Session Initiation Protocol

This chapter provides information about Session Initiation Protocol (SIP) and the interaction between SIP and Cisco Unified Communications Manager.

- SIP Trunk Configuration, page 1
- SIP Phone Configuration, page 1
- SIP Networks, page 1
- SIP and Cisco Unified Communications Manager, page 2
- SIP Functions and Features, page 14
- Cisco Unified Communications Manager SIP Endpoints Overview, page 42
- SIP Line Side Overview, page 44
- SIP Standards, page 44
- Cisco Unified Communications Manager Functionality on SIP Phones, page 47

SIP Trunk Configuration

The Set Up SIP Trunk provides an overview of the steps that are required to configure SIP trunk in Cisco Unified Communications Manager, along with references to related procedures and topics.

SIP Phone Configuration

The Phone Configuration provides an overview of the steps that are required to configure a Cisco Unified IP Phone that runs SIP.

If you want to configure a third-party phone that runs SIP, see the Cisco Unified Communications Manager Administration Guide.

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 behalf of the client. 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 Communications Manager 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 comprise either a user name or an E.164 address. Cisco Unified Communications Manager only supports E.164 addresses; it does not support e-mail addresses.

• An e-mail address format (employee@company.com) that is supported on Cisco Unified Communications Manager with SIP route patterns.

**SIP and Cisco Unified Communications Manager**

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.

SIP trunks connect Cisco Unified Communications Manager networks and SIP networks that are served by a SIP proxy server, as the figure below demonstrates. As with other protocols, SIP components fit under the device layer of Cisco Unified Communications Manager architecture. As is true for the H.323 protocol, you can configure multiple logical SIP trunks in the Cisco Unified Communications Manager database and associate them 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 Communications Manager nodes under SIP trunk device pools also achieves redundancy.

SIP trunks can simultaneously run on all nodes and Cisco Unified Communications Manager can randomly choose from any of the available SIP trunks that can reach a given node. The system ensures that, over time and on average, all 16 nodes in the core cluster are used equally. This practice prevents system resources on some nodes from remaining idle while other nodes handle an unsustainable call burden.
Callback to external numbers is not supported on SIP ICTs.

Figure 1: SIP and Cisco Unified Communications Manager Interaction

SIP trunks support multiple port-based routing. Multiple SIP trunks on Cisco Unified Communications Manager 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 comprise IP, FQDN, or SRV). For TLS, SIP trunks use X.509 Subject Name to do the routing.

For SIP trunks, Cisco Unified Communications Manager 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. After the call is accepted, Cisco Unified Communications Manager uses the configuration for the SIP profile setting, Reroute Incoming Request to new Trunk based on, which is configured on the SIP trunk on which the call arrives, to determine whether the call gets rerouted to another SIP trunk. Depending on the configuration, Cisco Unified Communications Manager may perform one of the following tasks:

- Never reroute to a different SIP trunk.
- Parse the IP address or domain name and port number in the contact header and attempt to match the information to a SIP trunk; if a SIP trunk is found, reroute the call. If no SIP trunk is found, the SIP trunk on which the call arrived handles the call.
- Parse the IP address or domain name and port number in the Call-Info header, look for the parameter, purpose=x-cisco-origIP, and attempt to match the IP address and port to a SIP trunk; if a SIP trunk is found, reroute the call. If no SIP trunk is found or if the parameter does not exist in the Call-Info header, the SIP trunk on which the call arrived handles the call.

Media Termination Point (MTP) Devices

You can configure Cisco Unified Communications Manager 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 Communications Manager will attempt to dynamically allocate an MTP if the DTMF methods for the call are not compatible. For example, phones that are running SCCP support only out-of-band DTMF, and Cisco Unified IP Phones using SIP (7905, 7912, 7940, 7960) support only RFC2833. Because the DTMF methods are not identical, Cisco Unified Communications Manager will dynamically allocate an MTP. If, however, a phone that is
running SCCP that supports RFC2833 and out of band, such as Cisco Unified IP Phone 7971, calls a Cisco
Unified IP Phone 7940 that is using SIP, Cisco Unified Communications Manager 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**

Although Cisco Unified Communications Manager provides an MTP Required check box for SIP IP
phones, you should not check this check box for Cisco Unified IP Phones that are running SIP. (Only
generic, third-party SIP IP phones use this check box.) Checking this check box can cause problems with
Cisco Unified Communications Manager features such as shared lines. When this check box is not checked,
Cisco Unified Communications Manager will still insert MTPs dynamically as needed. Thus, little or no
benefit occurs in checking the MTP Required check box for Cisco Unified IP Phones.

---

### Configure Regions 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 SIP and Media Termination Point Required is enabled, Cisco Unified Communications
Manager 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 phone that is running SIP 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/AAC-LD
(mpeg4-generic) codec).

### SIP Service Parameters

You can individually configure SIP timers and counters for functionality on different servers.

#### SIP Interoperability

The SIP Interoperability Enabled service parameter, which supports the Cisco CallManager service, determines
whether Cisco Unified Communications Manager supports Session Initiation Protocol (SIP) for SIP stations
and SIP trunks. Devices that run SIP, for example, phones and trunks, require that you set this parameter to
True; when you set this parameter to False, Cisco Unified Communications Manager ignores SIP messages,
and SIP devices do not function; that is, phones that run SIP cannot register with Cisco Unified Communications
Manager and SIP trunks cannot interact with Cisco Unified Communications Manager. The default value
specifies True. You must restart the Cisco CallManager service if you change the value of this parameter.

#### 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 1: SIP Timers That Are Supported in Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>Timer</th>
<th>Default Value</th>
<th>Default Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trying</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait for a 100 response before retransmitting the INVITE.</td>
</tr>
<tr>
<td>Connect</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait for an ACK response before retransmitting the 2xx response to the INVITE.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait for a 2xx response before retransmitting the BYE request.</td>
</tr>
<tr>
<td>Expires</td>
<td>180000 milliseconds</td>
<td>60000 to 300000</td>
<td>Valid time that is allowed for an INVITE request.</td>
</tr>
<tr>
<td>rel1xx</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait before retransmitting the reliable1xx responses.</td>
</tr>
<tr>
<td>PRACK</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait before retransmitting the PRACK request.</td>
</tr>
<tr>
<td>PUBLISH</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>This parameter specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager will wait to re-send a PUBLISH request. If a response is not received before the time specified in this timer expires, Cisco Unified Communications Manager re-sends the request when this timer expires.</td>
</tr>
</tbody>
</table>

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

### Table 2: SIP Retry Counters That Are Supported in Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>Retry Counter</th>
<th>Default Value</th>
<th>Default Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>6</td>
<td>1 to 10</td>
<td>Number of INVITE retries</td>
</tr>
<tr>
<td>Response</td>
<td>6</td>
<td>1 to 10</td>
<td>Number of RESPONSE retries</td>
</tr>
</tbody>
</table>
### Retry Counter

<table>
<thead>
<tr>
<th>Retry Counter</th>
<th>Default Value</th>
<th>Default Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYE</td>
<td>10</td>
<td>1 to 10</td>
<td>Number of BYE retries</td>
</tr>
<tr>
<td>Cancel</td>
<td>10</td>
<td>1 to 10</td>
<td>Number of Cancel retries</td>
</tr>
<tr>
<td>PRACK</td>
<td>6</td>
<td>1 to 10</td>
<td>Number of PRACK retries</td>
</tr>
<tr>
<td>Rel1xx</td>
<td>10</td>
<td>1 to 10</td>
<td>Number of Reliable 1xx response retries</td>
</tr>
<tr>
<td>PUBLISH</td>
<td>6</td>
<td>1 to 10</td>
<td>This parameter specifies the number of times that Cisco Unified Communications Manager re-sends the PUBLISH message.</td>
</tr>
</tbody>
</table>

### Supported Audio Media Types

The following table describes the various supported audio media types:

#### Table 3: Supported Audio Media Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 u-law</td>
<td>PCMU</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>GSM Full-rate</td>
<td>GSM</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>G.723.1</td>
<td>G723</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>G.711 A-law</td>
<td>PCMA</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>G.722</td>
<td>G722</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>G.722.1</td>
<td>G7221</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>G.728</td>
<td>G728</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>G.729</td>
<td>G729</td>
<td>18</td>
<td>Support all combinations of annex A and B</td>
</tr>
<tr>
<td>RFC2833 DTMF</td>
<td>Telephony-event</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AAC-LD (mpeg4-generic)</td>
<td>mpeg4-generic</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>
### Supported Video Media Types

The following table describes the various supported video media types:

**Table 4: Supported Video Media Types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>MP4A-LATM</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>ILBC</td>
<td>iLBC</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AMR</td>
<td>AMR</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AMR-WB</td>
<td>AMR-WB</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>

### Supported Application Media Type

The following table describes the supported application media types:

**Table 5: Supported Application Media Types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.261</td>
<td>H261</td>
<td>31</td>
</tr>
<tr>
<td>H.263</td>
<td>H263</td>
<td>34</td>
</tr>
<tr>
<td>H.263+</td>
<td>H263-1998</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>H.263++</td>
<td>H263-2000</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>H.264</td>
<td>H264</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>

### Supported T38fax Payload Type

The following table describes the various supported application media types:

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.224 FECC</td>
<td>H224</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>
Table 6: Supported T38fax Payload Type

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>T38fax</td>
<td>Not applied</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

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, the Disable Early media on 180, and the Reroute Incoming Request to new Trunk based on configuration. For more information on SIP profiles, see the SIP Profiles for Endpoints, on page 51.

SIP Trunk Security Profiles

Cisco Unified Communications Manager Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings. You apply the configured settings to the SIP trunk when you choose the security profile in the Trunk Configuration window.

SIP UDP Port Throttling

SIP UDP port throttle thresholds help prevent Denial of Service (DOS) attacks from SIP trunks and SIP stations. When the incoming packet rate exceeds the configured threshold for a SIP station or SIP trunk UDP port, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold. These throttle thresholds apply only to SIP UDP ports and do not affect SIP TCP or TLS ports.

Tip

Be aware that the enterprise parameter Denial-of-Service Protection Flag must be set to True for these parameter values to take effect.

The following table describes the configurable threshold values:

Table 7: SIP UDP Port Throttling Thresholds

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Default Value</th>
<th>Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Station UDP Port Throttle Threshold</td>
<td>50</td>
<td>10-500</td>
<td>The SIP Station UDP Port Throttle Threshold parameter defines the maximum incoming packets per second that Cisco Unified Communications Manager can receive from a single (unique) IP address that is directed at the SIP station UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.</td>
</tr>
</tbody>
</table>
Definition

The SIP Trunk UDP Port Throttle Threshold defines the maximum incoming packets per second that a SIP trunk can receive from a single (unique) IP address that is directed at the SIP trunk UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Default Value</th>
<th>Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Trunk UDP Port Throttle Threshold</td>
<td>200</td>
<td>10-500</td>
<td>The SIP Trunk UDP Port Throttle Threshold defines the maximum incoming packets per second that a SIP trunk can receive from a single (unique) IP address that is directed at the SIP trunk UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.</td>
</tr>
</tbody>
</table>

Tip

If the incoming packet rate on a SIP trunk UDP port from a single IP address exceeds the configured SIP Trunk UDP Port Throttle Threshold during normal traffic, reconfigure the threshold. When a SIP trunk and SIP station share the same incoming UDP port, Cisco Unified Communications Manager throttles packets based on the higher of the two service parameter values. You must restart the Cisco CallManager service for changes to these parameters to take effect.

