Trunk Configuration in the *Cisco Unified CallManager Administration Guide*.

SIP Trunk Configuration Checklist

Table 41-7 provides an overview of the steps that are required to configure SIP trunk in Cisco Unified CallManager, along with references to related procedures and topics.

Configuration Considerations

Because Cisco Unified CallManager does not perform validation on your configuration, consider the following restrictions when you configure SIP trunks:

- Cisco Unified CallManager does not support outbound MWI notification on a SIP trunk that is assigned to a Route List or a Route Group. If you want Cisco Unified CallManager to send outbound MWI notification on a SIP trunk, you must assign the SIP trunk directly to a route pattern.
- Each SIP trunk must have a unique SIP routing configuration for SIP routing to work. Cisco Unified CallManager uses a combination of information from incoming SIP messages to route the SIP message to the correct SIP trunk. A SIP trunk routing configuration is unique if the following statements apply:
  - No other trunk is configured with the same values for the Incoming Transport Protocol, Incoming Port, and Destination Address fields.
  - No other trunk is configured with Transport Layer Security (TLS) selected as the Incoming Transport Protocol and the same values in the Incoming Port and X.509 Subject Name fields. The X.509 Subject Name parameter can consist of a list of names.

  The Incoming Transport Protocol, Incoming Port, and X.509 Subject Name parameters get configured in SIP Trunk Security Profile Configuration in Cisco Unified CallManager Administration. Choose **System > Security Profile > SIP Trunk Security Profile Configuration**. This menu option yields the Find and List SIP Trunk Security Profile window. Use this window to search for existing SIP Trunk Security Profiles or click **Add New** to add a new profile.

  The Destination Address and the selected SIP Trunk Security profile gets configured on the Trunk Configuration window in Cisco Unified CallManager. Choose **Device-> Trunk**. This menu option yields the Find and List Trunks window. Use this window to search for existing Trunks or click **Add New** to add a new trunk and choose SIP trunk as the Trunk Type.

  The following example shows a valid configuration:

```
Trunk#1: Incoming Transport Protocol=TCP/UDP, Incoming Port=5060, Destination
Address=10.10.10.1
Trunk#2: Incoming Transport Protocol=TCP/UDP, Incoming Port=5060, Destination
Address=10.10.10.2
Trunk#3: Incoming Transport Protocol=TCP/UDP, Incoming Port=5080, Destination
Address=10.10.10.1
Trunk#4: Incoming Transport Protocol=TLS, Incoming Port=5061, X.509 Subject
Name=my_ccm1, my_ccm2
Trunk#5: Incoming Transport Protocol=TLS, Incoming Port=5061, X.509 Subject
Name=my_ccm3
Trunk#6: Incoming Transport Protocol=TLS, Incoming Port=5081, X.509 Subject
Name=my_ccm_1
```

  The following example shows an invalid configuration:

```
Trunk#1: Incoming Transport Protocol=TCP/UDP, Incoming Port=5060, Destination
Address=10.10.10.1
Trunk#2: Incoming Transport Protocol=TCP/UDP, Incoming Port=5060, Destination
Address=10.10.10.1
Trunk#3: Incoming Transport Protocol=TLS, Incoming Port=5061, X.509 Subject
Name=my_ccm1, my_ccm2
Trunk#4: Incoming Transport Protocol=TLS, Incoming Port=5081, X.509 Subject
Name=my_ccm2
Trunk#5: Incoming Transport Protocol=TLS, Incoming Port=5061, X.509 Subject
Name=my_ccm2
Trunk#6: Incoming Transport Protocol=TLS, Incoming Port=5081, X.509 Subject
Name=my_ccm2
```

  Trunk #2 conflicts with Trunk #1 because the protocol, incoming port, and destination address are identical.

Trunk #5 conflicts with Trunk #3 because the protocol and incoming port are identical, and both trunks include my_ccm2 in their list of X.509 Subject Names.

Trunk #6 conflicts with Trunk #4 because the protocol, incoming port, and X.509 Subject Name are identical.

