Configure Gateways

Gateway Overview

Cisco offers a wide variety of voice and video gateways. A gateway provides interfaces that allow the Unified Communications network to communicate with an external network. Traditionally, gateways have been used to connect the IP-based Unified Communications network to legacy telephone interfaces such as the PSTN, a private branch exchange (PBX), or legacy devices such as an analog phone or fax machine. In its simplest form, a voice gateway has an IP interface and a legacy telephony interface, and the gateway translates messages between the two networks so that the two networks can communicate.

Gateway Protocols

Most Cisco gateways offer multiple deployment options and can be deployed using any one of a number of protocols. Depending on the gateway that you want to deploy, your gateway may be configurable using any of the following communication protocols:

- Media Gateway Control Protocol (MGCP)
- Skinny Call Control Policy (SCCP)
- Session Initiation Protocol (SIP)
- H.323

Vendor Interface Cards

The Vendor Interface Card (VIC) must be installed on the gateway to provide a connection interface for external networks. Most gateways offer multiple VIC options and each VIC may offer many different ports and connection types for both analog and digital connections.

Refer to your gateway documentation for the protocols, cards, and connections that are offered with your gateway.

Gateway Setup Prerequisites

Install the Hardware

Before you configure the gateway in Cisco Unified Communications Manager, you must perform the following tasks on your gateway hardware:

- Install and configure the gateway
- Install any vendor interface cards (VICs) on the gateway.
- Use the CLI to configure IOS on the gateway.

For details, refer to the hardware and software documentation that comes with your gateway.

Note To get to the default web pages for many gateway devices, you can use the IP address of that gateway. Make your hyperlink url = http://x.x.x.x/, where x.x.x.x is the dot-form IP address of the device. The web page for each gateway contains device information and the real-time status of the gateway.

Plan the Gateway Deployment

Before configuring the gateway in Cisco Unified Communications Manager, make sure that you adequately plan the types of connections that you want to configure on the gateway. Many gateways can be configured using any one of MGCP, SIP, H.323, or SCCP as the gateway protocol. The connection types for each type of deployment vary according to the protocol that you choose and the VICs that are installed on the gateway. Be sure to understand the following:

- Which gateway protocols does your gateway support.
- What types of port connections the VICs on the gateway support.
- What types of connections are you planning on configuring?
- For analog connections, are you connecting to the PSTN, legacy PBX, or to legacy devices.
- For digital access connections, are you connecting to a T1 CAS interface, or to a PRI interface?
- For FXO connections, how do you want to direct incoming calls? Are you directing incoming calls to an automated IVR or to an attendant?

Gateway Configuration Task Flow

Perform the following tasks to add your network gateways to Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Perform any of the following procedures depending on the protocol that you want to deploy: • Configure MGCP Gateway, on page 3 • Configure SCCP Gateway, on page 10 • Configure SIP Gateway, on page 13 • Configure H.323 Gateway, on page 15	Configure your gateways in the Unified Communications Manager. Many Cisco gateways can be deployed using any one of MGCP, SCCP, SIP, or H.323 as the gateway protocol. Review your gateway documentation to determine which protocols your gateway supports and which protocol is best for your deployment.
Step 2	Configure Clusterwide Call Classification for Gateway, on page 16	**Optional**. Configure a clusterwide service parameter to classify all calls coming from the gateway ports in your network to be internal (OnNet) or external (OffNet).
Step 3	Block OffNet Gateway Transfers, on page 16	**Optional**. Block Unified Communications Manager from transferring calls from one external (OffNet) gateway to another external gateway, configure the **Block OffNet to Offnet Transfer** service parameter.

Configure MGCP Gateway

Perform the following tasks to configure a Cisco gateway to use an MGCP configuration.

Before you begin

Confirm Unified CM port connections for MGCP gateways. From Cisco Unified CM Administration, go to **System** > **Cisco Unified CM**, select the server and confirm the configured MGCP Listen port and MGP Keep-alive ports. In most cases, there is no need to change the default port settings.

Procedure

	Command or Action	Purpose
Step 1	Configure MGCP (IOS) Gateway, on page 4	Add the gateway in Cisco Unified CM Administration and choose **MGCP** as the gateway protocol. Configure the gateway with the appropriate slots and vendor interface cards (VICs).
Step 2	Configure Gateway Port Interface, on page 5	Configure the gateway port interface for the devices that connect to the VICs that are installed on the gateway. Most VICs include multiple port connections and options so you may have to configure a few different port interface types.

