CHAPTER 5

Configuring IP Connectivity Settings

This section describes the following topics:

About IP Connectivity

In the IP Connectivity section of the Settings tab, you can select the IP connectivity mode in which the gateway operates, set the address of the gatekeeper with which the gateway registers, and define the way in which the gateway interacts with the gatekeeper.

You can configure the IP connectivity mode in the following two ways:

- Using a gatekeeper—The gateway registers with a gatekeeper and uses the gatekeeper for every call (see the "Configuring the Gateway to Register With a Gatekeeper" section on page 5-1).
- Peer-to-Peer—The gateway connects directly to a peer device without the need for a gatekeeper (see the "Configuring the Gateway for Peer-to-Peer IP Connectivity" section on page 5-3). Peer devices include Cisco Unified CallManager.

⚠ **Caution** Changing the IP connectivity mode setting causes the gateway to reset.

Configuring the Gateway to Register With a Gatekeeper

In the IP Connectivity section of the Settings tab, you can configure the gateway to register with a gatekeeper.

Procedure

Step 1 In the gateway interface, on the sidebar, click **Gateway** (if not already selected).

Step 2 Click the **Settings** tab.

Step 3 Click the **IP Connectivity** button.

Step 4 In the IP connectivity mode field, choose **Using gatekeeper**.

Step 5 Make one of the following selections:

- Select the **Gatekeeper auto discover and register** option button for the gateway to automatically search for and attempt to register to a gatekeeper.
- Select the **Specify Gatekeeper address** option button to specify the gatekeeper to which the gateway registers.

Step 6 In the Gatekeeper address field, do one of the following:

- Type the IP address of the gatekeeper to which the gateway registers.

—or—

- Click **Browse**.

The Discovered Gatekeepers dialog box appears, displaying all gatekeepers located on the same network segment as the gateway.

- Select a discovered gatekeeper.
- Click **OK**.

Step 7 In the Gatekeeper port field, type the port number of the gatekeeper. The default setting is 1719.

Step 8 Select the **Registration refresh every n seconds** check box to set the Time To Live interval (in seconds) that determines how often the gateway sends a "keep alive" message to the gatekeeper to ensure that the gateway registration is listed with the gatekeeper and does not expire. Enter a value in seconds in the field.

Step 9 In the Gateway registration mode field, choose the method of registration of services with the gatekeeper:

- Version 1—For gatekeepers that support H.323 version 1.
- Version 2—For gatekeepers that support H.323 version 2 or later.

Step 10 (PRI gateways only) Select the **Unregister from Gatekeeper on ISDN connection failure** check box to force the gateway to unregister from its gatekeeper when both ISDN D-channel connections are no longer active. The gatekeeper is forced to send new IP-to-ISDN calls through a different gateway, thus ensuring high call completion rates. The gateway re-registers to the gatekeeper when the ISDN connected is restored.

Step 11 (Serial gateways only) Select the **Unregister from Gatekeeper when no cable is connected** check box to force the gateway to unregister from its gatekeeper when no cable connection is found. When at least one cable is connected to the gateway, the gateway can register to its gatekeeper. If no cables are connected to the gateway, the gateway is automatically unregistered from the gatekeeper.

Step 12 Select the **Send load balancing messages (RAI)** check box to enable the sending of RAI messages to the gatekeeper for the purpose of load balancing on the network. If you select this option, perform step 13 and step 14.

Gatekeepers can perform load balancing on the network using feedback from the gateway in the form of Resource Available Indication (RAI) messages that inform the gatekeeper of gateway resource availability. If the gateway is unavailable, the gatekeeper performs line hunting operations to route the call to an alternative gateway.

When you set the gateway for RAI/RAC, it sends periodic RAI messages that inform the gatekeeper of the current resource availability in the gateway. The gatekeeper responds with Resource Available Confirmation (RAC) messages to acknowledge receipt of the RAI messages. In step 13 and step 14, you can configure the upper and lower threshold for triggering RAI messages according to resource availability in the gateway.

Step 13 In the Send 'busy' when load is more than field, enter the upper threshold for gateway resource utilization as a percentage of total resources. When resource use is greater than the threshold, the gateway sends the gatekeeper a 'busy' RAI message, indicating to the gatekeeper that it should stop routing calls to this gateway.

Step 14 In the Send 'free' when load is more than field, enter the lower threshold for gateway resource utilization as a percentage of total resources. When resource use is less than the threshold, the gateway sends the gatekeeper a 'free' RAI message, indicating to the gatekeeper that it can resume routing calls to this gateway.

Configuring the Gateway for Peer-to-Peer IP Connectivity

In the IP Connectivity section of the Settings tab, you can configure the gateway for peer-to-peer IP connectivity.

Procedure

Step 1 In the gateway interface, on the sidebar, click **Gateway** (if not already selected).

Step 2 Click the **Settings** tab.

Step 3 Click the **IP Connectivity** button.

Step 4 In the IP connectivity mode field, choose **Peer-to-Peer**.

Note Changing this setting causes the gateway to reset.