Table 41-7 Trunk Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Create a SIP profile (optional). Create a SIP trunk security profile (optional) Create a SIP trunk. Configure the destination address. Configure the destination port.	Configuring SIP Profiles, *Cisco Unified CallManager Administration Guide* Configuring a Trunk, *Cisco Unified CallManager Administration Guide* Trunk Configuration Settings, *Cisco Unified CallManager Administration Guide*
Step 2	Associate the SIP trunk to a Route Pattern or Route Group.	SIP Route Pattern Configuration, *Cisco Unified CallManager Administration Guide* Route Group Configuration, *Cisco Unified CallManager Administration Guide* Route List Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	Configure SIP timers, counters, and service parameters, if necessary.	Service Parameters Configuration, *Cisco Unified CallManager Administration Guide.* For specific configurable values, see SIP Timers and Counters, page 41-4.
Step 4	Reset the SIP trunk	Configuring a Trunk, *Cisco Unified CallManager Administration Guide*

Cisco Unified CallManager SIP Endpoints Overview

The Cisco SIP IP phones 7911, 7941, 7961, 7970, and 7971 are deployed as a SIP endpoint in a Cisco Unified CallManager Back to Back User Agent (B2BUA) environment. The primary interface between the phone and other network components is the SIP protocol. In addition to SIP, other protocols are used for various functions such as DHCP for IP address assignment, DNS for domain name to address resolution, and TFTP for downloading image and configuration data.

This section provides an example illustration and brief description of the B2BUA and peer-to-peer environments.

Figure 41-4 Cisco Unified CallManager B2BUA Network

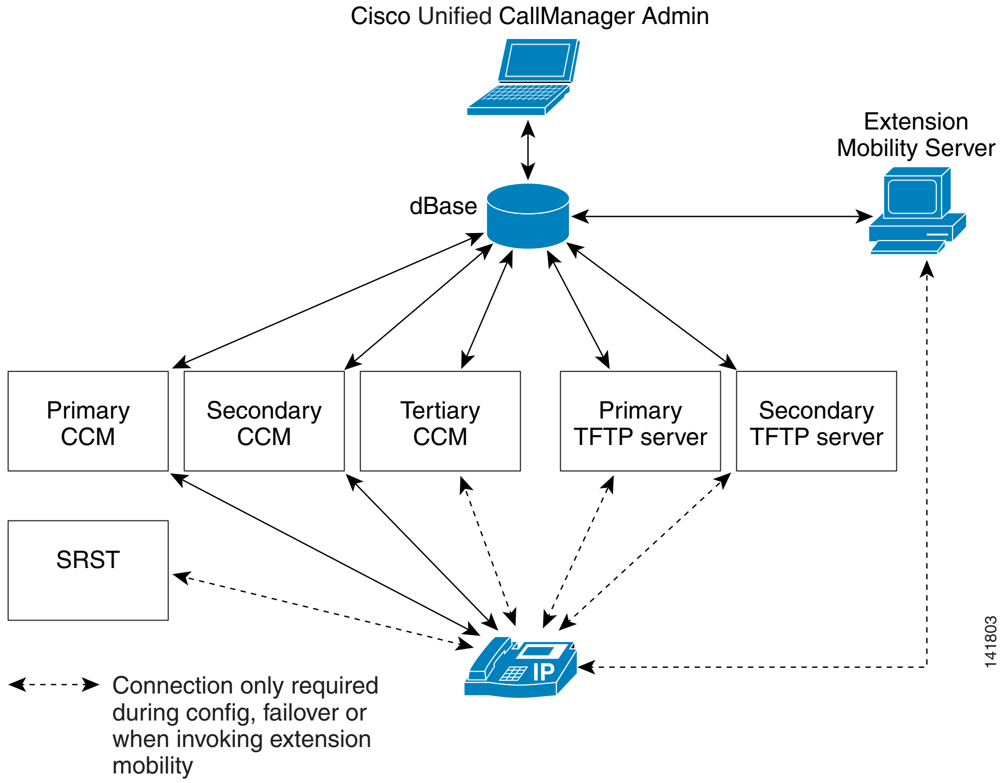


Figure 41-4 shows a simplified example of a Cisco Unified CallManager B2BUA network. There is a main site and a branch office deployment. Each site has a mixture of SIP and SCCP phones. The main site contains the Cisco Unified CallManager cluster and Voice Mail server. Each phone at the main site and the branch office site are homed to a set of primary, secondary, and tertiary Cisco Unified CallManagers. This provides redundancy of call control in the event of the failure of an individual Cisco Unified CallManager server.

SIP phones at the main site direct all session invitations to Cisco Unified CallManager. Based on routing configuration and destination, Cisco Unified CallManager will either extend a call locally to another SIP or SCCP phone, through the main site voice gateway across the IP WAN to one of the phones in the branch office, or through the main site voice gateway to the PSTN. Calls originating from phones in the branch office are routed similarly with the added ability of routing calls to the PSTN through the branch office voice gateway.

The branch office has an SRST gateway deployed for access to the main site IP WAN and for PSTN access. SIP phones in the branch office will direct all session invitations to the Cisco Unified CallManager at the main site. Similarly to the phones at the main site, Cisco Unified CallManager may extend the call to a phone at the main site, through the main site voice gateway across the IP WAN to a phone in the branch office, or to the PSTSN. Depending on the routing configuration of the Cisco Unified CallManager cluster, PSTN calls originating from the phones in the branch office can be routed to the PSTN through the gateway at the main site or they can be routed locally to the PSTN through the branch office gateway.