	Command or Action	Purpose
		Tip After you configure a port interface, from the **Related Links** drop-down list, select the **Back to MGCP Configuration** option to return to the **Gateway Configuration** window, where you can select and configure another port interface.
Step 3	Add Digital Access T1 Ports for MGCP Gateway, on page 8	**Optional**. If you have configured a digital access T1 CAS port interface, add T1 CAS ports to the gateway. You can add ports on an individual basis or add a range of ports simultaneously.
Step 4	Reset Gateway, on page 9	The configuration changes take effect after you reset the gateway.

Configure MGCP (IOS) Gateway

Perform the following procedure to add and configure an MGCP (IOS) gateway on the Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Add New**.

Step 3 From the **Gateway Type** drop-down list, select the gateway and click **Next**.

Step 4 From the **Protocol** drop-down list, choose **MGCP** and click **Next**.

Step 5 In the **Configured Slots, VICs and Endpoints** area, perform the following steps:

a) From each **Module** drop-down list, select the slot that corresponds to the Network Interface Module hardware that is installed on the gateway.

b) From each **Subunit** drop-down list, select the VIC that is installed on the gateway.

c) Click **Save**.
The **Port** icons appear. Each Port icon corresponds to an available port interface on the gateway. You can configure any port interface by clicking the corresponding port icon.

Step 6 Complete the remaining fields in the **Gateway Configuration** window. For more information on the fields, see the system Online Help.

Step 7 Click **Save**.

Configure Gateway Port Interface

You can configure the port connections for the devices that connect to the VICs that are installed on the gateway. Most VICs include multiple port connections and options so you may have to configure a few different port interface types.

Select any of the following tasks, depending on the type of interface that you want to configure:

- Configure Digital Access PRI Ports, on page 5
- Configure Digital Access T1 Ports for MGCP Gateway, on page 5
- Configure FXS Ports, on page 6
- Configure FXO Ports, on page 7
- Configure BRI Ports, on page 8

Configure Digital Access PRI Ports

Configure the PRI port interface for an MGCP (IOS) gateway.

Before you begin

Configure MGCP (IOS) Gateway, on page 4

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway on which you want to configure PRI ports.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, locate the Module and Subunit that contains the BRI port that you want to configure and click the **Port** icon that corresponds to the BRI port that you want to configure.
The **Gateway Configuration** window displays the BRI port interface.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 Complete the remaining fields in the **Gateway Configuration** window. Refer to the online help for field descriptions.

Step 6 Click **Save**.

Step 7 (Optional) If you want to configure more port interfaces for the gateway, from the **Related Links** drop-down list, choose **Back to MGCP Configuration** and click **Go**.

The **Gateway Configuration** window displays the available port interfaces for the gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 9.

Configure Digital Access T1 Ports for MGCP Gateway

Configure the port interface for digital access T1 CAS ports on an MGCP (IOS) gateway.

Before you begin

Configure MGCP (IOS) Gateway, on page 4

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway on which you want to configure a T1 port.

Step 3 In the **Configured Slots, VICs and Endpoints** area, locate the Module and Subunit on which you want to set up a Digital Access T1 (T1-CAS) port and click the corresponding **Port** icon.

Step 4 From the **Device Protocol** drop-down list, choose **Digital Access T1** and click **Next**.

Step 5 Enter the appropriate gateway configuration settings.

For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

For more information on adding ports to the Digital Access T1 CAS port interface, see Add Digital Access T1 Ports for MGCP Gateway, on page 8.

Configure FXS Ports

Configure Foreign Exchange Station (FXS) ports on an MGCP gateway. You can use FXS ports to connect the gateway to a Plain Old Telephone Service (POTS) legacy phone or to another legacy device such as a fax machine, speakerphone, legacy voice-messaging system, or Interactive Voice Response (IVR).

Before you begin

You must add a gateway before configuring ports.

Procedure

Step 1 In the Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway on which you want to configure FXS ports.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, click the **FXS Port** icon for the port that you want to configure.
The Port Selection area displays.

Step 4 From the **Port Type** drop-down list, choose the type of connection that you want to configure:

- **POTS**—Select this option if you want to connect this port to a POTS device such as a legacy phone.
- **Ground Start**—Select this option if you want to use ground a start signaling to connect this port to an unattended legacy device such as a fax machine, legacy voice-messaging system, or IVR.
- **Loop Start**—Select this option if you want to use a loop start signaling to connect this port to an unattended legacy device such as a fax machine, legacy voice-messaging system, or IVR.

