CHAPTER 41

Understanding Cisco Unified Communications Manager Trunk Types

In a distributed call-processing environment, Cisco Unified Communications Manager communicates with other Cisco Unified Communications Manager clusters, the public switched telephone network (PSTN), and other non-IP telecommunications devices, such as private branch exchanges (PBXs) by using trunk signaling protocols and voice gateways.

This section covers the following topics:

Trunk Configuration Checklist

Table 41-1 provides an overview of the steps that are required to configure trunk interfaces in Cisco Unified Communications Manager, along with references to related procedures and topics.

See the following sections:

Configuration Considerations for SIP trunks

In a call-processing environment that uses Session Initiation Protocol (SIP), use SIP trunks to configure a signaling interface with Cisco Unified Communications Manager for SIP calls. SIP trunks (or signaling interfaces) connect Cisco Unified Communications Manager clusters with a SIP proxy server. The SIP signaling interface uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more endpoints. For more information about SIP and configuring SIP trunks, see the "SIP and Cisco Unified Communications Manager" section on page 40-2.

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

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

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

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

  The following example shows a valid configuration:

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

  The following example shows an invalid configuration:

```
Trunk#1: Incoming Transport Protocol=TCP/UDP, Incoming Port=5060, Destination
Address=10.10.10.1
Trunk#2: Incoming Transport Protocol=TCP/UDP, Incoming Port=5060, Destination
Address=10.10.10.1
Trunk#3: Incoming Transport Protocol=TLS, Incoming Port=5061, X.509 Subject
Name=my_ccm1, my_ccm2
Trunk#4: Incoming Transport Protocol=TLS, Incoming Port=5081, X.509 Subject
Name=my_ccm2
Trunk#5: Incoming Transport Protocol=TLS, Incoming Port=5061, X.509 Subject
Name=my_ccm2
Trunk#6: Incoming Transport Protocol=TLS, Incoming Port=5081, X.509 Subject
Name=my_ccm2
Trunk#7: Incoming Transport Protocol=TCP/UDP, Incoming Port=5060, Destination
Address=myhost.domain.com
```

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

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

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

Trunk #7 conflicts with Trunk #1, because if myhost.domain.com resolves to 10.10.10.1, the protocol, incoming port, and destination address are identical.

Table 41-1 Trunk Configuration Checklist

Configuration Steps		Procedures and Related Topics
For H.225/H.323 and Intercluster Trunks		
Step 1	Gather the endpoint information, such as IP addresses or host names, that you need to configure the trunk interface.	*Cisco Unified Communications Solution Reference Network Design (SRND)*
Step 2	For gatekeeper-controlled trunks, configure the gatekeeper.	Gatekeeper and Gatekeeper-Controlled Trunk Configuration Checklist, page 8-3 Cisco Unified Communications Manager SIP Endpoints Overview, page 40-38
Step 3	Add the appropriate trunks in Cisco Unified Communications Manager Administration. • H.225 trunks (gatekeeper controlled) • Intercluster trunks (gatekeeper controlled) • Intercluster trunks (non-gatekeeper controlled)	Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 4	Configure the gatekeeper-controlled intercluster trunks or H.225 trunks to specify gatekeeper information. Configure the non-gatekeeper-controlled trunks with the IP address or host name for the remote Cisco Unified Communications Manager server.	Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 5	Configure a route pattern or route group to route calls to each gatekeeper-controlled trunk. Configure a route pattern or route group to route calls to each non-gatekeeper-controlled trunk.	Route Pattern Configuration,*Cisco Unified Communications Manager Administration Guide* Route Group Configuration, *Cisco Unified Communications Manager Administration Guide* Cisco Unified Communications Manager SIP Endpoints Overview, page 40-38
Step 6	Reset the trunk interface to apply the configuration settings.	Resetting a Trunk, *Cisco Unified Communications Manager Administration Guide*