Step 5 In the Peer hunting mode field, choose one of the following options:

- Always start from first peer—The gateway attempts to connect a call to the first peer device on the Peer list section. If the call fails due to one of the H.323 call disconnect reasons (see the "About Peer-to-Peer H.323 Call Disconnect Reasons" section on page 5-5), the gateway tries each peer device in the Peer list section in order until the call is successfully connected. If the gateway fails to connect the call after trying all the peer devices on the list, it rejects the call.
- Always start from last successful peer—The gateway attempts to connect a call to the last peer device in the Peer list section with which a call was successfully established. An arrow in the Peer list section indicates with which of the peer devices a call was last connected successfully. If the call fails due to one of the H.323 call disconnect reasons (see the "About Peer-to-Peer H.323 Call Disconnect Reasons" section on page 5-5), the gateway tries each peer device in the Peer list section in order until the call is successfully connected. The arrow moves to the peer device with which the call connection is successful. If the gateway fails to connect the call after trying all the peer devices on the list, it rejects the call and the arrow indicates with which peer device a call was last connected successfully. This is the default setting.
- Round Robin—As for the Always start from last successful peer setting, except that the arrow advances to the next peer device in the Peer list section even if the call connection succeeds.

Note The peer hunting process starts when any of the following events occur: the gateway fails to establish a Transmission Control Protocol (TCP) connection to the specified peer device after a timeout; the gateway receives a "Release Complete" message from a peer device with a "No Resources" call rejection reason, or one of the other reasons that the Peer-to-Peer disconnect reason add advanced command specifies; or the gateway establishes a TCP connection to the specified peer device, but does not receive a valid H.323 message from the peer device after a timeout.

Step 6 In the Peer list section, you can configure peer devices currently configured to work with the gateway. The Peer list section displays all configured peer devices in a table with the following columns:

- Peer #—The sequential number of the peer in the list.
- Description—The description of the peer device.
- IP Address—The peer IP address.
- IP Port—The peer IP port number.
- Calls—Displays "Yes" or "No" to indicate whether or not there are currently any active calls between the peer and gateway.

To change the order of peer devices used in peer hunting, select a peer device and click the up or down arrow button to change its order.

To add or edit a peer device, click **Add** or select the peer device and click **Edit**. Perform the following steps in the Add peer or Edit peer dialog box:

- In the IP Address field, type or edit the peer IP address.

Note Two peers cannot have the same IP address or host name/Uniform Resource Locator (URL).

- In the IP Port field, enter or edit the peer IP port number.
- In the Description field, enter or edit the description of the peer.
- Click **Upload**.

Note You cannot add a single peer to the Peer list section more than once.

To delete a peer device, select the peer device and click **Delete**. Deleting a peer does not cause its active calls to disconnect, but no new calls are routed to the deleted peer.

Note The peer hunting process stops when one of the peer devices accepts the call or when the call is rejected with a disconnect reason. When a gateway has scanned the Peer list section and still cannot connect a call, the following rules apply: if at least one of the peers rejected the call due to capacity overload, the call rejection reason (towards the call originator) is "No Resources"; in all other cases, the call rejection reason is "Unreachable Destination."

Step 7 In the Peer hunting timeout (sec) field, enter the length of time (between 1 and 10 seconds) for which the gateway waits for a Transmission Control Protocol (TCP) response from each peer device contacted. The default value is 5 seconds.

Step 8 Select the **Accept calls from defined peers only** check box if you want the gateway to reject incoming calls from IP-side entities not defined in the peer list. If deselected, the gateway allows incoming calls from IP-side entities not defined in the Peer list section.

Step 9 (PRI gateways only) In the Reject calls from peer devices when less than ***n*** B channels are free field, type the lower capacity threshold for rejecting calls from H.323 peer devices. The default setting is 6.

About Peer-to-Peer H.323 Call Disconnect Reasons

Table 5-1 lists the reasons for which the gateway peer-to-peer hunting module might disconnect a call.

Table 5-1 Peer-to-Peer H.323 Call Disconnect Reasons

Number	H.323 Call Disconnect Reason
1	There is no available bandwidth.
2	Gatekeeper resources have been exhausted.
3	The destination cannot be reached.
4	The destination rejected the transaction request.
5	Version is not compatible.
6	No permission to perform requested transaction.
7	The destination gatekeeper cannot be reached.
8	Gateway resources have been exhausted.
9	Destination address is not formatted correctly.
10	LAN crowding has caused the call to be dropped.
11	The destination is busy and cannot respond to the call transaction.
12	Undefined reason for transaction failure.
13	Call should be routed to a gatekeeper.
14	Call should be forwarded.
15	Call should be routed to an MC.
16	Call deflection has occurred.
17	Access denied.
18	The called party is not registered at the destination.
19	The calling party is not registered.
20	The connection failed and a new one should be made.
21	The called party has no H.245 capabilities.
22	Facility message sends conference list choice.
23	Request to establish H.245 connection.
24	An indication from an endpoint or a gatekeeper to send a new set of tokens in the *tokens* and/or *cryptoTokens* field of the Facility message.
25	Indicates that the purpose of the message is to update feature set information that was previously sent in the Facility message.

Table 5-1 Peer-to-Peer H.323 Call Disconnect Reasons (continued)

Number	H.323 Call Disconnect Reason
26	Indicates that the purpose of the message is to forward elements of another message, if that message cannot be sent.
27	Indicates that the purpose of the message is to transport higher-layer information.