SIP Trunks Between Releases of Cisco Unified CallManager and Cisco Unified Communications Manager

Cisco Unified Communications Manager Release 6.0 (and later) and Cisco Unified CallManager Release 4.0 (and later, including 5.x) support TCP and UDP as Transport Types when they are used with SIP trunks. However, release 4.x uses one TCP connection per SIP call; releases 5.x and 6.x and later support multiple SIP calls over the same TCP connection (referred to as TCP connection reuse).

The following Cisco products support TCP; however, not all support TCP Reuse:

- Cisco Unified CallManager Release 4.1 - No TCP Connection Reuse
- Cisco Unified CallManager Release 4.2 - No TCP Connection Reuse
- Cisco Unified CallManager Release 5.0(2) - TCP Connection Reuse
- Cisco Unified CallManager Release 5.1(x)- TCP Connection Reuse
- Cisco Unified Communications Manager Release 6.0(x) and later - TCP Connection Reuse
- Cisco IOS 12.3(8)T and above - TCP Reuse
- Cisco IOS 12.3(8)T and below - No TCP Reuse

The following table lists the SIP trunk connectivity that is supported among Cisco Unified CallManager and Cisco Unified Communications Manager releases and the IOS gateway.
Table 8: SIP Trunk Compatibility Matrix

<table>
<thead>
<tr>
<th></th>
<th>Cisco Unified CallManager Release 4.x</th>
<th>Cisco Unified CallManager 5.x and Cisco Unified Communications Manager 6.x</th>
<th>IOS 12.3(8)T</th>
<th>Below IOS 12.3(8)T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CallManager Release 4.x</td>
<td>UDP/TCP</td>
<td>UDP only</td>
<td>UDP only</td>
<td>UDP/TCP</td>
</tr>
<tr>
<td>Cisco Unified CallManager 5.x and Cisco Unified Communications Manager 6.x and later</td>
<td>UDP only</td>
<td>UDP/TCP</td>
<td>UDP/TCP</td>
<td>UDP only</td>
</tr>
<tr>
<td>IOS 12.3(8)T</td>
<td>UDP only</td>
<td>UDP/TCP</td>
<td>UDP/TCP</td>
<td>UDP only</td>
</tr>
<tr>
<td>Below IOS 12.3(8)T</td>
<td>UDP/TCP</td>
<td>UDP only</td>
<td>UDP/TCP</td>
<td>UDP/TCP</td>
</tr>
</tbody>
</table>

If a Release 6.x (or later) system makes multiple calls over a TCP-based SIP trunk to a 4.x system, the 4.x system will only connect one call. The rest of the calls will not get connected. When using SIP trunks between 4.x and 6.x (or later) systems, you must configure both systems to use UDP as the Outgoing Transport Type, so calls between the release 4.x and 6.x (or later) systems will connect properly.

To configure UDP, use Cisco Unified Communications Manager Administration:

- For Cisco Unified Communications Manager Release 6.0 (and later) that is connecting to a Release 4.x system, choose UDP as the Outgoing Transport Type from the SIP Trunk Security Profile Configuration window.
- For Cisco Unified CallManager Release 4.0 (and later) that is connecting to a Release 6.x (or later) system, choose UDP as the Outgoing Transport Type from the Trunk Configuration window.

**SIP Forking for SIP Trunk**

Call setup (INVITE) requests sent by Cisco Unified Communications Manager on a SIP trunk may be replicated and forwarded to multiple destinations by a SIP proxy (called forking). Cisco Unified Communications Manager supports forking, subject to the following limitations:

- Cisco Unified CallManager Release 4.x does not accept provisional responses (such as 180 Ringing) from more than five destinations. It does not accept a successful response (200 Ok) from any destination that is not among the first five to respond.
- Cisco Unified CallManager Release 5.x and Cisco Unified Communications Manager Release 6.x do not accept provisional responses (such as 180 Ringing) from more than 20 destinations. They do not accept a successful response (200 Ok) from any destination that is not among the first 20 to respond.
• If Cisco Unified CallManager Releases 4.x, Cisco Unified CallManager Release 5.x, and Cisco Unified Communications Manager Release 6.x accept a provisional response (183 Session Progress) that contains a session (media) description, they do accept a successful (200 Ok) response only from the same destination, and they will not accept any change in the session description from the provisional response to the successful response.

• If Cisco Unified CallManager Releases 4.x, Cisco Unified CallManager Release 5.x, and Cisco Unified Communications Manager Release 6.x are configured to acknowledge provisional responses (with the SIP PRACK method), Cisco Unified Communications Manager will not accept provisional responses and/or a successful response from any destination other than the first one to respond.

No other configuration options affect Cisco Unified Communications Manager support of downstream SIP forking.

SIP Transparency and Normalization

Cisco Unified Communications Manager can connect to a variety of endpoints, including PBXs, gateways, and service providers. Each endpoint may implement the SIP protocol differently, which can cause a unique set of interoperability issues. SIP transparency and normalization allow Cisco Unified Communications Manager to interoperate seamlessly with a variety of PBXs and service providers. Normalization allows you to modify incoming and outgoing SIP messages at a protocol level on their way through Cisco Unified Communications Manager. Transparency allows Cisco Unified Communications Manager to pass headers, parameters, and content bodies from one call leg to another.

Normalization

To normalize messages, Cisco Unified Communications Manager allows you to add or update scripts to the system and then associate the scripts with one or more SIP trunks or SIP lines. The normalization scripts that you create allow you to preserve, remove, or change the contents of any SIP headers or content bodies, known or unknown. Normalization scripts can be applied to either SIP trunks in the Trunk Configuration window or they can be applied to SIP lines in the SIP Profile Configuration window.

For inbound messages, normalization occurs just after receiving the message from the network. For outbound messages, normalization occurs just prior to sending the message to the network. Normalization applies to any SIP trunk or SIP line with a script configured against the trunk or SIP profile in Cisco Unified Communications Manager, regardless of the type of device to which the trunk connects on the other side. Normalization occurs per call leg and does not require the other call leg to be SIP. The call can specify SIP line to SIP trunk, SCCP to SIP trunk, MGCP to SIP trunk, H.323 to SIP trunk, and so on.

The script environment (and thus context) is maintained over the life of the SIP trunk or SIP device until the trunk gets reset or the device is reset. The script writer implements a Lua module and provides a set of callback functions to manipulate messages (for example, inbound_INVITE, outbound_180_INVITE, and so on). The environment makes the SIP message and SDP (if present) accessible via a set of APIs.

The Cisco script environment controls memory consumption. If a script exceeds its configured memory usage threshold, an error occurs.

Transparency

Transparency refers to the ability to pass information from one call leg to the other. SIP transparency allows inbound SIP message information, such as proprietary headers, to pass through from one side of the Cisco Unified Communications Manager to the other so that the information gets included in the outbound SIP message.
Transparent pass-through only applies to a SIP trunk to SIP trunk call.

In this release, Cisco Unified Communications Manager supports transparency for the following message types:

- Unknown header (pass-through)
- Unknown parameter (pass-through)
- Unknown content body (pass-through)
- Initial INVITE, reINVITE, UPDATE, INFO, BYE, 18x, 200 (INVITE, UPDATE), 4/5/6xx
- One-to-one transaction when possible (in other words, reINVITE triggers one reINVITE on the other side)

For more information on transparency, see the Developer Guide for SIP Transparency and Normalization.

You can also configure REFER transparency so that Cisco Unified Communications Manager passes on REFER requests to another endpoint rather than acting on them. REFER transparency is key in call center applications, where the agent sending the REFER (initiating the blind transfer) resides in a geographic area remote from both of the other call parties. With REFER transparency, the local Cisco Unified Communications Manager drops from the call when the local agent gets removed. Without REFER transparency, the call signaling remains connected through the Cisco Unified Communications Manager of the agent that initiates the transfer. The load associated with the call and continued use of MTP devices (if allocated during the initial call), remained with the Cisco Unified Communications Manager of the agent initiating the transfer, resulting in signaling delays between the parties in the new call.

You enable REFER transparency by associating the refer-passthrough script or a custom REFER transparency script with one or more SIP trunks on the Trunk Configuration window (Device > Trunk). You must configure the fields in the Normalization Script group box.

For information on creating customer scripts, refer to the Developer Guide for SIP Transparency and Normalization. To upload custom scripts in Cisco Unified Communications Manager, use the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script).

**Tracing for SIP Normalization**

Cisco Unified Communications Manager provides tracing for SIP normalization to provide the following functionality:

- To trace both the nonnormalized and the normalized message for the purpose of debugging call failures
- To allow scripts to produce traces for the purpose of debugging scripts
- To produce traces when scripts fail unexpectedly for the purpose of maintaining the system

To debug scripts and call failures, enable tracing by checking the SDI Enable SIP Call Processing check box on the Trace Configuration window in Cisco Unified Serviceability. This option allows you to trace incoming and outgoing SIP messages before and after normalization.

---

**Note**

SIP Normalization produces traces only if you enable tracing on the Normalization script.

To generate traces from the script for debugging purposes, check the Enable Trace check box that appears in Cisco Unified Communications Manager Administration in the Trunk Configuration window for SIP trunks.
or the SIP Profile Configuration window for SIP lines. When checked, the trace.output and trace.format APIs that are provided to the Lua script writer produce SDI trace.

---

**Note**

Cisco recommends that you enable tracing only while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.

If you enable SDI tracing, Cisco Unified Communications Manager produces additional SDI error-level traces, including the following traces:

- Script failed to load
- Script execution error (bad argument)
- Script aborted (ran too long)

These traces include the following information:

- SIP trunk name or SIP profile name
- Lua script name
- Lua script line number where the failure occurred, if applicable
- Information specific to the failure

**Alarms for SIP Normalization**

Cisco Unified Communications Manager identifies SIP normalization script usage and errors; that is, the system keeps timestamps as to when the script opens and closes as well as when errors and resource warnings occur.

The system generates the following alarms:

- SIPNormalizationScriptOpened
- SIPNormalizationScriptClosed
- SIPNormalizationResourceWarning
- SIPNormalizationScriptError
- SIPNormalizationAutoResetDisabled

To find these alarms, access the CallManager Alarm Catalog in Cisco Unified Serviceability.

**Performance Counters for SIP Normalization**

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including script status and errors. Performance counters operate slightly differently for SIP lines and SIP trunks:

- For SIP lines, each script has only one set of performance counters. This is true even if two endpoints share the same script.
For SIP trunks, each device that has an associated script causes a new instance of these counters to be created. When you disassociate a script from the device, or remove the device from Cisco Unified Communications Manager Administration, the instance of these counters gets removed.

For more information on performance counters, see the Cisco Unified Real-Time Monitoring Tool Administration Guide.

Dependency Records

To find trunks that use a specific normalization script, choose Dependency Records from the Related Links drop-down list box that is provided on the Cisco Unified Communications Manager Administration SIP Normalization Script Configuration window. The Dependency Records Summary window displays information about trunks that are using the script. To find more information about a specific trunk, click the Trunk link; then, click the name of the trunk from the Dependency Records Details window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

SIP Functions and Features

Cisco Unified Communications Manager supports the functions and features in this section for SIP calls.

Basic Calls Between SIP Endpoints and Cisco Unified Communications Manager

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 Communications Manager device. A Cisco Unified Communications Manager 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 that answers 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 thing 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 Communications Manager always sends a 183 Session Progress message with SDP. Although Cisco Unified Communications Manager 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 200 OK response.