Table 41-1 Trunk Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
For SIP Trunks		
Step 1	Gather the endpoint information, such as IP addresses or host names, that you need to configure the trunk interface.	*Cisco Unified Communications Solution Reference Network Design (SRND)* Cisco Unified Communications Manager SIP Endpoints Overview, page 40-38
Step 2	Configure the SIP proxy.	Understanding Session Initiation Protocol, page 40-1
Step 3	Create a SIP profile. Create a SIP trunk security profile. Create a SIP trunk. For trunk security, check the SRTP Allowed check box and then choose the Consider Traffic on This Trunk Secure settings (optional). Configure the destination address(es). Configure the destination port.	SIP Profile Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide* *Cisco Unified Communications Manager Security Guide*
Step 4	Associate the SIP trunk to a Route Pattern or Route Group.	SIP Route Pattern Configuration, *Cisco Unified Communications Manager Administration Guide* Route Group Configuration, *Cisco Unified Communications Manager Administration Guide* Route List Configuration, *Cisco Unified Communications Manager Administration Guide*
Step 5	Reset the SIP trunk.	Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide*

Table 41-1 Trunk Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 6	Configure SIP timers, counters, and service parameters, if necessary. If you are using PUBLISH to communicate to a Cisco Unified Presence, choose the configured trunk in the CUP PUBLISH Trunk field of the Service Parameters Configuration window. **Tip** Verify that the The SIP Interoperability Enabled service parameter, which supports the Cisco CallManager service, is set 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.	Service Parameter Configuration, *Cisco Unified Communications Manager Administration Guide.* SIP Timers and Counters, page 40-5
Step 7	To facilitate interoperability among a variety of endpoints, including PBXs, gateways, and service providers, you may need to enable SIP normalization and transparency. Normalization allows you to preserve, remove, or change the contents of any SIP headers or content bodies, known or unknown. To enable normalization, you create scripts as described in the *Developer Guide for SIP Transparency and Normalization* and import them in Cisco Unified Communications Manager Administration. SIP transparency allows you to pass information from one call leg to the other. You enable SIP transparency using scripting, as described in the *Developer Guide for SIP Transparency and Normalization.*	SIP Transparency and Normalization, page 40-10 *Developer Guide for SIP Transparency and Normalization* SIP Normalization Script Configuration, *Cisco Unified Communications Manager Administration Guide* SIP Normalization Script Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 8	To configure an early offer enabled SIP trunk, edit the SIP profile, and check the **Early Offer support for voice and video calls (insert MTP if needed)** check box. **Note** Make sure that the MTP uses IOS version 15.1(2)T or later.	SIP Profile Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*

Table 41-1 Trunk Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 9	If you use SCCP phones with SCCP version 20 support (which provides media port information through the getPort capability) and you enabled early offer on a SIP trunk, set the following CallManager service parameters (**System > Service Parameters**): • Port Received Timer for Outbound Call Setup • Port Received Timer After Call Connection • Fail Call Over SIP Trunk if MTP Allocation Fails • Fail Call If Trusted Relay Point Allocation Fails	Service Parameter Configuration, *Cisco Unified Communications Manager Administration Guide*
Step 10	To prevent Cisco Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services, edit the appropriate SIP profile, and check the **Send send-receive SDP in mid-call INVITE** check box. **Note** This check box applies only to early offer enabled SIP trunks and has no impact on SIP line calls. When you enable **Send send-receive SDP in mid-call INVITE** for an early offer SIP trunk in tandem mode, Cisco Unified Communications Manager inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line. In tandem mode, Cisco Unified Communications Manager depends on the SIP devices to initiate reestablishment of media path by sending either a delayed offer INVITE or mid-call INVITE with send-recv SDP. When you enable both **Send send-receive SDP in mid-call INVITE** and **Require SDP Inactive Exchange for Mid-Call Media Change** on the same SIP profile, the **Send send-receive SDP in mid-call INVITE** setting overrides the **Require SDP Inactive Exchange for Mid-Call Media Change** setting, so Cisco Unified Communications Manager does not send an INVITE with a=inactive SDP in mid-call codec updates. For SIP line side calls, the **Require SDP Inactive Exchange for Mid-Call Media Change** check box applies when enabled. **Note** To prevent the SDP mode from being set to inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter (**System > Service Parameters**) to *True*.	SIP Profile Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 11	To track the status of remote destinations, configure SIP OPTIONS. Use SIP Profile Configuration to enable SIP OPTIONS. Check the **Enable OPTIONS Ping to monitor destination status for trunks with service type "None (Default)"** check box.	SIP Profile Configuration, *Cisco Unified Communications Manager Administration Guide* SIP OPTIONS, page 40-28

