CHAPTER 3

Basic Configuration for the Gateway

This section describes the following topics:

Viewing the Status Tab

The Status tab displays the current rate of use of gateway resources, the total number of current calls, and servicing details. Table 3-1 lists the information in the Status tab.

Table 3-1 Status Tab Sections

Section Name	Description
General	• Status—Indicates the operational status of the gateway: OK or Failure. In cases of failure, a text description of the problem appears. For example, "PRI connection, remote side: loss of frame alignment."
Gateway Resource Meter	• Overall Gateway usage (%)—Displays the rate of gateway resources currently in use. • CPU usage (%)—Displays the rate of CPU resources currently in use. • Audio transcoder usage (%)—Displays the rate of audio transcoding resources currently used for video calls. • ISDN B channels in use—Displays the total number of Integrated Services Digital Network (ISDN) B channels currently in use (Cisco Unified Videoconferencing 3545 PRI Gateway only).

Table 3-1 Status Tab Sections (continued)

Section Name	Description
Calls	• Number of calls—Displays the total number of calls currently in progress in the gateway.
Servicing Gatekeeper	• IP address—Displays the IP address of the gatekeeper to which the gateway is currently registered. • Host name—Displays the name of the servicing gatekeeper.

Related Topics

- Viewing B Channel Status, page 3-2
- Refreshing Gateway Status, page 3-3

Viewing B Channel Status

Note This section applies only to Cisco Unified Videoconferencing 3545 PRI Gateway.

From the Status tab in the gateway interface, you can view detailed status information for each B channel.

Procedure

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

Step 2 Click the **Status** tab (if not already selected).

Step 3 Click **Details**.

The Details dialog box appears, displaying the following information:

- Port 1 and Port 2—Displays the status of each of the B channels and of the D channel for each of the PRI ports.
- Disabled—Displays the number of disabled B channels for each port.
- Used—Displays the number of B channels currently in use for each port.
- Free—Displays the number of B channels currently available for each port.
- D channel—Displays the number of D channels for each port.

Refreshing Gateway Status

You can refresh the information that appears in the Status tab.

Procedure

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

Step 2 Click the **Status** tab (if not already selected).

Step 3 On the toolbar, click **Refresh**.

The information that appears in the Status tab is now refreshed.

Configuring Gateway Settings

In the Settings tab of the gateway interface, you can configure gatekeeper and Interactive Voice Response (IVR) addressing, the type of connection to the IP network, dialing delimiters, media encoding/decoding protocols, Quality of Service levels, which events cause the gateway to send SNMP traps, gateway resource levels for T.120 enabled and audio transcoded video calls, security settings, and advanced settings such as load balancing support.

The following topics discuss the settings you can configure in the Settings tab:

Setting the Unit Identifier

In the Basics section of the Settings tab, you can set the gateway identifier, which is the name that the gateway uses when registering to a gatekeeper and when dialing to endpoints.

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 **Basics** button (if not already selected).

Step 4 In the Gateway Identifier field, type the gateway identifier.

Configuring IVR Settings

In the IVR section of the Settings tab, you can configure the gateway to route calls using an Interactive Voice Response (IVR) system.

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 **IVR button**.

Step 4 Select the type of IVR functionality:

- Use internal IVR—Enables the gateway IVR functionality so that incoming calls can route to an endpoint on the IP network. Follow step 6 to step 8.

Note The IVR must be enabled for the port that supports IVR.

- Use external IVR—Select to set the IP address and port number for an IVR system in another device. Follow step 10 and step 11.

Step 5 Select the **IVR registers with gatekeeper** check box to enable the internal IVR to register with the gatekeeper.

Step 6 In the IVR registration name field, type the IVR registration alias used with the gatekeeper.

Step 7 Deselect the **Transfer to Operator when '*' pressed during IVR** check box to ignore the IVR operator digit (which is currently "*") and make it part of the dial string.

Step 8 In the IVR Operator Extension field, set the E.164 number of an endpoint that is registered with the gatekeeper to function as an IVR operator for incoming calls. To do this, type the same number for the IVR operator extension for each of the IP terminals that you want to include in the single number access. You can also use an ISDN endpoint as the IVR operator extension. To do this, define the IVR operator extension using the format <gateway service><ISDN number>.