Step 5 Click **Next**.
The **Port Configuration** window displays the configuration for the port interface with an analog access as the device protocol.

Step 6 From the **Device Pool** drop-down list, select a device pool.

Step 7 Complete the remaining fields in the **Port Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 8 Click **Save**.

Step 9 (Optional) To configure more port interfaces on the MGCP IOS gateway, from the **Related Links** drop-down list, select **Back to Gateway** and click **Go**.

The **Gateway Configuration** window displays the available ports for the gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 9.

Configure FXO Ports

Configure Foreign Exchange Office (FXO) ports on an MGCP (IOS) gateway. You can use FXO ports to connect the gateway to the PSTN or a legacy PBX.

Note Unified Communications Manager assumes all loop-start trunks lack the positive disconnect supervision. Configure trunks with the positive disconnect supervision as ground start, so that the active calls can be maintained during a server failover.

Before you begin

Configure MGCP (IOS) Gateway, on page 4

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway for which you want to configure FXO ports.

Step 3 From the **Configured Slots, VICs, and Endpoints** area, locate the **Module** and **Subunit** that contain the FXO port on which you want to set up an FXO port interface and click the **Port** icon for the port that you want to configure.

Step 4 From the **Port Type** drop-down list, select either **Ground-Start** or **Loop-Start**.

Note If you are configuring the VIC-2 FXO port, you must select the same port type for both ports of the subunit module.

Step 5 From the **Device Pool** drop-down list, select a device pool.

Step 6 In the **Attendant DN** text box, enter the directory number to which you want to route all incoming calls from this port connection. For example, a zero or the directory number for an attendant.

Step 7 Complete any remaining fields in the **Port Configuration** window. Refer to the online help for field descriptions.

Step 8 Click **Save**.

Step 9 (Optional) To configure more port interfaces on the MGCP IOS gateway, from the **Related Links** drop-down list, select **Back to Gateway** and click **Go**.

The **Gateway Configuration** window displays the available ports for the gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 9.

Configure BRI Ports

Configure a BRI port interface for an MGCP (IOS) gateway.

Before you begin

Configure MGCP (IOS) Gateway, on page 4

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway on which you want to configure BRI ports.

Step 3 In the **Configured Slots, VICs, and Endpoints** section, locate the subunit that uses BRI ports and click the **Port** icon for the port that you want to configure.
The **Gateway Configuration** window displays the information for the BRI port interface.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 Enter the appropriate Gateway Information and Port Information settings. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

Step 7 (Optional) If you want to configure more port interfaces for the gateway, from the **Related Links** drop-down list, choose **Back to MGCP Configuration** and click **Go**.

The **Gateway Configuration** window displays the available port interfaces for the MGCP gateway.

When you have completed configuring more ports interfaces, see Reset Gateway, on page 9.

Add Digital Access T1 Ports for MGCP Gateway

Add and configure T1 CAS ports to a T1 Digital Access port interface for an MGCP gateway. You can add and configure up to 24 T1 CAS ports. You can also add ports on an individual basis or add and configure a range of ports simultaneously. If you enter a range of ports, Unified Communications Manager applies the configuration to the entire range of ports.

Before you begin

Configure Digital Access T1 Ports for MGCP Gateway, on page 5

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway that contains the T1 CAS port interface.

Step 3 Click **Add a New Port**.

Step 4 From the **Port Type** drop-down list, select the type of port that you want to add and click **Next**.

Step 5 Enter port numbers in the **Beginning Port Number** and **Ending Port Number** fields to specify the range of ports that you want to add and configure.

For example, enter `1` and `10` to add ports 1 through 10 to the port interface simultaneously.

Step 6 From the **Port Direction** drop-down list, configure the direction of calls passing through this port:

- **Bothways**—Select this option if the port allows both inbound and outbound calls.
- **Inbound**—Select this option if the port allows inbound calls only.
- **Outbound**—Select this option if the port allows outbound calls only.