Cisco Unified Communications Manager Trunk Configuration

Trunk configuration in Cisco Unified Communications Manager Administration depends on the network design and call-control protocols that are used in the IP WAN. All protocols require that either a signaling interface (trunk) or a gateway be created to accept and originate calls. For some IP protocols, such as MGCP, you configure trunk signaling on the gateway. You specify the type of signaling interface when you configure the gateway in Cisco Unified Communications Manager. For example, to configure QSIG connections to Cisco Unified Communications Manager, you must add an MGCP voice gateway that supports QSIG protocol to the network. You then configure the T1 PRI or E1 PRI trunk interface to use the QSIG protocol type. For more information about configuring gateways, see the "Understanding Cisco Unified Communications Manager Voice Gateways" section on page 38-1.

Related Topics

- Trunks and Gatekeepers in Cisco Unified Communications Manager, page 41-7
- Trunk Types in Cisco Unified Communications Manager Administration, page 41-8

Trunks and Gatekeepers in Cisco Unified Communications Manager

In addition to using gateways to route calls, you can configure trunks in Cisco Unified Communications Manager Administration to function in either of the following ways:

- Gatekeeper-Controlled Trunks, page 41-7
- Non-Gatekeeper-Controlled Trunks, page 41-8

Gatekeeper-Controlled Trunks

Gatekeepers that are used in a distributed call-processing environment provide call routing and call admission control for Cisco Unified Communications Manager clusters. Intercluster trunks that are gatekeeper-controlled can communicate with all remote clusters. Similarly, an H.225 trunk can communicate with any H.323 gatekeeper-controlled endpoints including Cisco Unified Communications Manager clusters. Route patterns or route groups can route the calls to and from the gatekeeper. In a distributed call-processing environment, the gatekeeper uses the E.164 address (phone number) and determines the appropriate IP address for the destination of each call, and the local Cisco Unified Communications Manager uses that IP address to complete the call.

For large distributed networks where many Cisco Unified Communications Manager clusters exist, you can avoid configuring individual intercluster trunks between each cluster by using gatekeepers.

When you configure gatekeeper-controlled trunks, Cisco Unified Communications Manager creates a virtual trunk device. The gatekeeper changes the IP address of this device dynamically to reflect the IP address of the remote device. Specify these trunks in the route patterns or route groups that route calls to and from the gatekeeper.

See *Cisco Unified Communications Solution Reference Network Design (SRND)* for more detailed information about gatekeeper configuration, dial plan considerations when using a gatekeeper, and gatekeeper interaction with Cisco Unified Communications Manager.

Non-Gatekeeper-Controlled Trunks

With no gatekeepers in the distributed call-processing environment, you must configure a separate intercluster trunk for each remote device pool in a remote cluster that the local Cisco Unified Communications Manager can call over the IP WAN. You also configure the necessary route patterns and route groups to route calls to and from the various intercluster trunks. The intercluster trunks statically specify the IP addresses of the remote devices.

Related Topics

- Trunk Types in Cisco Unified Communications Manager Administration, page 41-8
- Trunk Configuration Checklist, page 41-1

Trunk Types in Cisco Unified Communications Manager Administration

Your choices for configuring trunks in Cisco Unified Communications Manager depend on whether the IP WAN uses gatekeepers to handle call routing. Also, the types of call-control protocols that are used in the call-processing environment determine trunk configuration options.