**DTMF Relay Calls Between SIP Endpoints and Cisco Unified Communications Manager**

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

**Forward DTMF Digits From SIP Devices to Gateways or Interactive Voice Response (IVR) Systems for Dissimilar DTMF Methods**

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

*Figure 2: Forwarding DTMF Digits*

The previous figure begins with media streaming, and the MTP device has been informed of the DTMF dynamic payload type.

1. The phone that is running SIP initiates a payload type response when the user enters a number on the keypad. The phone that is running SIP transfers the DTMF inband digit (per RFC 2833) to the MTP device.
2. The MTP device extracts the inband DTMF digit and passes the digit out of band to Cisco Unified Communications Manager.
3. Cisco Unified Communications Manager then relays the DTMF digit out of band to the gateway or IVR system.
Generate DTMF Digits for Dissimilar DTMF Methods

As discussed in DTMF Relay Calls Between SIP Endpoints and Cisco Unified Communications Manager, on page 15, SIP sends DTMF inband digits, while Cisco Unified Communications Manager only supports out-of-band digits. The software MTP device receives the DTMF out-of-band tones and generates DTMF inband tones to the SIP client.

**Figure 3: Generating DTMF Digits**

![Figure 3: Generating DTMF Digits]

The figure shown 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 Communications Manager collects the out-of-band digits from the SCCP IP phone.

2. Cisco Unified Communications Manager passes the out-of-band digits to the MTP device.

3. The MTP device converts the digits to RFC 2833 RTP-compliant inband 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 Communications Manager 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 Ringback Tone During Blind Transfer, on page 16 describes a blind transfer, which is unique as a supplementary service because it requires Cisco Unified Communications Manager to provide a media announcement.

Ringback Tone During Blind Transfer

For SCCP-initiated blind transfers, Cisco Unified Communications Manager needs to generate tones or ringback after a call already has connected. In other words, Cisco Unified Communications Manager 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 Communications Manager uses an annunciator software device that is often located with an MTP device.

With an annunciator, Cisco Unified Communications Manager 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 sections which follow describe supplementary services that a SIP endpoint can initiate.

**SIP-Initiated Call Transfer**

Cisco Unified Communications Manager supports SIP-initiated call transfer and accepts REFER requests or INVITE messages that include a Replaces header.

**Call Hold**

Cisco Unified Communications Manager supports call hold and retrieve that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. For example, when a SCCP IP phone user retrieves a call that another user placed on hold, Cisco Unified Communications Manager 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 Communications Manager 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, on page 17.

**Call Forward**

Cisco Unified Communications Manager supports call forward that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. With call forwarding redirection requests from SIP devices, Cisco Unified Communications Manager processes the requests. For call forwarding that is initiated by Cisco Unified Communications Manager, the system uses no SIP redirection messages. Cisco Unified Communications Manager 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 Communications Manager and how Cisco Unified Communications Manager conveys these identification services in the SIP:

- Line Identification Services
  - Calling Line Presentation (CLIP) and Restriction (CLIR)
Cisco Unified Communications Manager 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.

**Call Line and Name Identification Presentation**

Cisco Unified Communications Manager 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 Communications Manager. The From header field indicates the initiator of the request. Cisco Unified Communications Manager 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 Communications Manager sets the Party field of the Remote-Party-ID header to calling for calling ID services.