The SRST gateway also acts as a backup call control server in the event of an IP WAN outage. Both the SIP and SCCP phones will failover to the SRST gateway during a WAN failure. By doing so, the phones in the branch office are able to have their calls routed by the SRST gateway. This includes calls originating and terminating within the branch office and calls originating and terminating in the PSTN.

SIP Line Side Overview

The SIP line side feature affects Cisco Unified CallManager architecture, the TFTP server, and the Cisco Unified IP Phones. The SIP phone features are equivalent to the SCCP phone features and behave similarly. Cisco SIP IP Phones 7941/61/71/70/11 will support all features. Cisco SIP phones 7905/12/40/60 support a reduced feature set (for example, limited MOH and failover capabilities). SIP trunk side applications work for both SCCP and SIP phones.

For detailed information on the SIP phone features capabilities, refer to the user guide for the specific Cisco SIP phone.

SIP Standards

The following SIP standards are supported in Cisco Unified CallManager:

- RFC3261, RFC3262 (PRACK), RFC3264 (offer/answer), RFC3311 (UPDATE), 3PCC, page 41-16
- RFC3515 (REFER) also Replaces and Referred-by Headers, page 41-17
- Remote Party Id (RPID) Header, page 41-17
- Diversion Header, page 41-17
- Replaces Header, page 41-17
- Join Header, page 41-17
- RFC3265 + Dialog Package, page 41-18
- RFC3265 + Presence Package, page 41-18
- RFC3265 + KPML Package, page 41-18
- RFC3265 + RFC3842 MWI Package (unsolicited notify), page 41-18
- Remotecc, page 41-18
- RFC4028 Session Timers, page 41-18

RFC3261, RFC3262 (PRACK), RFC3264 (offer/answer), RFC3311 (UPDATE), 3PCC

This SIP standard supports the following Cisco Unified CallManager features:

- Basic Call
- Hold and Resume
- Music on Hold
- Distinctive Ringing
- Speed dialing
- Abbreviated Dialing
- Call Forwarding (e.g. 486 and 302 support)
- Meet-me
- Pickup, Group Pickup, Other Group Pickup
- 3 way calling (local SIP phone mixing)

- Parked Call Retrieval
- Shared line: Basic Call

RFC3515 (REFER) also Replaces and Referred-by Headers

These SIP standards support the following Cisco Unified CallManager features:

- Consultative Transfer
- Early Attended Transfer
- Blind Transfer

Remote Party Id (RPID) Header

This SIP standard supports the following Cisco Unified CallManager features:

- Calling Line Id (CLID)
- Calling Party Name Id (CNID)
- Dialed Number Id Service (DNIS)
- Call by call Calling Line Id Restriction (call by call CLIR)

RPID is a SIP header used for identification services. RPID is used to indicate the calling, called, and connected remote party information to the other party for identification and call-back, legal intercept, indication of user identification and user location to emergency services, and the identification of users for accounting and billing services.

Diversion Header

This SIP standard supports the following Cisco Unified CallManager features:

- Redirected Number Id Service (RDNIS)
- Call Forward All Activation, Call Forward Busy, Call Forward No Answer

Replaces Header

This SIP standard supports the following Cisco Unified CallManager feature:

- Shared Line: Remote Resume

Join Header

This SIP standard supports the following Cisco Unified CallManager feature:

- Shared Line: Barge

RFC3265 + Dialog Package

This SIP standard supports the following Cisco Unified CallManager feature:

- Shared Line: Remote State Notifications

RFC3265 + Presence Package

These SIP standards support the following Cisco Unified CallManager features:

- BLF on Speed Dial
- BLF on Missed, Placed, Received Calls lists

RFC3265 + KPML Package

These SIP standards support the following Cisco Unified CallManager features:

- Digit Collection
- OOB DTMF

RFC3265 + RFC3842 MWI Package (unsolicited notify)

These SIP standards support the following Cisco Unified CallManager feature:

- Message Waiting Indication

Remotecc

This SIP standard supports the following Cisco Unified CallManager features:

- Adhoc conferencing
- Remove Last Participant
- Conflist
- Immediate Diversion
- Call Park
- Call Select
- Shared Line: Privacy

RFC4028 Session Timers

Allows periodic refresh of the SIP sessions through re-INVITE and allows Cisco Unified CallManager to determine whether the signalling connection to the remote is still active.