You can configure these types of trunk devices in Cisco Unified Communications Manager Administration:

- H.225 Trunk (Gatekeeper Controlled), page 41-8
- Intercluster Trunk (Gatekeeper Controlled), page 41-8
- Intercluster Trunk (Non-Gatekeeper Controlled), page 41-9
- SIP Trunk, page 41-9

H.225 Trunk (Gatekeeper Controlled)

In an H.323 network that uses gatekeepers, use an H.225 trunk with gatekeeper control to configure a connection to a gatekeeper for access to other Cisco Unified Communications Manager clusters and to H.323 devices. An H.225 trunk can communicate with any H.323 gatekeeper-controlled endpoint. When you configure an H.323 gateway with gatekeeper control in Cisco Unified Communications Manager Administration, use an H.225 trunk. To choose this method, use **Device > Trunk** and choose **H.225 Trunk (Gatekeeper Controlled)**.

You also configure route patterns and route groups to route calls to and from the gatekeeper. For more information, see the "Gatekeepers and Trunks" section on page 8-10.

Intercluster Trunk (Gatekeeper Controlled)

In a distributed call-processing network with gatekeepers, use an intercluster trunk with gatekeeper control to configure connections between clusters of Cisco Unified Communications Manager systems. Gatekeepers provide call admission control and address resolution for intercluster calls. A single intercluster trunk can communicate with all remote clusters. To choose this method, use **Device > Trunk** and choose **Inter-Cluster Trunk (Gatekeeper Controlled)** in Cisco Unified Communications Manager Administration.

You also configure route patterns and route groups to route the calls to and from the gatekeeper. In this configuration, the gatekeeper dynamically determines the appropriate IP address for the destination of each call, and the local Cisco Unified Communications Manager uses that IP address to complete the call

For more information about gatekeepers, see the "Gatekeepers and Trunks" section on page 8-10.

Intercluster trunks support location-based call admission control (CAC) through use of the specially designated Phantom location. See "Location-Based Call Admission Control Over Intercluster Trunk" section on page 8-9 for additional information.

Intercluster Trunk (Non-Gatekeeper Controlled)

In a distributed network that has no gatekeeper control, you must configure a separate intercluster trunk for each device pool in a remote cluster that the local Cisco Unified Communications Manager can call over the IP WAN. The intercluster trunks statically specify the IP addresses or host names of the remote devices.To choose this method, use **Device > Trunk** and choose **Inter-Cluster Trunk (Non-Gatekeeper Controlled)** in Cisco Unified Communications Manager Administration.

Note You must specify the IP addresses of all remote Cisco Unified Communications Manager nodes that belong to the device pool of the remote non-gatekeeper-controlled intercluster trunk.

You also configure the necessary route patterns and route groups to route calls to and from the intercluster trunks.

Intercluster trunks support location-based call admission control (CAC) through use of the specially designated Phantom location. See "Location-Based Call Admission Control Over Intercluster Trunk" section on page 8-9 for additional information.

SIP Trunk

In a call-processing environment that uses Session Initiation Protocol (SIP), use SIP trunks to configure a signaling interface with Cisco Unified Communications Manager for SIP calls. SIP trunks (or signaling interfaces) connect Cisco Unified Communications Manager clusters with a SIP proxy server. The SIP signaling interface uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more endpoints. For more information about SIP and configuring SIP trunks, see the "SIP and Cisco Unified Communications Manager" section on page 40-2.

To configure a SIP trunk in Cisco Unified Communications Manager Administration, choose **Device > Trunk** and then **SIP Trunk**. For information on configuration tasks, see the "Cisco Unified Communications Manager SIP Endpoints Overview" section on page 40-38.

Tip You must also configure route groups and route patterns that use the SIP trunks to route the SIP calls.

To receive QSIG basic calls and features, such as MWI, Call Transfer, Call Diversion, Call Completion, Path Replacement, and Identification Services, across an intercluster SIP trunk or a SIP gateway, configure a SIP trunk with QSIG as the tunneled protocol. For information about configuring SIP trunks, see "Trunk Configuration Settings" 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.

To turn off RPID headers on the SIP gateway, apply a SIP profile to the voIP dial peer on the gateway, as shown in the following example:

```
voice class sip-profiles 1000
request ANY sip-header Remote-Party_ID remove
response ANY sip-header Remote-Party-ID remove

dial-peer voice 124 voip
destination-pattern 3...
signaling forward unconditional
session protocol sipv2
session target ipv4:<ip address>
voice-class sip profiles 1000
```

SIP trunks support location-based call admission control (CAC) through use of the specially designated Phantom location. See "Location-Based Call Admission Control Over Intercluster Trunk" section on page 8-9 for additional information.