**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
```

**Call 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, see Enhanced Call Identification Services, on page 17 in the Cisco Unified Communications Manager 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 Communications Manager sets the calling name in the From header to a configurable string. Cisco Unified Communications Manager 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 Communications Manager leaves out the calling line in the From header; however, Cisco Unified Communications Manager 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 Communications Manager 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

SIP CLI Handling Change
Cisco Unified Communications Manager provides a SIP feature that deliver two sets of calling party identities for outgoing SIP calls, and allows selective CLI (Calling Line Identification) for incoming SIP calls based on SIP headers.

Outgoing SIP Call with Two Sets of Identities
When switch-board data is configured on a SIP Trunk, the original caller identification is not overwritten by the data in the SIP headers, for the outgoing sip messages, when the Maintain Original Caller ID DN and Caller Name in Identity Headers are checked.

Outgoing SIP Call with Two Set of Identities - SIP Line
When Maintain Original Caller ID DN and Caller Name in Identity Headers are configured on the SIP Trunk, all outgoing SIP calls are impacted. This feature can also be configured for groups of SIP line devices via SIP Profiles. On the phone section of the SIP profile page, two new text boxes were added named Caller ID DN and Caller Name to mirror the switch-board data on a SIP Trunk. On the trunk section of SIP profile a new checkbox was added called Allow Passthrough of Configured Line Device Caller Information.

Incoming CLI for SIP Calls
Cisco Unified Communications Manager allows you to enhance identity selection, presentation and restriction on SIP interfaces. The addition of new configuration fields used for presentation on the SIP Trunk as well as on the SIP profiles to control corresponding SIP phones provides this new functionality.

With the introduction of the Outgoing Identity feature, an incoming SIP call can have two sets of calling party identities. Incoming CLI (Calling Line Identification) was introduced to aid in selecting the identity for call processing. Selection is controlled via a new list box for Calling Line Identification Presentation.
In some networks, there are two sets of identities maintained, network provided identity (trusted) and user provided identity (non-trusted). In terms of SIP calls, identity headers including P-Asserted-Identity (PAI), P-Preferred-Identity (PPI) and Remote-Party-ID (RPID) carry the network provided identity, while the FROM header carries the user provided identity. Previous releases of Cisco Unified Communications Manager provided only a single set of identities for outgoing calls. The identities in the identity headers and FROM headers were exactly the same and there was no way to differentiate between the network provided identity and the user provided identity. Typically, the administrator configures each user device with a Directory Number (DN) and a display name. An outgoing call from this DN would carry its directory number and display name in both Identity headers and the FROM header. Administrators can also configure another identity on a SIP trunk. This identity, sometimes called a switchboard identity, is used to hide each individual caller's identity. It can be configured on the Caller Information section of a SIP Trunk for outbound calls. The configuration includes two fields, Caller ID DN and Caller Name. The caller's original directory number and display name are overwritten when such configurations are enabled.

Cisco Unified Communications Manager provides configurations where the administrator can enable both the switchboard identity and original caller identity. The switchboard identity is carried in the FROM header and original caller identity will be carried in Identity headers. Such configuration can be enabled for each SIP Trunk or SIP user device.

For the incoming calls from within the network, Cisco Unified Communications Manager provides configurations to accept the network provided identity carried in Identity headers or the user provided identity carried in FROM header. Cisco Unified Communications Manager maintains a single set of identities per call.

---

**Note**

Three different identity headers are supported: PAI, PPI and RPID. Depending on the Call Routing Information configuration on the SIP trunk page, one or two of these headers may be present in an outgoing request or response.

Outgoing Call with Original Caller Identity is configured by default in the Call Routing Information. By default the Remote-Party-Id and Asserted-Identity checkboxes are checked and the Asserted-Type and SIP Privacy fields are set to Default.

To configure an outgoing call with the switchboard identity, set the Caller ID DN and Caller Name on the Calls section of SIP Trunk configuration page. These provide the switchboard identity and hide the caller's identity.

For calls originated from Cisco Unified Communications Manager devices, the Identity headers are set to the line ID of the device and the From header is set to either the same as the Identity header or the switchboard information. This is provision-able and does not require changes in Cisco Unified Communications Manager. On the SIP Trunk Configuration page, there is a new checkbox for Maintain Original Caller ID DN and Caller Name in Identity Headers which is used to control the display name and number of outgoing SIP messages. When enabled for the outgoing SIP messages, the configured value Caller ID DN will not override the phone number and the configured Caller Name will not overwrite the caller name in outgoing Identity headers.

---

**Connected Line and Name Identification Presentation**

Cisco Unified Communications Manager uses connected line and name identification as a supplementary service to provide the calling party with the connected party number and name. The From header field indicates the initiator of the request. Cisco Unified Communications Manager uses Remote-Party-ID headers in 18x, 200, and re-INVITE messages to convey connected information. Cisco Unified Communications Manager sets the Party field of Remote-Party-ID header to called.
Example 1
Cisco Unified Communications Manager receives an INVITE message with a destination address of 800555. Cisco Unified Communications Manager 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.
Similar to Calling ID services, users can restrict connected number and name independently of each other.

Example 1
Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager uses the SIP Diversion header in the initial INVITE message to carry available RDNIS information.

Note
When a call gets redirected from a DN to a voice-mail server/service that is integrated with Cisco Unified Communications Manager using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP Diversion header. This behavior is expected because the diversion header gets used by the Cisco Unified Communications Manager server to choose a mailbox.
Redirection

The following scenario represents the behavior that you will get if the Redirect by Application check box on the SIP Profile Configuration window is unchecked. With this configuration, the redirection from the SIP network is handled at the SIP stack level, and the system accepts and forwards all redirection requests to the address in the Contact header of the redirection response. The call is automatically forwarded out the same trunk on which the redirection response was received. No additional routing logic is applied to handle or restrict how the call is redirected occurs. For example, if the redirection contact in a 3xx response to an outgoing INVITE was a Cisco Unified Communications Manager 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 Communications Manager 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.

If the Redirect by Application check box is checked Cisco Unified Communications Manager passes the Contact header through its routing engine and uses routing logic to forward the redirection request to the address in the Contact header. For SIP requests, if the host portion of the Contact header is not a local Unified CM, a SIP route pattern is required to map the host portion of the Contact header to an outgoing trunk or Unified CM will not be able to route the call.

The Redirect by Application check box allows an 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 information on how Unified CM routes SIP requests, see "Routing of SIP Requests in Unified CM" in the Dial Plan chapter of the Cisco Unified Communications System SRND.

Support of G. Clear Codec for SIP Trunks

The G. Clear (Clear channel) codec enables tandem switching of Digital Signal-0 (DS-0) data circuits through a voice network that uses SIP trunks and Cisco Unified Communications Manager. The G.Clear codec uses 64 kb/s of bandwidth (not including IP packet overhead), which is similar to the G.711 codec. The Cisco Unified Communications Manager selects the codec of a voice call and prioritizes the G. Clear codec ahead of the G.711 mulaw and G.711 alaw codecs in the media table.

You may require the G.Clear codec or the G.729 codec in a region or some other low-bandwidth codec for calls to remote regions. The G.729 codec, which is optimized for speech, uses significantly less bandwidth than the G. Clear codec. Be aware that the G.Clear codec is an option only to explicitly allow it to run in lower bandwidth regions.

G. Clear codec calls require separate Differentiated Services Code Point (DSCP) values in the header of IP packets. This differs from traditional voice codecs and video calls and must be tagged uniquely by the MLPP precedence level. Service parameters apply these capabilities.

G. Clear codec calls maintain consistency throughout the gateway by using the RTP dynamic payload type 125. The dynamic payload type gets statically allocated by using Cisco Unified Communications Manager.
SIP trunk support for the G. Clear codec provides intercluster operability. The codec, which is negotiated as a supported media type in SIP Session Description Protocol (SDP) messaging, gets statically encoded to RTP payload type 125.

**Note**

No G. Clear codec support exists for media termination points.

Support exists for ISDN bearer capability for incoming ISDN data calls (restricted and unrestricted digital) that exit the VoIP network on another T1 PRI trunk.

The following figure shows a typical SIP trunk deployment that has the G.Clear codec enabled.

**Figure 4: SIP Trunk Deployment with G. Clear Codec**

Two SIP service parameters enable the G. Clear codec over SIP trunks: SIP Route Class Naming Authority and SIP Clear Channel Data Route Class Label. The SIP Route Class Naming Authority parameter represents the naming authority and context for the labels that are used in SIP signaling that represent the route class. The value specifies a domain name that is owned by the naming authority. The default specifies cisco.com. To signal a particular route class value, Cisco Unified Communications Manager incorporates the domain name and the appropriate route class label, as defined in the SIP Clear Channel Data Route Class Label service parameter, into the SIP signaling.

The SIP Clear Channel Data Route Class Label represents the clear channel data route class in SIP signaling. This parameter and the SIP Route Class Naming Authority parameter create the complete signaling syntax for the SIP clear channel data route class value. The default specifies ccdata.

Route class signaling proves useful when you are interworking with TDM networks that make routing decisions based on route class and clear-channel data route classes. The default domain name that is specified in the parameter applies to interaction between Cisco switches. You can change the parameter to any vendor- or deployment–specific requirements. The far-end switch should receive the same value that is configured in the parameter.

The following entities do not get supported or are disabled:

- H.323 ICTs with the G. Clear codec do not get supported.
- Skinny Client Control Protocol (SCCP) devices with the G. Clear codec do not get supported.
- T1 and E1 CAS with the G. Clear codec do not get supported.
- RSVP with the G. Clear codec does not get supported.
- MLPP over E1 trunks does not get supported.
- Echo cancellation and zero suppression for outbound G. Clear codec calls gets disabled.
• Frame aligning individual DS-0 circuits that transit the VoIP network do not get supported because terminal equipment takes responsibility for the bonding of the individual DS-0 circuits that are defined by ITU H.244.

• Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager do not work with G. Clear that is enabled.

• DTMF signaling with the G.Clear codec does not get supported

---

**Note**

Cisco Unified Communications Manager ignores DTMF configuration settings for all calls on which G.Clear is advertised in the list of codecs, irrespective of whether G.Clear is chosen as the codec for the call.

---

**Early Offer for G.Clear Calls**

Cisco Unified Communications Manager supports limited early offer for G.Clear data calls (also known as clear channel). The Early Offer for G.Clear Calls feature provides support for third-party SIP user agents that can do early offer to negotiate data calls without using a Media Termination Point. MTPs do not support the G.Clear codec.

If you enable both Media Termination Point Required and Early Offer for G.Clear Calls for a SIP device, the system does not allocate the MTP if the G.Clear codec is present in the offer. The system only allocates the MTP if the call is not G.Clear, and the MTP is required.

The Early Offer for G.Clear Calls feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP), including CCD, G.nX64, and X-CCD.

To enable or disable Early Offer for G.Clear Calls, choose one of the following options on the SIP Profile Configuration window in Cisco Unified Communications Manager Administration:

- Disabled (default)
- CLEARMODE
- CCD
- G.nX64
- X-CCD

---

**Support of Multilevel Precedence and Preemption for SIP Trunks**

Cisco Unified Communications Manager Administration supports Voice over Secured IP (VoSIP) networks with Multilevel Precedence and Preemption (MLPP) for SIP trunks. It adds a Resource Priority and SIP-Reason header to messages. SIP-signaled resources are prioritized by Cisco Unified Communications Manager to free up those resources so that the networks can function during emergencies and congestion. Resource Priority Namespace Network Domains and Resource Priority Namespace Lists can be configured to enable prioritization as required.
Resource Priority Namespace Network Domains

The Resource Priority Namespace Network Domain in SIP signaling is similar to the ISDN precedence Information Element (IE) and ISDN User Part (ISUP) precedence parameters used in legacy TDM MLPP networks.

The Resource Priority Namespace Network Domain is included on outbound calls and based on translation patterns or route patterns directing the call to the SIP trunk. The following messages include the configured Resource Priority Namespace Network Domain:

- INVITE
- UPDATE
- REFER