Step 7 For EANDM ports, from the **Calling Party Selection** drop-down list, choose how you want the calling number to display for outbound calls from the device that is attached to this port:

- **Originator**—Send the directory number of the calling device.
- **First Redirect Number**—Send the directory number of the redirecting device.
- **Last Redirect Number**—Send the directory number of the last device to redirect the call.
- **First Redirect Number (External)**—Send the directory number of the first redirecting device with an external phone mask applied.
- **Last Redirect Number (External)**—Send the directory number of the last redirecting device with the external phone mask applied.

Step 8 Click **Save**.

Step 9 If you want to configure more ports for the MGCP gateway, from **Related Links** select **Back to Gateway** and click **Go**. When the Digital Access T1 port interface appears, perform either of the following steps:

- If you want to add additional Digital Access T1 CAS ports to this port interface, return to step 3 (**Add a New Port**) of this procedure.
- If you want to configure more port interfaces on the gateway, from **Related Links** select **Back to MGCP Configuration** and click **Go**. The **Gateway Configuration** window displays the available ports for the gateway subunit modules.
- When you have completed configuring more ports interfaces, see Reset Gateway, on page 9.

Reset Gateway

Most gateways need to be reset for configuration changes to take effect. We recommend that you complete all necessary gateway configuration before performing a reset.

Note Resetting an H.323 gateway only reinitializes the configuration that Unified Communications Manager loaded and does not physically restart or reset the gateway.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Find** and select the gateway.

Step 3 Click the check box beside the gateway that you want to reset and click **Reset Selected**. The **Device Reset** dialog box appears. Do one of the following actions:

Step 4 Click **Reset**.

MGCP Caller-ID Restriction

If FROM header contains a special character(s) in the incoming SIP requests, it impacts the SIP-MGCP/323 call flow and the system disconnects the call or displays issues. Hence fix the networking node from where the request is reaching out to Unified Communications Manager.

For Example:

- Special characters present along with alphabets like "Per%cent" affect the display name.
- Many special characters present like "0%09%0A%01%05%0A%01%03%0A%01%04" could disconnect the call as the remote name being sent to MGCP side as CRCX can have issues.

Configure SCCP Gateway

Perform the following tasks to configure a Cisco gateway to use an SCCP configuration.

Procedure

	Command or Action	Purpose
Step 1	Configure SCCP as Gateway Protocol, on page 10	Configures a gateway to use SCCP as the gateway protocol.
Step 2	Enable Autoregistration of Nonconfigured Analog FXS Ports	Enables auto registration of nonconfigured analog FXS ports.
Step 3	Enable Auto Registration for Analog Phones, on page 11	Enables auto registration for the specified ports to fetch the DN from the pool of auto-registration DNs.

Configure SCCP as Gateway Protocol

You can configure a Cisco gateway to use SCCP as the gateway protocol. You can use this deployment option to connect Unified Communications Manager to analog access devices or ISDN BRI devices using FXS or BRI ports. You cannot connect an SCCP gateway to digital access T1 or E1 trunks.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Add New**.

Step 3 From the **Gateway Type** drop-down list, choose a gateway that uses SCCP and click **Next**.

Step 4 From the **Protocol** drop-down list, choose **SCCP**.

Step 5 In the **Configured Slots, VICs and Subunits** section, perform the following steps:

a) For each **Module** drop-down list, select the slot that corresponds to the Network Interface Module hardware that is installed on the gateway.
b) For each **Subunit**, select the VIC that is installed on the gateway.

Step 6 Complete the remaining fields in the **Gateway Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 7 Click **Save**.
The **Port** icons appear alongside the subunit modules. Each port icon corresponds to a configurable port interface on the gateway. You can configure an analog access or ISDN BRI phone on a port by clicking the corresponding port icon.

Step 8 Apply the changes to the gateway when you complete the update:

a) Click **Reset Gateway**. The **Restart Gateway** pop-up appears.
b) Click **Reset**.

Enable Auto Registration for Analog Phones

Enable auto registration for specified ports to fetch the directory numbers from the pool of auto-registration DNs. By default, Unified Communications Manager does not allow auto registration for analog phones. The administrator must configure the gateway module to support analog phones to auto-register with Unified CM through their corresponding gateways using the SCCP protocol.

Note Supported gateway types are VG310, VG350, VG400, VG450, and ISR4K series.

Before you begin

- Enable autoregistration and specify the range of DNs that get assigned to the new endpoints while they connect to the network. For more information, see Enable Autoregistration section.
- Enable auto-config with SCCP protocol in the gateway. For more information, see CUCM Auto Configuration for SCCP Gateways guide.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Add New**.