Note 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. For more information about Cisco IME, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Related Topics

- Blocking Transfer Capabilities by Using Service Parameters, page 41-13
- Dependency Records for Trunks and Associated Route Groups, page 41-13

Trunks and the Calling Party Normalization Feature

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without needing to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

SIP trunks and MGCP gateways can support sending the international escape character, +, for calls. H.323 gateways/trunks do not support the + because the H.323 protocol does not support the international escape character, +. QSIG trunks do not attempt to send the +. For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway/trunk. For outgoing calls through a gateway/trunk that does not support +, the international escape character + gets stripped when Cisco Unified Communications Manager sends the call information to the gateway/trunk.

SIP does not support the number type, so calls through SIP trunks only support the Incoming Calling Party Unknown Number (prefix and digits-to-strip) settings.

For information on how to configure this feature for your trunk, see the "Calling Party Normalization" section in the *Cisco Unified Communications Manager Features and Services Guide*.

You can configure the international escape character, +, to globalize the calling party number. For information on the international escape character, +, see "Using the International Escape Character +" section on page 16-22.

Applying the International Escape Character, +, to Inbound Calls Over H.323 Trunks

The H.323 protocol does not support the international escape character, +. To ensure that correct prefixes, including the international escape character, +, get applied for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configuring the incoming called party settings ensures that when a inbound call comes from a H.323 gateway or trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway.

For example, to ensure that the correct DN patterns get used with SAF/call control discovery for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, or H.323 (non-gatekeeper controlled) trunk window. See the following example for more information.

- A caller places a call to +19721230000 to Cisco Unified Communications Manager A.
- Cisco Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type.
- For this inbound call from the trunk, Cisco Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.

You can configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 (gatekeeper-controlled) windows.

The service parameters support the Cisco CallManager service. To configure the service parameters, click **Advanced** in the Service Parameter Configuration window for the Cisco CallManager service; then, locate the H.323 pane for the following parameters:

- Incoming Called Party National Number Prefix - H.323
- Incoming Called Party International Number Prefix - H.323
- Incoming Called Party Subscriber Number Prefix - H.323
- Incoming Called Party Unknown Number Prefix - H.323

These service parameters allow you to prefix digits to the called number based on the Type of Number field for the inbound offered call. You can also strip a specific number of leading digits before the prefix gets applied. To prefix and strip digits by configuring these parameter fields, use the following formula, x:y, where x represents the exact prefix that you want to add to called number and y represents the number of digits stripped; be aware that the colon separates the prefix and the number of stripped digits. For example, enter 91010:6 in the field, which means that you want to strip 6 digits and then add 901010 to the beginning of the called number. In this example, a national call of 2145551234 becomes 910101234. You can strip up to 24 digits and prefix/add up to than 16 digits.

Transferring Calls Between Trunks

Using Cisco Unified Communications Manager Administration, you can configure trunks as OnNet (internal) trunks or OffNet (external) trunks by using Trunk Configuration or by setting a clusterwide service parameter. Used in conjunction with the clusterwide service parameter, Block OffNet to OffNet Transfer, the configuration determines whether calls can be transferred over a trunk.

To use the same trunk to route both OnNet and OffNet calls, associate the trunk with two different route patterns. Make one trunk OnNet and the other OffNet with both having the Allow Device Override check box unchecked.

Configuring Transfer Capabilities Using Trunk Configuration

Using Cisco Unified Communications Manager Administration Trunk Configuration, you can configure a trunk as OffNet or OnNet. The system considers calls that are coming to the network through that trunk as OffNet or OnNet, respectively. Use the Trunk Configuration window field, Call Classification, to configure the trunk as OffNet, OnNet, or Use System Default. See Table 41-2 for description of these settings.

The Route Pattern Configuration window provides a drop-down list box called Call Classification, which allows you to configure a route pattern as OffNet or OnNet. When Call Classification is set to OffNet and the Allow Device Override check box is unchecked, the system considers the outgoing calls that use this route pattern as OffNet (if configured as OnNet and check box is unchecked, outgoing calls are considered OnNet).