For inbound calls, the network domain is compared to a list of acceptable network domains. The network domain of an incoming call is examined only if the call terminates to a Cisco Unified Communications Manager endpoint. For all other call types, the network domain is not validated against a local configuration. The configuration of acceptable network domains must be added to the SIP Profile.

SIP trunks can respond to updated precedence signals and the following supplementary services:

- Precedence Call Waiting
- Call Transfer
- Call Forwarding
- Three-way Calling

The following headers, mapping, and queuing are not supported:

- Accept-Resource-Priority header.
- Inclusion of RP header in PRACK and ACK.
- Mapping of precedence levels between namespaces.
- Call queuing and other non-MLPP services.

Support for Secure V.150.1 Modem Over IP Over SIP Trunks

Support for secure V.150.1 based Modem over IP (MoIP) communications between an IP STE and legacy (BRI or analog) Secure Terminal Equipment (STE) across a SIP trunk and an intercluster SIP trunk. SIP trunks transport the Session Description Protocol (SDP) information for outbound calls and signal Cisco Unified Communications Manager when MoIP SDP information is received for inbound calls. Devices can call between clusters by using SIP to negotiate a V.150.1 secure call.

Note

No configuration of MoIP over SIP trunks is required.
Support for G.729a and G.729b Codecs Over SIP Trunks

G.729a and G.729b are low-bandwidth codecs that can be used for calls that are initiated over SIP trunks. Be aware that this feature is required for endpoints that do not support delayed media calls and do not want to use a higher-bandwidth codec, such as G.711.

Because an MTP needs to be pre-allocated for early-offer calls, you must configure an external MTP or transcoder device to use this feature. The software MTP does not support G.729 over SIP trunks. Although this feature supports all four G.729 codecs (G.729, G.729a, G.729b, and G.729ab), the system cannot distinguish between G.729 and G.729a or between G.729b and G.729ab. Therefore, Cisco Unified Communications Manager Administration provides only two options for configuring these codecs on SIP trunks: G729/G729a and G729b/G729ab.

The G.729 codec over SIP trunks applies only to outgoing calls, and incoming calls are not affected. Be aware that the system does not support midcall codec switching from G.729 to any other codec.

Support for SIP T.38 Interoperability with Microsoft Exchange

The T.38 standard comes from the ITU-T Recommendation for real-time transfer of Group 3 facsimile (fax) communication over IP networks. In Cisco Unified Communications Manager, the implementation of T.38 interoperability with Microsoft Exchange enables the system to switch a call from audio to T.38 fax.

The following steps show how the Microsoft Exchange Server establishes a call to a fax machine:

1. The exchange server establishes an audio call with the fax machine.
2. The fax machine send fax tones (CNG) to the exchange server.
3. The exchange server recognizes the fax tones and tries to renegotiate the call as a T.38 fax (or T.38 fax relay) call.

Cisco Unified Communications Manager Administration allows you to configure a SIP Profile that supports T.38 fax communication. This profile applies to SIP trunks only, not phones that are running SIP or endpoints.

Support for QSIG Tunneling Over SIP

Cisco Unified Communications Manager supports interworking between QSIG and SIP messages over a SIP trunk on the IP network toward another Cisco Unified Communications Manager or QSIG-SIP gateway to support QSIG calls and features, such as Message Waiting Indication (MWI), Call Transfer, Call Diversion, Call Back, Call Completion, Path Replacement, and Identification Services. To receive these features, Cisco Unified Communications Manager allows you to configure a SIP trunk with QSIG as the tunneled protocol. For information about how to configure SIP trunks, see Support of G. Clear Codec for SIP Trunks, on page 22 in the Cisco Unified Communications Manager Administration Guide.

Note
Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway.
When you create a SIP trunk with Cisco Intercompany Media Engine (IME) selected as the trunk service type, the default for the Tunneled Protocol field is QSIG. QSIG must be the tunneled protocol for QSIG features to work on a Cisco IME trunk.

---

**Note**

Cisco Unified Communications Manager supports only connection retention mode for Call Back on an a Cisco IME trunk.

---

### SIP PUBLISH

SIP PUBLISH provides the preferred mechanism for Cisco Unified Communications Manager Release 6.0 (and later) to send IP phone presence information to Cisco Unified Presence Release 6.0 (and later) over a SIP trunk because it provides improved performance. PUBLISH also provides presence information on a line basis; for example, for do not disturb and mobility. Only outbound PUBLISH gets supported. (Cisco Unified Communications Manager Release 6.0 [and later] uses SUBSCRIBE/NOTIFY for presence when communicating to Cisco Unified Presence release 1.0.)

PUBLISH represents a SIP method for event state publication. RFC 3903 provides a framework for the publication of event state from a user agent to an entity that is responsible for the composition of this event state and distributing it to interested parties through the SIP Events framework. The mechanism that is described in RFC 3903 can extend to support publication of any event state for which an appropriate event package exists.

In addition, RFC 3903 defines a concrete usage of that framework for the publication of presence state by a presence user agent to a presence compositor.

SIP trunk works with Cisco Unified Presence to provide the presence information for the Cisco Unified Communications Manager registered phones. In release 5.0, Cisco Unified Presence collected the presence information from Cisco Unified CallManager through the SIP subscription mechanism.

The Cisco Unified Communications Manager to Cisco Unified Presence interaction works properly when the SIP subscription mechanism is used; however, this mechanism brings some performance concerns. Both Cisco Unified Communications Manager and Cisco Unified Presence must maintain a separate subscription dialog for each phone that is being watched. Moreover, if a phone is interested by two different users, and each user has a different watch rule, Cisco Unified Presence will issue two different SUBSCRIBE requests to the Cisco Unified Communications Manager SIP trunk for the same number.

In Cisco Unified Communications Manager Release 6.0 (and later), a SIP trunk can use PUBLISH as the mechanism for the presence interaction with Cisco Unified Presence. Cisco Unified Communications Manager acts as the Event Publication Agent (EPA), publishing the presence information of its managed phones; Cisco Unified Presence acts as the Event State Compositor (ESC), receiving the published presence information, aggregating it, and updating the watcher phone displays accordingly.

---

### Cisco Unified Communications Manager and Cisco Unified Presence High-Level Architecture Overview

The figure below shows how Cisco Unified Communications Manager, Cisco Unified Presence, and Cisco Unified IP Phones work together.

- Cisco Unified Communications Manager manages all the IP phones, and Cisco Unified Communications Manager uses the SIP or SCCP interface to control the phones.
• An HTTP interface also exists between the IP phones and Cisco Unified Presence. This interface gets used for Cisco Unified Presence to update phone screens. It also gets used for Cisco Unified Presence to detect user login/logout activities.

• The SIP trunk interface gets used to pass the presence data between Cisco Unified Communications Manager and Cisco Unified Presence.

Figure 5: SIP PUBLISH High-Level Architecture

Cisco Unified Communications Manager Administration Configuration Tips for PUBLISH

The following configuration tips apply to Cisco Unified Communications Manager Administration when a SIP trunk is configured for PUBLISH:

• From the SIP Trunk Configuration window, configure a SIP trunk to access the Cisco Unified Presence (destination address).

Tip

To maximize the distributed performance in a multinode cluster, Cisco recommends that you configure the SIP trunk to use the default device pool.

• From the Service Parameters Configuration window for the Cisco CallManager service, in the CUP PUBLISH Trunk field, choose the SIP trunk that you configured.

• Configure a Cisco Unified Presence end user (User Management > End User Configuration) and assign a licensing unit to the user (System > Licensing > Capabilities Assignment).

• Associate the end user with the line appearance (Device > Phone Configuration). From the Phone Configuration window, click the DN that the user will use to access the Cisco Unified Presence. Click the Associate End Users button. From the Find and List Users window, choose an end user that will access the Cisco Unified Presence.

Note You can associate one line appearance with up to five end users.

• DND Support for SIP Trunk PUBLISH—Because DND is device based in release 6.0 (and later), if a device is changed to the DND state, all Cisco Unified Presence-enabled line appearances that are associated with this device could get published. When a device gets changed to the DND state, DND as
well as the busy/idle status will get published together to give Cisco Unified Presence more flexibility to process the data.

• Shared Lines-If Phone A and Phone B are sharing DN 1000, when a user picks up Phone A and makes a call on the line 1000, Cisco Unified Communications Manager notifies Cisco Unified Presence that line 1000 is busy. This information gives the watcher the illusion that all lines for DN 1000 are busy. This does not represent accurate information because line 1000 on Phone B remains idle. Cisco Unified Communications Manager tells Cisco Unified Presence that line 1000 on Phone A is busy. In release 6.0 (and later), Cisco Unified Communications Manager publishes by line appearance. The system considers a line appearance a (DN, Device) pair.

• Multiple Partitions-When Cisco Unified Communications Manager publishes the presence status of a DN, it also shows the partition in which the DN is associated.

• Associating Username-With shared line and multiple partitions supported, Cisco Unified Presence cannot assume that it works only with one DN for each phone and also one partition across the whole Cisco Unified Communications Manager system. In release 6.0 (and later), because a line appearance can be associated with an end user, a SIP trunk will publish the status of the line appearance on behalf of the end user that is associated with that line appearance, which means it can get used to identify Cisco Unified Presence-enabled lines. If a line appearance is associated with an end user, the system is considered as Cisco Unified Presence-enabled; therefore, its presence information will get published.

**Service Parameters for PUBLISH**

The following Cisco CallManager service parameters get used to configure PUBLISH:

- CUPS PUBLISH Trunk
- Default PUBLISH Expiration Timer
- Minimum PUBLISH Expiration Timer
- Retry Count for SIP Publish
- SIP Publish Timer

**Serviceability Performance Counters**

Cisco Unified Serviceability collects and displays the following PUBLISH-related performance counters:

- SIP_StatsPublishIns
- SIP_StatsPublishOuts
- SIP_StatsRetryPublishOuts
- SIP_StatsRetryRequestsOut

The following performance counters exist in Cisco Unified CallManager Release 5.x, but the PUBLISH feature impacts their values:

- SIP_SummTotalOutReq
- SIP_SummTotalInRes
- SIP_StatsRetryRequestsOut
Security Recommendations

RFC 3903 suggests the use of TLS and digest authentication against issues such as Access Control, Denial of Service Attacks, Replay Attacks, and Man in the Middle Attacks. Because Cisco Unified Communications Manager and Cisco Unified Presence support TLS and digest authentication, no changes occurred in release 6.0. The administrator can configure and enable TLS and digest authentication for Cisco Unified Communications Manager and Cisco Unified Presence. Additionally, you can use IPSec as an alternative to TLS.

BAT Support

The following BAT tools assist in migrating Cisco Unified Presence users to Cisco Unified Communications Manager:

- BAT provides a tool that examines all Cisco Unified Presence licensed users and their primary extensions and associated device line appearances for users after Cisco Unified Communications Manager is upgraded from 5.x to 6.0 (and later). You need this tool during the upgrade/migration of Cisco Unified Presence when connecting to Cisco Unified Communications Manager (because all the backend subscriptions get deleted and the new line appearance-based presence needs to be available for the Cisco Unified Presence users). To perform the migration, BAT uses the Export and Update functions. The export csv format follows: UserID, Device, Directory Number, Partition. The last three columns form a line appearance.

- To access the Export and Update windows, choose **Bulk Administration > Users > Export Line Appearance** and **Bulk Administration > Users > Line Appearance > Update Line Appearance**.

- The Export and Update windows include a check box, Export Line Appearance for CUP User Only (and Update Line Appearance for CUP Users Only). When this check box gets checked, the export or update operation gets performed on the Cisco Unified Presence users. Non-Cisco Unified Presence users do not get exported or updated.

SIP OPTIONS

In Cisco Unified Communications Manager, the SIP OPTIONS method allows a SIP trunk to track the status of remote destinations. By sending outgoing OPTIONS and checking the incoming response message, the SIP trunk knows whether remote peers are ready to receive a new request. The SIP trunk does not attempt to set up new calls to unreachable remote peers; this approach allows for quick failovers.

Cisco Unified Communications Manager uses SIP OPTIONS as a keep-alive mechanism on the SIP trunk. Cisco Unified Communications Manager periodically sends an OPTIONS request to the configured destination address on the SIP trunk. If the remote SIP device fails to respond or returns a SIP error response, Cisco Unified Communications Manager tries to reroute the calls by using other trunks or by using a different address, depending on the configuration.

The OPTIONS request lies outside the context of a call; therefore, the request allows Cisco Unified Communications Manager to detect failures even if no calls are present on the SIP trunk. This approach allows any subsequent calls to be rerouted more quickly. The SIP OPTIONS method prevents calls from incurring large timeout and retry delays before the calls get rerouted.

**Cisco Unified Communications Manager Configuration Tips**

The following configuration tips apply to Cisco Unified Communications Manager Administration when a SIP trunk is configured for OPTIONS:
• Configure a SIP profile to enable SIP OPTIONS. (Use the Device > Device Settings > SIP Profile menu option in Cisco Unified Communications Manager Administration.) Copy the Standard SIP Profile and rename the copy; for example, OPTIONS Profile. Check the Enable OPTIONS Ping to monitor destination status for trunks with service type "None (Default)" check box. SIP OPTIONS is disabled by default.