Step 9 Select or deselect the **Return to main IVR menu if IP extension # is unreachable** check box to enable or disable an IVR retry.

Note This check box is selected by default except after a software upgrade, in which case it is deselected.

Regardless of whether or not this check box is selected, if a call cannot be connected, the user is played an IVR message that states the reason why the call cannot be connected, followed by instructions as to what to do next.

Step 10 In the IVR address field, type the IP address for the IVR system on the external device.

Step 11 In the Port field, type the port number for the IVR system on the external device. The default port setting is 1620.

Configuring Outgoing Call Delimiters

In the Delimiters section of the Settings tab, you can configure outgoing call delimiter characters.

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 **Delimiters** button.

Step 4 In the Second number delimiter field, type the character used as a second number delimiter for dialing more than one ISDN number in setting up a 2B call. You can use the pound sign (#), asterisk (*) or comma (,) as a delimiter in outgoing calls only. Not available in Cisco Unified Videoconferencing 3545 Serial Gateway.

Step 5 In the TCS4 extension delimiter field, type the character used as an extension number for TCS4 outgoing IP-to-ISDN call routing. You can use the pound sign (#), asterisk (*) or comma (,) as a delimiter in outgoing calls only. This setting does not apply for voice calls.

Note Since the comma cannot be used in the Party number field of the MCU Conference Control interface, we recommend that you do not use the comma as a second number delimiter or as a TCS4 extension delimiter.

About Encoding/Decoding Protocols

A number of video conferencing terminal applications require the G.722 and G.722.1 audio compression codecs to provide high quality voice communications. The G.722 and G.722.1 formats, using a digital sampling rate of 7 KHz, provide higher quality voice sampling with a greater dynamic range. The gateway does not transcode G.722 or G.722.1, but supports them transparently. Since the G.722 codec is of a much higher audio quality than other codecs and requires higher bandwidths, the gateway supports G.722 and G.722.1 at the following call bit rates:

- G.722 is supported in calls at 224, 256, 336, 384, 448, 512 Kbps (all gateways) and 768, 1472 and 1920 Kbps.
- G.722.1 is supported in calls at 64, 2B, and 128 Kbps.

Both endpoints in a call must support G.722 and G.722.1 audio codecs.

About Audio Transcoding

The Cisco Unified Videoconferencing 3545 PRI Gateway supports audio transcoding through the Audio Transcoder Module (TCM). Other Cisco gateways support audio transcoding through on-board Digital Signal Processing (DSP).

The TCM is a PCI mezzanine card (PMC) that implements Digital Signal Processing (DSP). The TCM has a processing capacity of up to 20 channels for audio transcoding in video calls.

The gateway TCM can perform audio transcoding between the following types of audio protocols:

- G.711 (ISDN) to G.723.1 (IP)
- G.723.1 (IP) to G.711 (ISDN)
- G.728 (ISDN) to G.711 (IP)
- G.711 (IP) to G.728 (ISDN)

Note When your unit includes both a gateway and MCU, G.728 transcoding is supported on the MCU only.

Each audio codec differs in the audio quality, compression, and bit rates that it provides. The G.711 codec provides toll quality audio at 64 Kbps, the G.728 codec provides near toll quality audio at 16 Kbps, and the G.723.1 codec provides voice quality audio at 5.3 or 6.4 Kbps.

Endpoints on the ISDN network usually support the G.711 and G.728 codecs. Endpoints on IP networks support G.711 and G.723.1 codecs. By performing transcoding between these audio protocols, the gateway can support communication between endpoints with codecs that are incompatible with each other.

Audio transcoding can also optimize the audio bandwidth usage either on the IP network (G.723.1 < > G.711) or on the ISDN network (G.728 < > G.711). Transcoding is particularly useful for ISDN codecs, where bandwidth can be limited to 128 Kbps for a video call. For example, when transcoding between G.728 and G.711 takes place, the audio bandwidth usage is compressed to 16 Kbps. This provides an additional 40 Kbps of bandwidth to the existing video bit rate on the ISDN network, contributing to improved video quality.

Note The gateway automatically performs A-Law G.711-to-µ-Law G.711 translation between the IP and ISDN sides if needed.

You can configure the gateway to prioritize the transcoding, giving preference to a particular codec that is applied to calls, thus optimizing the resource allocation utilized by each call.