Cisco Unified CallManager Functionality Supported by SIP Phones

The following Cisco Unified CallManager functions are supported on Cisco SIP phones:

Dial Plans

Unlike the SCCP phones, the SIP phones collect digits locally before sending them to Cisco Unified CallManager. The SIP phones use a local dial plan to know when enough digits have been entered and to trigger an INVITE with the collected digits. SIP phones that are in SRST mode will continue to use any configured dial plans that they receive from Cisco Unified CallManager. See SIP Dial Rules, page 19-4 for more information.

PLAR

Private Line Automatic Ringdown (PLAR) is a term used by traditional telephony systems that refers to a phone configuration whereby any time the user goes off hook, the phone immediately dials a preconfigured number. The user is unable to dial any other numbers from that phone (or line). This is implemented in for SCCP IP phones in Cisco Unified CallManager by using partitions, calling search space (CSS), and translation patterns; neither the device configuration nor line configuration indicates that PLAR is setup for the phone.

Administrators use SIP Dial Rules for configuring PLAR in SIP phones. Phones configured for PLAR will have a one-line dial plan configuration specifying the appropriate target pattern. When the user goes off hook, the phone will populate the INVITE with the target string and immediately send the request to Cisco Unified CallManager. The user does not enter any digits. See Configuring SIP Dial Rules, page 30-3 for more information.

Softkey Handling

The administrator uses Cisco Unified CallManager Administration to modify the softkey sets that the phone displays. Keys can be added, removed, and their positions can be changed. This data gets written to the database and is sent to the SCCP phone via Station messages as part of the phone registration/initialization process. For Cisco SIP phones, however, instead of sending the keys in Station Messages, the Cisco Unified CallManager TFTP server builds the file that contains the softkey sets. The SIP phone retrieves these files from the TFTP server and the new softkey sets overwrites the softkey sets that are built into the phone. This allows Cisco Unified CallManager to modify the default softkeys and also lets Cisco Unified CallManager manipulate the softkey events, so that it can directly control some phone-level features.

For features that are configured by using the Softkey Configuration window but are not supported by the SIP phone, the softkey will be displayed, but the phone will display a message that the key is not active. This is consistent with the SCCP phone behavior.

The Dial softkey appears as part of the default softkey set when the SIP phone is operating in SRST mode.

Note The Cisco SIP IP Phones 7905, 7912, 7940, and 7960 do not download softkeys. These phones get their softkey configuration in the phone firmware.

DSCP Configuration

Cisco SIP phones get their DSCP information from the configuration file that gets downloaded to the device. The DSCP setting is for the device; whereas, the SCCP phones can get the DSCP setting for a call. DSCP values get configured in the Enterprise Parameters Configuration window, and in the Cisco Unified CallManager Service Parameters Configuration window.

SIP Profiles for Endpoints

Because SIP attributes rarely change, Cisco Unified CallManager uses SIP profiles to define SIP attributes that are associated with SIP trunks and Cisco SIP IP phones. Having these attributes in a profile instead of adding them individually to every SIP trunk and SIP phone decreases the amount of time administrators spend configuring SIP devices and allows the administrator to change the values for a group of devices. Because the SIP profile is a required field when configuring SIP trunks and phones, Cisco Unified CallManager provides a default SIP; however, administrators can create customized SIP profiles. SIP profiles get assigned to SIP devices by using Cisco Unified CallManager Administration.

The software on the SIP phone uses the majority of SIP values that are sent via TFTP to the phones.

For information on configuring SIP profiles, see Configuring SIP Profiles in the *Cisco Unified CallManager Administration Guide*.

Network Time Protocol (NTP)

You can configure phone Network Time Protocol (NTP) references in Cisco Unified CallManager Administration to ensure that a Cisco SIP IP Phone gets its date and time from the NTP server. If all NTP servers do not respond, then the SIP phone uses the date header in the 200 OK response to the REGISTER message for the date and time.

After you add the phone NTP reference to Cisco Unified CallManager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified on the phone page.

For information on configuring the NTP reference, see Phone NTP Reference Configuration in the *Cisco Unified CallManager Administration Guide*.

Where to Find More Information

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*

Related Topics

- Caller Identification and Restriction, page 17-29
- Understanding IP Telephony Protocols, page 40-1
- SIP Networks, page 41-1
- SIP and Cisco Unified CallManager, page 41-2
- SIP Functions That Are Supported in Cisco Unified CallManager, page 41-6
- SIP Trunk Configuration Checklist, page 41-12
- Understanding Cisco Unified CallManager Trunk Types, page 42-1
- Trunk Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Dial Rules Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Profile Configuration, *Cisco Unified CallManager Administration Guide*