• From the SIP profile that you created, update the two request timers if necessary. One timer gets used when the SIP trunk is in service or partially in service; the second timer gets used when the SIP trunk is out of service. Cisco Unified Communications Manager initiates the SIP OPTIONS requests to the configured destination address(es) of the SIP trunk by using the configured transport protocol (for example, UDP or TCP).

  Note When the request timers expire, Cisco Unified Communications Manager checks whether it has received responses to all previously sent OPTIONS requests. Cisco Unified Communications Manager does not send any new OPTIONS requests if it is still waiting for responses to previous OPTIONS requests. Thus, the system does not burden the network with multiple concurrent OPTIONS requests.

  • From the SIP profile that you created, set the SIP OPTIONS retry timer and counter.

  • Configure a SIP trunk (if one is not already configured). The trunk service type of the SIP trunk must specify None (default). Dynamic SIP trunks, such as Call Control Discovery, Extension Mobility Cross Clusters, and Intercompany Media Services, are not supported.

  • Use Trunk Configuration to configure the destination information. Multiple destinations can be configured. If the destination address is configured as a host name (instead of a dotted IP address), and multiple addresses are returned, the system sends OPTIONS messages to the returned addresses until a response is received. If no response is received before all returned addresses have been exhausted, the SIP trunk gets marked as "target in down state."

  Note For SIP trunks, Cisco Unified Communications Manager supports up to 16 IP addresses for each DNS SRV and up to 10 IP addresses for each DNS host name. The order of the IP addresses depends on the DNS response and may be identical in each DNS query. The OPTIONS request may go to a different set of remote destinations each time if a DNS SRV record (configured on the SIP trunk) resolves to more than 16 IP addresses, or if a host name (configured on the SIP trunk) resolves to more than 10 IP addresses. Thus, the status of a SIP trunk may change because of a change in the way a DNS query gets resolved, not because of any change in the status of any of the remote destinations.

  • Assign the SIP profile that has OPTIONS Ping enabled to the SIP trunk.

When the destination of a SIP trunk includes or resolves to more than one IP address, call routing uses a random selection algorithm to select the destination IP address for the next call on a SIP trunk. If SIP OPTIONS is enabled for the trunk, the state information for the selected IP address determines whether to send the INVITE or advance to the next destination.

**SIP OPTIONS and Secure SIP Trunks**

The SIP OPTIONS method supports secure SIP trunks for which the Transport Type setting specifies TLS in the SIP trunk security profile. Unlike other requests or responses (such as INVITE), Cisco Unified
Communications Manager does not verify the X.509 Subject Name setting (configured in the SIP trunk security profile) for OPTIONS requests or responses. So, a remote destination can be marked as available based on OPTIONS request or response, but the call setup request (such as INVITE) may fail with a reason code 403 Forbidden. Misconfiguration of the X.509 Subject Name at either the Cisco Unified Communications Manager that sends the OPTIONS request or at the Cisco Unified Communications Manager that receives and responds to the OPTIONS request may cause this failure.

Consider the following two scenarios.

**Scenario 1**

Unified CM 1 sends an OPTIONS request over a SIP trunk to Unified CM 2 and receives a 200 OK response. The X.509 Subject Name in the SIP trunk security profile is misconfigured at Unified CM 2; therefore, Unified CM 2 gets marked as available at Unified CM 1. When the INVITE gets sent from Unified CM 1 to Unified CM 2, Unified CM 2 sends a 403 Forbidden message to Unified CM 1. The following figure illustrates this scenario.

![Figure 6: X.509 Subject Name Verification Failure at Destination](image)

**Scenario 2**

Unified CM 1 sends an OPTIONS request over a SIP trunk to Unified CM 2 and receives a 200 OK response. Unified CM 1 marks Unified CM 2 as available, although the X.509 Subject Name in the SIP trunk security profile is misconfigured at Unified CM 2; therefore, Unified CM 2 gets marked as available at Unified CM 1.
profile is misconfigured at Unified CM 1. In this case, the INVITE request from Unified CM 1 to Unified CM 2 fails. The following figure illustrates this scenario.

**Figure 7: X.509 Subject Name Verification Failure at Source**

![Diagram of X.509 Subject Name Verification Failure at Source]

SIP OPTIONS and Digest Authentication

When digest authentication is enabled for a SIP trunk (the Enable Digest Authentication check box is checked in the corresponding SIP trunk security profile), the remote destination gets marked as available upon receipt of a 401 (Unauthorized) response for the OPTIONS request. After receipt of a 401 response, OPTIONS is resent with the digest credentials; upon credential verification from the remote side, a 200 OK response is received for the OPTIONS request.

For an OPTIONS request where the SIP realm (upon receipt of an initial 401 response) or digest credentials are mismatched (remote side), any subsequent INVITE requests fail, even though the remote destination is marked as available.

Serviceability Alarms

The following alarms support SIP OPTIONS:

- SIPTrunkOOS
- SIPTrunkPartiallyISV
- SIPTrunkISV

SIP Early Offer

To enhance interoperability with third-party SIP devices, Cisco Unified Communications Manager allows you to configure SIP trunks to enable early offer for outgoing voice and video calls without requiring MTP, if media capabilities and media port information of the calling endpoint is available.

Outgoing Call Setup

For outgoing call setup for an early offer trunk, Cisco Unified Communications Manager includes an SDP with the calling device media port, codecs, and IP address of the calling device (when available); inserts an
MTP for early offer only when the media information for the caller is unavailable; and advertises multiple codecs when an MTP that supports multiple codecs gets inserted. In previous releases, Cisco Unified Communications Manager provided early offer SDP only when administrators enabled MTP Required or E2E RSVP on the outgoing SIP trunk. The early offer feature ensures that a higher percentage of outbound early offer SIP trunk calls get made without requiring an MTP, thus reducing the number of MTP resources that are needed and improving interoperability with third-party PBXs.

Cisco Unified Communications Manager supports early offer (without requiring MTP) when one of the following devices initiates the call:

- SIP phones
- SCCP phones with SCCP v20 support, which provides media port information through the getPort capability
- MGCP gateways
- Incoming H323 fast start calls
- Incoming early offer SIP trunk calls

---

**Note**

For endpoints where the media port information is not available (for example, H323 slow start calls or delayed offer SIP calls or legacy SCCP phones), Cisco Unified Communications Manager still allocates an MTP to provide SDP in the initial INVITE.

---

**Note**

For calls that any of the devices in the preceding list initiate, MTP may be needed due to other reasons, such as DTMF/codec mismatch, TRP required on the inbound or outbound trunk, or MTP required on the calling side.

---

**Mid-Call Setup**

Cisco Unified Communications Manager also enhances interoperability with third-party devices during mid-call operations, such as basic hold/resume operations, and during supplementary services, such as transfer and conference. In previous releases, Cisco Unified Communications Manager sent an INVITE with an inactive SDP (a=inactive attribute) to indicate a break in media path, sent a delayed offer INVITE to insert music on hold or to resume the media stream, and expected a send-recv offer SDP in the 200 OK. Because third-party devices often provide an inactive offer SDP in the 200 OK instead of providing a send-recv offer SDP, the media path remains in an inactive state and causes calls to drop.

Cisco Unified Communications Manager allows you to configure a parameter for an early offer SIP trunk so that Cisco Unified Communications Manager suppresses the sending of inactive or send-only SDP in mid-call INVITEs. When this parameter gets enabled, Cisco Unified Communications Manager connects the SIP trunk device directly to the MOH or annunciator device without breaking the existing media stream during call hold or during other feature invocation. Similarly, Cisco Unified Communications Manager connects the SIP trunk device to a line-side device directly during call resume without breaking the MOH or annunciator stream. By preventing the far-end media stream from getting set to inactive, Cisco Unified Communications Manager should always be able to resume the media path.
You should configure the suppression of inactive or sendonly SDP only if you experience interoperability issues with third-party SIP devices during hold-resume or during media resumption for supplementary services. Certain endpoints, such as Cisco Unity Connection, may not work if you enable this configuration.

Get Port Capability Support

Cisco Unified Communications Manager also provides a send-receive SDP in response to a delayed offer invite in an initial call or mid-call on a SIP trunk if the device that connects to a SIP trunk supports the GetPort capability. Cisco Unified Communications Manager provides this functionality regardless of whether the SIP trunk has been configured for early offer. If the device does not support the GetPort capability, Cisco Unified Communications Manager does not insert another MTP to provide a send-receive offer.

If you want to change the amount of time that Cisco Unified Communications Manager waits to receive the audio/video/data port from the SCCP device or MTP after the call is connected, you can configure the Port Received Timer After Call Connection service parameter. If Cisco Unified Communications Manager fails to receive the video port before the time specified in this parameter elapses, the call is initially established with two-way audio only. Two-way video may be established after another offer/answer transaction gets completed. If Cisco Unified Communications Manager fails to receive the audio port before the time specified in this timer expires, Cisco Unified Communications Manager attempts another offer/answer transaction to establish a two-way media path for both audio and video.

Increasing the timer allows more time for Unified CM to receive the port information but may result in delayed audio/video at the start or during the call. If the calling device is a CTI or Unified Video Advantage application using CAST protocol version 3, you may need to adjust the timer to accommodate the time that the application needs to open the connection and get the port information.

Early Offer Limitations and Interactions

The following limitations and interactions apply to the early offer feature:

- The early offer feature requires that your MTP uses IOS version 15.1(2)T or later.
- SRTP and video-Cisco Unified Communications Manager can advertise secure audio and/or video capabilities in the SDP of an initial INVITE, depending on the capabilities of calling device.
- End-to-end (E2E) RSVP-Because E2E RSVP provides an early offer by including an SDP in the initial INVITE, the early offer and E2E RSVP features are mutually exclusive in the SIP Profile Configuration window. When you choose E2E from the RSVP Over SIP drop-down list box, the Early Offer support for voice and video calls (insert MTP if needed) check box gets disabled.
- Single Number Reach (SNR)-When a call gets initiated to trunk single number reach (SNR) destinations from a SIP phone, SCCP v20 phone, or calling device whose media capabilities are available at setup, the INVITE SDP contains the IP address and port of the calling device. When an MTP is required to provide early offer for SNR trunk calls, a separate MTP port gets allocated for each SNR destination.
- IPv6-Cisco Unified Communications Manager sends delayed offer INVITEs for the following IPv6 scenarios, even if you have configured early offer on a SIP trunk:
  - SIP trunk is configured in IPv6 only mode.
  - Calling device is in IPv6 only mode.
  - SIP trunk is in dual mode and ANAT is enabled.
• SIP trunk is in dual mode and Media Address Preference is IPv6.

• For the delayed offer SIP call to early offer interworking case, Cisco Unified Communications Manager inserts an MTP to provide SDP on the outgoing call leg. The INVITE contains audio lines only. The INVITE that is sent on the outgoing leg includes audio media lines only. The calling video capabilities and cryptographic key of the device are not available to the tandem cluster; thus, no cryptographic attribute for audio or video media line exists. As a result, the outgoing INVITE SDP contains the IP and audio port of the MTP and no SRTP key or attributes in the audio media line and no video media lines.

• For the slow start H323 calls to early offer interworking case, Cisco Unified Communications Manager inserts an MTP to provide SDP on the outgoing call leg. The INVITE contains audio lines only. The INVITE sent on the outgoing leg includes audio media lines only. The calling video capabilities and cryptographic key of the device are not available to the tandem cluster; thus, no cryptographic attribute for audio or video media line exists. As a result, the outgoing INVITE SDP contains the IP and audio port of the MTP and no SRTP key or attributes in the audio media line and no video media lines. Cisco Unified Communications Manager escalates to video after it receives video TCS from H323 leg after media cut-through and if call admission control (CAC) allows video and the allocated MTP supports pass-through and multimedia.

• Cisco Unified Communications Manager sends delayed offer INVITEs for the following scenarios:
  * Mid-call media renegotiation
  * Call hold-Cisco Unified Communications Manager sends a delayed offer INVITE in mid-call when inserting MOH, because the MOH server might not support the same codec as the negotiated audio call. Cisco Unified Communications Manager needs the complete codec list from the far end to renegotiate media.
  * Call resume

  **Note** When a line-side device initiates a call transfer and leaves the call, Cisco Unified Communications Manager connects one or two trunk legs and sends a delayed offer INVITE in mid-call. Using a delayed offer INVITE ensures that features, such as video and SRTP, do not get dropped when transfers result in two trunk call legs getting connected.

• Cisco Unified Communications Manager sends a delayed offer INVITE or outgoing call fails when one of the following situations occurs:
  * If an allocated MTP, transcoder, or TRP does not support getPort capability and an outbound SIP trunk leg is enabled for early offer, Cisco Unified Communications Manager does not allocate another media resource to provide early offer.
  * When the Use Trusted Relay Point setting is enabled on a SIP trunk (Device > Trunk) and the allocated media resource does not support TRP capability or fails to provide the media port, Cisco Unified Communications Manager does not allocate another media resource. This situation can occur if the MTP or RSVP Agent is not configured for TRP.