About T.120 Data Collaboration Support

The gateway provides full end-to-end support for T.120 data collaboration sessions, provided all terminals support the T.120 standard in their conferencing applications. In video calls with data transfer, the gateway accepts whatever bandwidth the ISDN connection defines for the data and dynamically adjusts the outgoing bandwidth used for data by using the MLP, HMLP and VarMLP formats.

If transcoding or T.120 capabilities are required, the gateway has to reserve resources for these. The gateway can differentiate between those calls that support T.120 and those that do not. When receiving calls, the gateway can check whether you are reserving resources for transcoding or for T.120 capabilities.

The gateway enables the user to determine the trade-off between the number of non-T.120 calls that the gateway can support and the number of calls sent with T.120 capabilities. The total number of calls that the gateway can support is accordingly reduced by this reallocation of resources.

The H.320 standard defines space allocation within a call. The H.320 standard defines the logic for bit rate allocation among audio, video and data channels in the context of the overall bit rate of a call. If you work with T.120, reallocation of bandwidth is always at the expense of available video resources. The requirements of the H.320 standard govern this reallocation—it is not configured in the gateway. The gateway simply decides whether or not to send T.120 capabilities. You configure T.120 capabilities in the Advanced section of the gateway interface Settings tab.

Configuring Encoding/Decoding Protocols

In the Media Modes section of the Settings tab, you can configure and prioritize encoding and decoding protocols.

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 **Media Modes** button.

Step 4 In the Transcoding priority field, choose the priority that determines the order of requested audio transcoding or choose **Disable** to disable audio transcoding priority.

Note When your unit includes both a gateway and an MCU, G.728 transcoding is supported on the MCU only.

Step 5 You can configure the following audio codec settings:

- Select the **Enable G.722** check box to enable transparent support for the G.722 audio codec.
- Select the **Enable G.722.1** check box to enable transparent support for the G.722.1 audio codec.
- Select the **Enable G.728** check box to enable transparent support for the G.728 audio codec.

Step 6 You can configure the following video codec settings:

- Select the **Enable H.263** check box to enable transparent support for the H.263 video codec.
- Select the **Enable H.263+** check box to enable transparent support for the H.263+ video codec.
- Select the **Enable H.264** check box to enable transparent support for the H.264 video codec.

Step 7 You can configure the following data settings:

- Select the **Enable T.120** check box to enable transparent support for T.120 capabilities.
- Select the **Enable FECC** check box to enable transparent support for Far End Camera Control (FECC) capabilities.

Configuring ISDN Channel Bonding Settings for Downspeeding

In the Bonding section of the Settings tab, you can configure ISDN channel bonding parameters that affect downspeeding functionality.

Note The Bonding section is not available in Cisco Unified Videoconferencing 3545 Serial Gateway.

Downspeeding is the ability to complete and maintain a call when ISDN conditions are bad. In downspeeding, call capabilities are automatically renegotiated when a call fails. Downspeeding contributes to a higher percentage of call completion on the network. The gateway supports downspeeding at call setup and in mid-call.

With downspeeding, when connection problems occur at call setup, the gateway attempts to connect a call at a lower bit rate than that requested. Administrators can configure the gateway to attempt to connect a video call at a specified minimum bit rate, or to attempt to connect the call as a voice call.

In downspeeding, when connection problems occur in mid-call, the gateway attempts to connect a video call at the specified lower bit rate. When downspeeding is complete and the call is connected at the specified lower bit rate, the gateway notifies the Internet Protocol (IP) endpoint of the new call rate.

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 **Bonding** button.

Step 4 Select the **Enable bonding** check box to enable ISDN bonding support.

Step 5 In the Maximum B channels for bonded call field, choose the maximum number of B channels—3, 4, 5, 6, 8, 12, 23 or 30—that you want to allow for a single bonded call. The default setting for PRI gateways is 30.

When the number of B channels required to process a bonded call exceeds the number specified in this field, the gateway performs downspeeding as shown in Table 3-2.

Step 6 In the For bonded calls, allow downspeeding down to n B channels field, choose the minimum number of B channels that must be available before the gateway attempts to reconnect a video call.