Step 3 From the **Gateway Type** drop-down list, choose a gateway that uses SCCP and click **Next**.

Step 4 From the **Protocol** drop-down list, choose **SCCP**.

Step 5 In the **Gateway Details** section, perform the following steps:

a) Enter the last 10 digits of the **MAC Address** in the text box. The **Description** field value is auto-populated when you enter the MAC Address.

Note The MAC address of the gateway can either be the Ethernet MAC address or the Virtual MAC address assigned in the SCCP gateway's interface, communicating to the Unified Communications Manager.

When you provide the MAC address, each FXS port obtains the port name from the configured MAC address and its port number. The corresponding analog phones automatically register with this gateway.

For example, if NM-4VWIC-MBRD is selected in Module in Slot 0 drop-down list and VIC3-4FXS/DID-SCCP is selected in the **Subunit 0** drop-down list, 4 FXS port values are displayed namely **0/0/0, 0/0/1, 0/0/2, 0/0/3**. Click each port to view the corresponding port name in the **Description** field of **Phone Configuration** window. The displayed port name is the combination of MAC address and the port value.

The gateway uses the Virtual MAC address or Ethernet MAC address to communicate with the Unified Communications Manager based on the configuration. The Virtual MAC address can be used even when you replace the damaged gateway so that you do not need to perform any configuration changes in the Unified Communications Manager application.

b) Select the required **Cisco Unified Communications Manager Group** from the drop-down list to enable autoregistration.

Step 6 In the **Configured Slots, VICs and Endpoints** section, perform the following steps:

a) Select a slot corresponding to the Network Interface Module hardware that is installed on the gateway for each **Module** drop-down list and click **Save** to enable respective **Subunits**.
b) Select corresponding VICs installed on the gateway for one or more Subunits and click **Save**.

Note Slot and module indicate which slot and module have FXS ports. It also indicates a number of FXS ports.

Configure gateways only up to a Subunit level and not up to the port level as it auto-registers and obtain an auto DNs. For example, when the Subunit is selected to FXS, the corresponding FXS port selects one of the DN available in the auto-register DN pool and assigns the DN to the selected ports.

Step 7 Click **Apply Config**.

The gateway sends register request for all FXS configured ports regardless of whether that port is connected to a phone or not.

Enable Autoregistration of Nonconfigured Analog FXS Ports

Use this procedure to enable the autoregistration of nonconfigured Analog FXS Ports.

Procedure

Step 1 From Cisco Unified CM Administration, choose**System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the required server that is running.

Step 3 From the **Service** drop-down list, choose **Cisco Call Manager(Active)**.

Step 4 In the **Clusterwide Parameters (Device-PRI and MGCP Gateway)** section, ensure that the value of **Enable Auto Registration for FXS Ports** drop-down list is set to **True**.

Note Set the value of **Enable Auto Registration for FXS Ports** to **False** to disable the auto registration of nonconfigured Analog FXS ports.

Step 5 Click **Save**.

Troubleshooting Tips

Perform the following in Unified Communications Manager to ensure the ports are registered and obtain an auto DNs.

1. Configure SCCP as Gateway Type.
2. Enable Auto-registration
3. Select an Analog Phone as the Device Type
4. Ensure sufficient DNs are available in the pool to accommodate the number of voice ports.

Configure SIP Gateway

Perform the following tasks to configure a SIP gateway in Unified Communications Manager. Many Cisco gateways and third-party gateways can be configured to use SIP. Unified Communications Manager does not contain a gateway device type for SIP gateways.

Before you begin

You must install the gateway hardware in your network and configure the IOS software on the gateway before you add the gateway in Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profile, on page 14	Configure SIP settings and apply to a SIP profile. Trunk uses this settings to connect to the SIP gateway.
Step 2	Configure SIP Trunk Security Profile., on page 14	Configure a SIP Trunk Security Profile so that trunk uses this to connect to the SIP gateway. You can configure security settings, such as device security mode, digest authentication, and incoming/outgoing transport type settings.
Step 3	Configure SIP Trunk for SIP Gateway, on page 14	Configure a SIP trunk that points to the SIP gateway. Apply the SIP Profile and the SIP Trunk Security Profile to the SIP trunk.

Configure SIP Profile

Configure a SIP profile for your SIP gateway connection.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Perform either of the following steps:

- Click **Add New** to create a new profile.
- Click **Find** to select an existing SIP profile.