  * Depending on the setting of the Fail Call If MTP Allocation Fails service parameter or the Fail Call If TRP Allocation Fails service parameter, Cisco Unified Communications Manager sends a delayed offer or fails the call.
• Configure UPDATE and PRACK on the SIP trunk to provide ringback in blind transfer cases when the consult call leg on early offer SIP trunk provides inband ringback or announcements. If the trunk is not enabled for PRACK or if the far-end device does not support UPDATE, the transferee does not receive a ringback tone.

• As in previous releases, you cannot change the codec order in the offer SDP. Cisco Unified Communications Manager orders the codecs based on an internal list, typically from highest to lowest. To work around this issue, you can create a SIP Normalization script to reorder the codecs in the offer SDP.

Traces

The following examples show the traces that help you troubleshoot early offer calls.

SIP Trunk Trace

001685280 |2010/05/25 13:50:31.980 |100 |AppInfo
|||SIPCdpc(1,100,67,9)||1,100,67,9.1^*^*|//SIP/SIPCdpc(1,67,9)/ci=30801944/cid=14961/scid=0/StartTransition: requireInactiveSDPForMidcallMediaChange=0, isTrunkEnabledForVoiceEO=1

001685289 |2010/05/25 13:50:32.001 |100 |SdlSig |PolicyAndRSVPRegisterReq
|wait
|RSVPSessionMgr(1,100,91,1) |SIPCdpc(1,100,67,9)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00
|[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801944 Branch= 0 reg=Default cap=0 loc=0
MRGPKid=1db1ba42-9575-e3dc-ba78-fb11d56db546
PrecLev=5 VCall=F VCapa=F VCapCount=0 regiState=0 medReq=0 dataCapFl=2
IsEmccD=F
EmccDName=to-ccm84 rcId= ipMode=0 eoType=2 getPort=F sRTP=F cryptocap=0
tm=16
DTMF(wantRecep=1 provOOB=1 suppMeth=1 Cfg=1 PT=0 reqMed=0) hInCodec=F
distMed=F mediaEP=F
rsvpQoType=0 gosFallback=F status=0 sipOfferNeededInd=T hasSDP=F
gEOlocInfo={gEOlocPkid=, filterPkid=, gEOlocVal=, devType=8}

001685353 |2010/05/25 13:50:32.087 |100 |SdlSig |PolicyAndRSVPRegisterRes
|outCall_waitRSVPRes |SIPCdpc(1,100,67,9) |RSVPSession(1,100,93,5)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00
|[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=

Note

The values for eoType include the following: None (0), early offer for G.Clear (1), early offer for voice and video (2), and early offer for G.Clear voice and video (3).
30801944 Branch= 0 Status=1 rsvpPol=1 vCall=F e2eRSVPInserted=F eoStatus=1 hasSDPMsg=T
RSVPAgent: confID =0 ci =0 capCt =0 reg= mtpType =2 agentCt =0 agentAlloc =0 RemoAgent=F
DevCap=0 ipAddrMode=0

The valid values for eoStatus include the following: None(0), early offer for voice and video (1), early offer for G.Clear (2), Continue delayed offer (3), and failed call (4).

---

**Trace for StationD (SCCP Device) That Participates in an Early Offer Call**

001685325 |2010/05/25 13:50:32.064 |100 |SdlSig |DeviceMediaInfoReq |restart0
|StationD(1,100,50,13) |RSVPSession(1,100,93,5)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00
|[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801943 confID=30801943 callRefID=30801943 counter=1 mediaType=1 ipAddrMode=0 PPID=16777217
reqCode=1
001685327 |2010/05/25 13:50:32.064 |100 |SdlSig |StationPortReq |restart0
|StationD(1,100,50,13) |StationCdpc(1,100,51,1)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00
|[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] confID=30801943 PPID=16777217 CI=30801943 transportType=1 addrType=0 mediaType=1

Response from the SCCPv20 device:

001685328 |2010/05/25 13:50:32.081 |100 |AppInfo
|||StationInit(1,100,49,1)||1,100,49,1.100207^172.18.199.61^SEP001319ACCA00|StationInit:

(0000013) **PortRes** IpAddr=0x399eb00, **Port=31780**, RTCPPort=0,
confID=30801943, PPID=16777217
001685330 |2010/05/25 13:50:32.081 |100 |SdlSig |StationPortRes |outgoing_call_proceeding3
|StationCdpc(1,100,51,1) |StationD(1,100,50,13)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00
|[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801943 confID=30801943 ptpID=16777217
ipAddr=0x(ac,12,c7,3d,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) port=31780 =.type=0. RTCPPort=0 mediaType=1

001685331 |2010/05/25 13:50:32.082 |100 |SdlSig |DeviceMediaInfoRes |wait
|RSVPSessionMgr(1,100,91,1) |StationCdpc(1,100,51,1)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00
|[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=
30801943 confID=30801943 callRefID=30801943 mediaType=1 ipType=0
PPID=16777217 reqCode=1
port=31780 RTCPPort=0 ipAddrType=0 ipv4=172.18.199.61 status=0

---

Cisco Unified Communications Manager System Guide, Release 9.1(1)
Media Layer Trace for Early Offer Call When MTP Allocation Is Required

001686458 |2010/05/25 13:50:48.535 |100 |SdlSig |AuEarlyOfferConnectReq |waitForAll |MediaCoordinator(1,100,125,1) |RSVPSession(1,100,93,6) |1,100,49,1.100222^172.18.201.82^SEP0014F2E982F1 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] Party1: CI=30801945 capCount=7 region=Default xferMode=4 mrid=0 audioId=0 videoCap=F dataCap=2 activeCap=0 cryptoCapCount=0 flushIns=0 dtmCall=0 dtmPrimaryCI=0 IPFid=(0,0,0,0) dtMedia=F honorcodec=F EOType=0 MohType=0 Party2: CI=30801946 capCount=0 region=Default xferMode=16 mrid=0 audioId=0 videoCap=F dataCap=2 activeCap=0 cryptoCapCount=0 flushIns=0 dtmCall=0 dtmPrimaryCI=0 IPFid=(0,0,0,0) dtMedia=F honorcodec=F EOType=2 MohType=0 videoCall=F confID =0 ci =0 capCt =0 reg= mtpType =2 agentCt =0 agentAllo =0 RemoAgent=F DevCap=0 ipAddrMode=0 mtpInsReason=32 hasSDP=F

Note: Valid values for mtpInsReason include the following: None (0), TRP Side B (1), TRP Side A (2), Transcoder Side A (4), MTP Side A (8), DTMF mismatch (16), early offer (32).

001686676 |2010/05/25 13:50:48.646 |100 |SdlSig |AuEarlyOfferConnectReply |wait |RSVPSession(1,100,93,6) |MediaCoordinator(1,100,125,1) |1,100,49,1.100223^172.18.197.154^MTP_sinise |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] ciParty1=30801945 ciParty2=30801946 devicePidParty1=(1,100,50,3) devicePidParty2=(1,100,67,10) err=0 videoFlag=F hasSDP=T.

Note: Valid values for Err codes for media resource allocation failures include the following: No Error (0), TRP allocation Side B (1), TRP Side A (2), Transcoder Side A (3), MTP Side A (4), MTP for DTMF mismatch (5), MTP for early offer (6).

Troubleshooting Early Offer Issues

For assistance in troubleshooting early offer problems, see the following table.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The initial outgoing INVITE for an early offer SIP trunk call does not contain an SDP.</td>
<td>1. Verify that you checked the Enable Early Offer for voice and video calls check box on the SIP associated with the early offer trunk.</td>
</tr>
<tr>
<td></td>
<td>2. Verify that the SIP trunk is not in IPv6 only mode or dual-mode trunk with ANAT or media preference set to IPv6.</td>
</tr>
<tr>
<td></td>
<td>3. Verify that calling device is not an IPv6-only device.</td>
</tr>
<tr>
<td></td>
<td>4. If initiating calls from pre SCCP v20 device or H323 Slowstart device or if this is a delayed offer incoming call, verify that MTP allocation is taking place.</td>
</tr>
<tr>
<td></td>
<td>5. Ensure that the caller or SIP trunk media resource group list has an MTP available. Verify that the MTP firmware supports getPort capability. If the MTP image does not support getPort capability, upgrade to a newer image, IOS release 15.1(2)T or later.</td>
</tr>
<tr>
<td></td>
<td>6. For an SCCP v20 calling device, verify that the device provides the media port in StationPortRes/DeviceMediaInfoRes. If not, check for a timeout event-GetPortResponseTimer or TimeoutWaitingForPortInfo.</td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| An outgoing call for an early offer SIP trunk fails. Cisco Unified Communications Manager does not send an INVITE. | 1. If initiating calls from pre-SCCP v20 devices or H323 slowstart or delayed offer incoming trunk, verify that MTP allocation takes place and that the MTP supports SCCP v20.  
2. If the MTP allocation fails, do one or more of the following:  
   • Check the configuration for the Fail Call Over SIP Trunk If MTP Allocation Fails service parameter and set it to False.  
   • Include an MTP in the media resource group list that associates with the SIP trunk or default pool.  
3. If the MTP image does not support getPort capability, upgrade to a newer image, IOS release 15.1(2)T or later.  
4. If initiating calls from SCCP v20 devices, check whether Cisco Unified Communications Manager times out (typically after 2 seconds) while waiting for StationPortRes from the SCCP line device. If so, the SCCP device needs to be reset or phone logs need to be collected. Also, check the configuration of the Fail Call Over SIP Trunk If MTP Allocation Fails service parameter. If you want Cisco Unified Communications Manager to send a delayed offer invite, set the parameter to False. |
| The outgoing call for early offer SIP trunk always has SDP with one codec and the IP address and port of the MTP. | 1. Verify that the Media Termination Required check box is not checked in the Trunk Configuration window for this trunk.  
2. If the Media Termination Required check box is not checked on the Trunk Configuration window for this trunk, check whether a media resource is being allocated. Media resources can get allocated for local RSVP, TRP enabled on trunk, early offer, DTMF mismatch, or codec mismatch.  
3. Verify that the media resource is configured for pass-through codec. |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no video during initial call when</td>
<td>1  Verify that the Media Termination Required check box is</td>
</tr>
<tr>
<td>MTP is inserted in the call.</td>
<td>not checked in the Trunk Configuration window for this trunk.</td>
</tr>
<tr>
<td></td>
<td>2  Verify that Cisco Unified Communications Manager MTP is not allocated.</td>
</tr>
<tr>
<td></td>
<td>The Cisco Unified Communications Manager MTP does not support video</td>
</tr>
<tr>
<td></td>
<td>pass-through.</td>
</tr>
<tr>
<td></td>
<td>3  If an IOS MTP is allocated, verify that the IOS MTP is</td>
</tr>
<tr>
<td></td>
<td>configured with pass-through codec. IOS MTP supports video pass-through.</td>
</tr>
<tr>
<td></td>
<td>4  Verify that location call admission control allows a video call.</td>
</tr>
<tr>
<td>Call is not secured when MTP is inserted</td>
<td>1  Verify that the Media Termination Required check box is</td>
</tr>
<tr>
<td>in the call.</td>
<td>not checked in the Trunk Configuration window for this trunk.</td>
</tr>
<tr>
<td></td>
<td>2  Verify that the IOS MTP is configured with pass-through codec.</td>
</tr>
<tr>
<td></td>
<td>3  Verify that call does not initiate from H323 slowstart device or</td>
</tr>
<tr>
<td></td>
<td>delayed offer trunk.</td>
</tr>
</tbody>
</table>

**Cisco Unified Communications Manager SIP Endpoints Overview**

The Cisco Unified IP Phones 7911, 7941, 7961, 7970, and 7971 get deployed as a SIP endpoint in a Cisco Unified Communications Manager Back to Back User Agent (B2BUA) environment. The SIP provides the primary interface between the phone and other network components. In addition to SIP, other protocols get 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.
Cisco Business Edition 5000 does not support the following example.

**Figure 8: Cisco Unified Communications Manager B2BUA Network**

The figure above shows a simplified example of a Cisco Unified Communications Manager B2BUA network that shows a main site and a branch office deployment. Each site includes a mixture of phones that are running SIP and phones that are running SCCP. The main site contains the Cisco Unified Communications Manager cluster and voice mail server. Each phone at the main site and the branch office site homes to a set of primary, secondary, and tertiary Cisco Unified Communications Managers. This provides redundancy of call control in the event of the failure of an individual Cisco Unified Communications Manager server.

Phones that are running SIP that are at the main site direct all session invitations to Cisco Unified Communications Manager. Based on routing configuration and destination, Cisco Unified Communications Manager will either extend a call locally to another phone that is running SIP or phone that is running SCCP, 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 that are originating from phones in the branch office get routed similarly with the added ability of routing calls to the PSTN through the branch office voice gateway.

The branch office includes an SRST gateway that is deployed for access to the main site IP WAN and for PSTN access. Phones that are running SIP in the branch office will direct all session invitations to the Cisco Unified Communications Manager at the main site. Similarly to the phones at the main site, Cisco Unified Communications Manager 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 PSTN. Depending on the routing configuration of the Cisco Unified Communications Manager cluster, PSTN calls that originate from the phones in the branch office can get 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 phones that are running SIP and phones that are running SCCP will fail over to the SRST gateway during a
WAN failure. By doing so, the phones in the branch office can have their calls routed by the SRST gateway. This includes calls that originate and terminate within the branch office and calls that originate and terminate in the PSTN.

**SIP Line Side Overview**

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

**SIP Standards**

The SIP standards described in this section are supported in Cisco Unified Communications Manager.

**RFC3261 RFC3262 (PRACK) RFC3264 (Offer/Answer) RFC3311 (UPDATE) 3PCC**

This SIP standard supports the following Cisco Unified Communications Manager features:

- Basic Call
- Hold and Resume
- Music on Hold
- Distinctive Ringing
- Speed dialing
- Abbreviated Dialing
- Call Forwarding (for example, 486 and 302 support)
- Meet-Me
- Pickup, Group Pickup, Other Group Pickup
- 3-way calling (local mixing of phone that is running SIP)
- Parked Call Retrieval
- Shared line: Basic Call

**RFC3515 (REFER) Also Replaces and Referred-By Headers**

These SIP standards support the following Cisco Unified Communications Manager features:

- Consultative Transfer
- Early Attended Transfer
• Blind Transfer

Remote Party Id (RPID) Header

This SIP standard supports the following Cisco Unified Communications Manager 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 represents a SIP header that is used for identification services. RPID indicates the calling, called, and connected remote party information to the other party for identification and callback, 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 Communications Manager 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 Communications Manager feature:

• Shared Line: Remote Resume

Join Header

This SIP standard supports the following Cisco Unified Communications Manager feature:

• Shared Line: Barge

P-Charging-Vector Header

Cisco Unified Communications Manager 8.6(1) supports pass through of a SIP header called P-Charging-Vector (PCV) in network deployment. This PCV header is used to convey mobile or PSTN charging related information, such as the globally unique IP Multimedia Subsystem (IMS) charging identifier (ICID) value to the service providers.
A new SIP Normalization script, HCS-PCV-PAI-passthrough, is introduced as part of this feature. This script would be pre-installed on the Cisco Unified Communications Manager and has to be associated with all the SIP trunks that point to the network.