Table 3-2 Downspeeding Policy Operation

Call Direction	Downspeed Advanced Command Parameter	If Call B Channels Exceed the Maximum:
IP (LAN) to WAN (ISDN)	enable (default)	Gateway tries to call at the maximum number of B channels
IP (LAN) to WAN (ISDN)	disable	Call disconnects
WAN (ISDN) to LAN (IP)	enable (default)	Call disconnects
WAN (ISDN) to LAN (IP)	disabled	Call disconnects.

Configuring Quality of Service Settings

You can configure the gateway to add a Quality of Service (QoS) IP precedence code in the IP header of outbound packets on the IP network. Routers on the network that support this method can give precedence to such coded packets and facilitate the transmission of the packets more efficiently. You can set priority levels on the gateway for voice calls, video calls, or both.

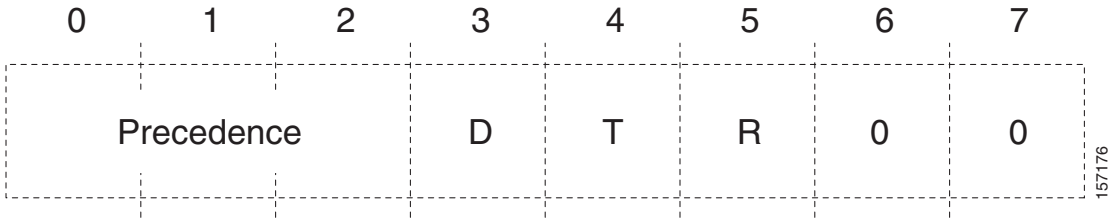
The Type of Service (TOS) field in the IP header contains eight bits and indicates the three abstract quality of service parameters:

Delay (D)

- Throughput (T)
- Reliability (R)

You can use the abstract parameters to choose the actual service parameters when transmitting a datagram through a particular network. The abstract parameters represent the three-way trade off between low delay, high throughput, and high reliability. Increasing the performance of one of the parameters can result in reduced performance of the other two. The TOS field in the IP header is shown in Figure 3-1.

Figure 3-1 TOS Field in the IP Header



Note The same fields can also be used to set DiffServ codepoint values

The function of each bit of the ToS field is as follows

- Bits 0-2: Precedence (an independent measure of the importance of the datagram)
- Bit 3: 0 = normal delay, 1 = low delay
- Bit 4: 0 = normal throughput, 1 = high throughput
- Bit 5: 0 = normal reliability, 1 = high reliability
- Bits 6-7: reserved for future use

The possible Precedence settings are as follows:

- 111 = Network Control
- 110 = Internetwork Control
- 101 = CRITIC/ECP
- 100 = Flash Override
- 011 = Flash
- 010 = Immediate
- 001 = Priority
- 000 = Routine

In the Quality of Service section of the Settings tab, you can assign a priority level to video and voice calls.

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 **Quality of Service** button.

Step 4 In the Quality of service support field, select one of the following option buttons:

- None—Select to disable quality of service support.
- Default (recommended)—Select to assign the default IP Type of Service (ToS) value for each media type.
- Custom—Select to assign your own IP ToS value for each media type. You can configure the following additional settings:
  - In the Control Priority (0-63) field, enter a whole number from 0 to 63 to set the priority level of signaling packets that the gateway sends out. The default value is 26.
  - In the Video Calls section Voice Priority (0-63) field, enter a whole number from 0 to 63 to set the priority level of voice packets that the gateway sends out. The default value is 34.
  - In the Video Priority (0-63) field, enter a whole number from 0 to 63 to set the priority level of video packets that the gateway sends out. The default value is 34.
  - In the Data Priority (0-63) field, enter a whole number from 0 to 63 to set the priority level of data packets that the gateway sends out. The default value is 26.
  - (PRI gateways only) In the Voice Calls section Voice Priority (0-63) field, enter a whole number from 0 to 63 to set the priority level of voice packets that the gateway sends out. The default value is 46.

Note You can click **Restore Defaults** to restore all default settings.

Configuring Alert Indications

In the Alert Indications section of the Settings tab, you can select which events trigger Simple Network Management Protocol (SNMP) traps. You can also define multiple SNMP servers to which the gateway sends the SNMP traps.

Note The gateway supports traps in the SNMPv1 format.

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 **Alert Indications** button.

Step 4 In the Events section, select events in the Disabled events field and click **Add** to select an event to monitor. Or, select an event in the Enabled events field and click **Remove** to remove that event from monitoring.