Step 3 Complete the fields in the **SIP Profile Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Configure SIP Trunk Security Profile.

Configure a SIP trunk security profile with security settings for a trunk that connects to a SIP gateway.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile.**

Step 2 Perform either of the following steps:

a) Click **Find** to select an existing profile.
b) Click **Add New** to create a new profile.

Step 3 Complete the fields in the **SIP Trunk Security Profile Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 4 Click **Save**.

Configure SIP Trunk for SIP Gateway

Configure a SIP trunk to connect Unified Communications Manager to a Cisco or third party gateway that uses SIP. Under this configuration, do not enter the gateway as a device in the **Gateway Configuration** window.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New** to set up a new SIP trunk.

Step 3 From the **Trunk Type** drop-down list choose **SIP Trunk**.

Step 4 From the **Protocol** drop-down list, choose **None**.

Step 5 In the **Destination Address** field of the SIP Information pane, enter an IP address, fully qualified domain name, or DNS SRV record for the SIP gateway.

Step 6 From the **SIP Trunk Security Profile** drop-down list, choose the SIP trunk security profile that you configured for this gateway.

Step 7 From the **SIP Profile** drop-down list box, choose the SIP profile that you configured for this gateway.

Step 8 Complete the fields in the **SIP Trunk Configuration** window. Refer to the online help for field descriptions.

Step 9 Click **Save**.

Configure H.323 Gateway

Configure an H.323 gateway in Unified Communications Manager for a non-gatekeeper H.323 deployment.

Note If your deployment includes H.323 gatekeepers, you can also add an H.323 gateway by setting up a gatekeeper-controlled H.225 trunk. This scenario is not documented in this guide because gatekeeper usage has been in steady decline recent years. If you want to configure gatekeepers and H.225 gatekeeper-controlled trunks, refer to the *Cisco Unified Communications Manager Administration Guide,* Release 10.0(1).

Note When a gateway is registered with Unified Communications Manager, the registeration status may display in Unified Communications Manager Administration as unknown.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Add New**.

Step 3 From the **Gateway Type** drop-down list, choose **H.323 Gateway**.

Step 4 In the **Device Name** field, enter the IP address or hostname of the gateway.

Step 5 If you want to use H.235 to configure a secure channel, check the **H.235 Data Passthrough** check box.

Step 6 Configure the fields in the **Gateway Configuration** window.

For more information on the fields and their configuration options, see the system Online Help.

Step 7 Click **Save**.

Step 8 Click **Reset** to reset the gateway and apply the changes.

Most gateways need to be reset for configuration changes to take affect. We recommend that you complete all necessary gateway configuration before performing a reset.

Configure Clusterwide Call Classification for Gateway

Configure the **Call Classification** setting for your network gateways. This setting determines whether the system considers the gateways in the network to be internal (OnNet) or external (OffNet).

The **Call Classification** field also appears in the configuration window for individual gateway port interfaces. By default, each gateway port interface is configured to use the setting from the clusterwide service parameter. However, if **Call Clasification** on a port is configured differently from the clusterwide service parameter, the setting on that port overrides the service parameter setting.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server on which the Cisco CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Under **Clusterwide Parameters (Device - General)**, configure one of the following values for the **Call Classification** service parameter.

- **OnNet**—Calls from this gateway are classified as originating from inside the company network.
- **OffNet**—Calls from this gateway are classified as originating from outside the company network.

Step 5 Click **Save**.

Block OffNet Gateway Transfers

Use this procedure if you want to configure the system to block calls that are transferred from one external (OffNet) gateway to another external (OffNet) gateway. By default, the system allows transfers from one external gateway to another external gateway.

The setting that determines whether a gateway is external (OffNet) or internal (OnNet) is determined by the Call Classification setting. It is configured using a clusterwide service parameter, or by configuring any of the following port interfaces:

- MGCP T1/E1 port interfaces
- MGCP FXO port interface
- H.323 gateways
- SIP trunks

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server on which the Cisco CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure a setting for the **Block OffNet to Offnet Transfer** service parameter:

- **True**—Select this option to cancel transfers between two external (OffNet) gateways.
- **False**—Select this option to allow transfers between two external (OffNet) gateways. This is the default option.

Step 5 Click **Save**.

Note You can also classify calls through a gateway as OnNet or OffNet by associating the gateway to a route pattern and configure **Call Classification** in the **Route Pattern Configuration** window.