For any calls that originate from a network, the Cisco Unified Communications Manager passes through the PCV header received from a network in the INVITE, UPDATE and 200 OK to the other side. Cisco Unified Communications Manager would additionally pass through the PCV header from a network via 200 OK SIP for the calls terminating in the Cisco Unified Communications Manager. Because these calls are routed back to the Cisco network via the same SIP trunk, the 200 OK message received by the Cisco Unified Communications Manager is passed as-is through the PCV header in the outgoing calls.

**RFC3265 + Dialog Package**

This SIP standard supports the following Cisco Unified Communications Manager feature:

- Shared Line: Remote State Notifications

**RFC3265 + Presence Package**

These SIP standards support the following Cisco Unified Communications Manager features:

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

**RFC3265 + KPML Package**

These SIP standards support the following Cisco Unified Communications Manager features:

- Digit Collection
- OOB DTMF

**RFC3265 + RFC3842 MWI Package (Unsolicited Notify)**

These SIP standards support the following Cisco Unified Communications Manager feature:

- Message Waiting Indication

**Remotecc**

This SIP standard supports the following Cisco Unified Communications Manager features:

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

RFC4028 Session Timers

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

Cisco Unified Communications Manager Functionality on SIP Phones

Cisco Unified Communications Manager supports the functions on Cisco Unified IP Phones described in this section.

BLF Call Pickup

Cisco Unified Communications Manager allows you to assign a line key as a BLF Call Pickup key. The BLF Call Pickup key behaves the same way as a BLF speed dial key on phones that are running SIP. The line key indicates the BLF status of the configured DN, and pressing the line key speed dials the configured DN. BLF Call Pickup adds an alerting indication when a call is alerting on the DN configured as the BLF Call Pickup DN. You can answer the alerting call by pressing the BLF Call Pickup DN while the call is showing an alerting state.

The subscription type PRESENCE+ALERTING is used by the SIP device layer to subscribe for the presence and alerting status of calls on a DN monitored by the BLF Call Pickup feature. The subscription for PRESENCE+ALERTING is handled by the line control of the monitored DN line. Line Control is responsible for notifying the Subscription Manager when a call is received for a DN that has been subscribed for.

Calling Party Normalization

Cisco Unified Communications Manager allows you to globalize calling party numbers of calls received through gateways. The calling party number can be transformed into E.164 format before being presented on the phone. This globalized number gets provided to the phone, so a user can dial back a received number without having to use the edit dial function.

An optional URI parameter (x-cisco-callback-number) for globalized numbers is added to the RPID header. The localized number is specified as the user part of the SIP URI. The same SIP URI is also specified in the From header sent by the Cisco Unified Communications Manager to the phone. When invoking the dial back feature, the phone will echo back the same SIP URI as the request URI in the INVITE to Cisco Unified Communications Manager. The Cisco Unified Communications Manager SIP Device layer will parse the request URI for the URI parameter containing the globalized number to use for routing. If it is not found, the SIP device layer will resort to using the localized form of the number found in the user portion of the SIP URI.
Be aware that the x-cisco-callback-number parameter is optional and will not get included in the RPID header of a conference call, and it will not get included when a call is marked as private.

CTI Support

Line-side SIP includes CTI functionality, which allows CTI applications such as Cisco Unified Communications Manager Assistant to support Cisco Unified IP Phones that are running SIP (for example, Cisco Unified IP Phone 7961). CTI capabilities on phones that are running SIP equate to those on phones that are running SCCP with a few exceptions. Some CTI features that are supported on phones that are running SIP include display text, set lamp, play tone, call park, and privacy support. For more information about CTI and Cisco Unified Communications Manager, see Computer Telephony Integration.

Dial Plans

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

Directed Call Pickup

Cisco Unified Communications Manager supports the Directed Call Pickup feature on phones that are running SIP. The Directed Call Pickup capabilities on phones that are running SIP equate to those on phones that are running SCCP. Directed Call Pickup allows you to pick up an alerting call on a DN directly by pressing the GPickUp softkey and entering the directory number. The phone that is running SIP will then send Cisco Unified Communications Manager an INVITE that includes the DN of the phone that you want to pick up.

Do Not Disturb

Cisco Unified Communications Manager supports do not disturb (DND) that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. A DND status change gets signaled from a SIP device to Cisco Unified Communications Manager that is using the SIP PUBLISH method. A DND status change gets signaled from a Cisco Unified Communications Manager to a SIP device that is using a dndupdate Remote-cc REFER request. Cisco Unified Communications Manager can also publish the do not disturb status for a device, along with the busy and idle status for the device.

Do Not Disturb (DND) Call Reject

The DND feature allows you to set one of two options in Cisco Unified CM User Options. You can set the DND feature to Ringer Off or Call Reject. Call Reject gets supported on both phones that are running SCCP and phones that are running SIP. When DND is active and Call Reject is selected, no incoming calls or audio and visual notifications get presented on the phone.
DSCP Configuration

Cisco Unified IP Phones that are running SIP get their DSCP information from the configuration file that gets downloaded to the device. The DSCP setting applies for the device, whereas, the phones that are running SCCP can get the DSCP setting for a call. DSCP values get configured in the Enterprise Parameters Configuration window, and in the Cisco Unified Communications Manager Service Parameters Configuration window.

E.164

Cisco Unified Communications Manager allows you to globalize calling party numbers of calls received through gateways. This includes the addition of the “+” sign found in E.164 formatted numbers, such as +14085551234. When a phone that is running SIP invokes the dial back feature from the call logs directory, the globalized number will get returned to the Cisco Unified Communications Manager for routing. E.164 support allows the SIP device layer to pass the entire globalized number string, including the + sign, to the DA.

Join and Join Across Lines

The Join feature operates similar to one or more instances of the ad-hoc conference feature for phones that are running SIP, except for without the consultative call. The Join Across Lines feature allows a user to join calls on multiple phone lines (either on different directory numbers or on the same directory number but on different partitions) to create a conference.

When a user initiates the Join or Join Across Lines feature, the phone that is running SIP will use the Join softkey message in the same way existing softkeys are sent to Cisco Unified Communications Manager from phones that are running SIP to invoke the join feature on selected lines.

Malicious Call Identification (MCID)

Cisco Unified Communications Manager supports the MCID feature on phones that are running SIP. The MCID capabilities on phones that are running SIP equate to those on phones that are running SCCP. The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call and presses the MCID softkey, a new Remote-cc REFER softkeyevent request is sent to Cisco Unified Communications Manager. This triggers Cisco Unified Communications Manager to record the call. The user is then sent a confirmation tone and a text message to acknowledge receiving the MCID notification. The confirmation tone is handled by a Remote-cc playtonereq to the phone, and the text message is a Remote-cc statuslineupdate indicating “Mcid Successful”.

Network Time Protocol (NTP)

You can configure phone Network Time Protocol (NTP) references in Cisco Unified Communications Manager Administration to ensure that a Cisco Unified IP Phone that is running SIP gets its date and time from the NTP server. If all NTP servers do not respond, the phone that is running SIP 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 Communications Manager 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 in the phone window.

For information on configuring the NTP reference, see SIP Dial Rules.

**PLAR**

Private Line Automatic Ringdown (PLAR), a term that is used by traditional telephony systems, refers to a phone configuration whereby any time the user goes off hook, the phone immediately dials a preconfigured number. The user cannot dial any other numbers from that phone (or line). This gets implemented in SCCP IP phones in Cisco Unified Communications Manager by using partitions, calling search space (CSS), and translation patterns; neither the device configuration nor line configuration indicates that PLAR is set up for the phone.

Administrators use SIP Dial Rules for configuring PLAR in phones that are running SIP. Phones that are configured for PLAR will have a one-line dial plan configuration that specifies 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 Communications Manager. The user does not enter any digits. See SIP Dial Rules for more information.

**Programmable Line Keys**

Cisco Unified IP Phones support line buttons (the buttons to the right of the display), which are used to initiate, answer, or switch to a call on a particular line. A limited number of features, such as speed dial, extension mobility, privacy, BLF speed dial, DND, and Service URLs, get assigned to these buttons. Each of these features are supported on phones that are running SIP and can be configured in Cisco Unified Communications Manager.

For information on the PLK feature, see Programmable Line Keys.

**Single Button Barge/cBarge**

Cisco Unified Communications Manager supports Single Button Barge/cBarge that a SIP device initiates. The Single Button Barge/cBarge capabilities on phones that are running SIP equate to those on phones that are running SCCP. The Single Button Barge/cBarge feature allows a user to simply press the shared-line button of a call that is in progress, to automatically add that user to the call.

**Single Call UI**

Cisco Unified Communications Manager supports a single call UI with the use of line rollovers on phones that are running SIP. A line rollover occurs if the max-calls-per-line and busy-trigger values are set to 1/1. For Transfer and Conference features, when the max-calls-per-line value is reached on the primary call, the phone can roll over the consult call to the closest line button with zero calls, or on the same DN in a different partition. If the max-calls-per-line and busy-trigger values are set to 2/1, the outbound consult call will be carried on the same button.
SIP Profiles for Endpoints

Because SIP attributes rarely change, Cisco Unified Communications Manager uses SIP profiles to define SIP attributes that are associated with SIP trunks and Cisco Unified IP Phones. Having these attributes in a profile instead of adding them individually to every SIP trunk and phone that is running SIP 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 SIP trunks and phones are configured, Cisco Unified Communications Manager provides a default SIP profile; however, administrators can create customized SIP profiles. SIP profiles get assigned to SIP devices by using Cisco Unified Communications Manager Administration.

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

For information on configuring SIP profiles, see SIP Dial Rules.

Soft Client Dual Registration

Cisco Unified Communications Manager does not allow two different endpoints to register to the same device name. For soft clients, this can present a problem because a soft client can be installed on multiple systems, such as a Cisco Jabber client for PC and a Cisco Jabber client for Macintosh, and can use the same registration from each system.

To handle registration attempts where a different soft client is already registered to that device name, soft clients can insert the following tags into the Supported header of SIP registration requests:

- **x-cisco-duplicate-reg**—When this tag is present, Cisco Unified Communications Manager automatically registers the second soft client and drops the first soft client registration.
- **x-cisco-graceful-reg**—The tag gives a soft client that is attempting to register to a registered device name the ability to gracefully override the existing registration session without having to automatically cancel the existing session. When this tag is present, Cisco Unified Communications Manager rejects the new registration attempt and returns a SIP 403 message. The soft client can either send a new registration attempt using just the x-cisco-duplicate-reg tag, which would de-register the first soft client, or abort the registration attempt, which would keep the first soft client registration intact.

If both tags are present, Cisco Unified Communications Manager gives precedence to the x-graceful-reg tag.

Softkey Handling

The administrator uses Cisco Unified Communications Manager Administration to modify the softkey sets that the phone displays. You can add and remove keys, and their positions can get changed. This data gets written to the database and gets sent to the phone that is running SCCP via Station messages as part of the phone registration/initialization process. For Cisco Unified IP Phones that support SIP, however, instead of sending the keys in Station Messages, the Cisco Unified Communications Manager TFTP server builds the file that contains the softkey sets. The phone that is running SIP retrieves these files from the TFTP server, and the new softkey sets overwrite the softkey sets that are built into the phone. This allows Cisco Unified Communications Manager to modify the default softkeys and also lets Cisco Unified Communications Manager manipulate the softkey events, so 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 phone that is running SIP, the softkey will display, but the phone will display a message that the key is not active, which is consistent with the behavior of the phone that is running SCCP.

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

**Note**

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

---

**Unified Mobile Communications Server (UMCS) Integration**

Cisco Unified Communications Manager supports integration with UMCS to extend the capabilities of Cisco Unified Communications Manager to Cisco Unified Mobile Communicator devices. The UMCS communicates with Cisco Unified Communications Manager using SIP over one or more TCP connections. Each TCP connection can be shared between multiple users.