You can use the same trunk to route both OnNet and OffNet calls by associating the trunk with two different route patterns: one OnNet and the other OffNet, with both having the Allow Device Override check box unchecked. For outgoing calls, the outgoing device setting classifies the call as either OnNet or OffNet by determining whether the Allow Device Override check box is checked.

In route pattern configuration, if the Call Classification is set as OnNet, the Allow Device Override check box is checked, and the route pattern is associated with an OffNet Trunk, the system considers the outgoing call as OffNet.

Table 41-2 Trunk Configuration Call Classification Settings

Setting Name	Description
OffNet	This setting identifies the trunk as being an external trunk. When a call comes in from a trunk that is configured as OffNet, the outside ring gets sent to the destination device.
OnNet	This setting identifies the trunk as being an internal trunk. When a call comes in from a trunk that is configured as OnNet, the inside ring gets sent to the destination device.
Use System Default	This setting uses the Cisco Unified Communications Manager clusterwide service parameter Call Classification.

Configuring Transfer Capabilities by Using Call Classification Service Parameter

To configure all trunks to be OffNet (external) or OnNet (internal), perform the following two steps:

1. Use the Cisco Unified Communications Manager clusterwide service parameter Call Classification.
2. Configure individual trunks to Use System Default in the Call Classification field that is on the Trunk Configuration window.

Blocking Transfer Capabilities by Using Service Parameters

Block transfer restricts the transfer between external devices, so fraudulent activity gets prevented. You can configure the following devices as OnNet (internal) or OffNet (external) to Cisco Unified Communications Manager:

- H.323 gateway
- MGCP FXO trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- SIP trunk

If you do not want OffNet calls to be transferred to an external device (one that is configured as OffNet), set the Cisco Unified Communications Manager clusterwide service parameter, Block OffNet to OffNet Transfer, to True.

If a user tries to transfer a call on an OffNet trunk that is configured as blocked, a message displays on the user phone to indicate that the call cannot be transferred.

Related Topics

- Route Pattern Configuration, *Cisco Unified Communications Manager Administration Guide*
- Gateway Configuration, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*

Dependency Records for Trunks and Associated Route Groups

To find route groups that use a specific trunk, choose Dependency Records from the Related Links drop-down list box that is provided on the Cisco Unified Communications Manager Administration Trunk Configuration window. The Dependency Records Summary window displays information about route groups that are using the trunk. To find more information about the route group, click the route group, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

For more information about Dependency Records, see "Accessing Dependency Records" in the *Cisco Unified Communications Manager Administration Guide*.

Related Topics

- Trunk Configuration Checklist, page 41-1
- Trunk Types in Cisco Unified Communications Manager Administration, page 41-8

H.235 Support for Trunks

This feature allows Cisco Unified Communications Manager trunks to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints so that the two endpoints can establish a secure media channel.

For more information, see the *Cisco Unified Communications Manager Security Guide*.

Where to Find More Information

Related Topics

- Trunk Configuration Checklist, page 41-1
- Cisco Unified Communications Manager Trunk Configuration, page 41-7
- Trunks and the Calling Party Normalization Feature, page 41-10
- Transferring Calls Between Trunks, page 41-12
- Dependency Records for Trunks and Associated Route Groups, page 41-13
- H.235 Support for Trunks, page 41-14
- Gatekeepers and Trunks, page 8-10
- Location-Based Call Admission Control Over Intercluster Trunk, page 8-9
- Cisco Voice Gateways, page 38-4
- Gateways, Dial Plans, and Route Groups, page 38-18
- Understanding Session Initiation Protocol, page 40-1
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*
- Gatekeeper Configuration, *Cisco Unified Communications Manager Administration Guide*
- Calling Party Normalization, *Cisco Unified Communications Manager Features and Services Guide*
- "Using the International Escape Character +" section on page 16-22

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design (SRND)*
- *Configuring Cisco Unified Communications Voice Gateways*
- *Cisco Unified Communications Manager Security Guide*