Step 5 Select the **Send SNMP Traps** check box to configure the IP address of the SNMP server to which the gateway sends SNMP trap notifications of the events selected in the **Enabled events** field. You can configure up to three different SNMP trap servers.

Step 6 In the Trap server IP and Port fields, enter the IP address and port number for each SNMP server to which you want the gateway to send SNMP trap notifications. To remove an SNMP server, set the SNMP server IP address to 0.0.0.0 and press the Upload button.

Related Topics

- Gateway Event Types, page 3-11
- Trap Severity Enumeration, page 3-15

Gateway Event Types

Table 3-3 lists proprietary Cisco SNMP trap event types for the Cisco Unified Videoconferencing 3545 PRI Gateway, as detailed in the RvTrapEventType textual convention.

Table 3-4 lists SNMP trap event types for the Cisco Unified Videoconferencing 3545 Serial Gateway, as detailed in the RvTrapEventType textual convention.

Note In certain cases, after a problem that caused a trap to be sent has been solved, an identical clearing trap is sent to indicate that the problem has been solved. The severity of the clearing trap is always 0. The trap OID and the RvTrapEventType value of the clearing trap are identical to those of the original trap sent when the problem occurred. The sending of a clearing trap is indicated by a severity level of "Clear."

Table 3-3 Cisco Unified Videoconferencing 3545 PRI GatewaySNMP Trap Event Types

Event Type	Trap is sent when ...	State	Severity
RAI status	A change in RAI status occurs.	TRUE	Warning
		FALSE	Clear
Bad video	Corrupt or empty video packets are present in the gateway. Includes the ID number of the call during which the event occurs.	TRUE	Minor
		FALSE	Clear
Power-up	The gateway has started to operate.		Information
Power-down	The gateway is shutting down.		Information
Gatekeeper registration state change	A change occurs in the registration status of the gateway.	TRUE	Clear
		FALSE	Minor
Loss of ISDN	A state change occurs for each enabled ISDN line.	TRUE	Critical
		FALSE	Clear
Loss of Ethernet	The network returns after going down. Indicates the time at which the network was restored.	TRUE	Critical
		FALSE	Clear
Max resource meter	A call could not be established because of a lack of one of the following resources—CPU, audio transcoder, DTMF detector or T.120 resources.		Warning
Network problem	A problem occurs on the network.	TRUE	Major
		FALSE	Clear
Card extract/Hot Swap	A card has been removed from the Cisco chassis under power or inserted into the chassis under power, or the when the gateway enters maintenance mode.	TRUE	Critical
		FALSE	Clear
Abnormal disconnect	A call has disconnected for a reason other than normal, busy or no answer.		Warning
ISDN downspeed	ISDN downspeeding to a lower rate is taking place.		Warning
Corrupt IVR messages on host	Corrupt IVR files are present in the gateway.		Warning
Corrupt WEB data	Corrupt web files are present in the gateway.		Major

Table 3-3 Cisco Unified Videoconferencing 3545 PRI GatewaySNMP Trap Event Types

Event Type	Trap is sent when ...	State	Severity
ISDN rollover activated	The gateway notifies the PSTN switch that the gateway cannot accept any further calls. ISDN rollover requires support by the PSTN switch application and presumes the availability of a pool of stacked gateways across the managed network. You can enable ISDN Rollover only after you set the gateway to work with the T1 interface.		Major
Call to peer rejected - trying alternate	A call to a peer has been rejected and the gateway is searching for an alternate peer.		Warning
Call from peer rejected due to capacity	A call from a peer has been rejected because the gateway does not have enough resources available.		Warning
Call to peer rejected by all listed peers	A call to a peer has been rejected by all listed peers.		Major
Call to peer failed - peer list empty	A call to a peer has failed because the peer list is empty.		Major
Incompatible sw version install	An attempt to burn a version of the gateway software onto incompatible hardware occurs.		Warning
Call from non-peer H.323 entity rejected	The gateway has rejected an incoming IP call because the source does not appear in the peer list.		Warning

Table 3-4 Cisco Unified Videoconferencing 3545 Serial Gateway SNMP Trap Event Types

Event Type	Trap is sent when ...	State	Severity
RAI status	A change in RAI status occurs.	TRUE	Warning
		FALSE	Clear
Bad video	Corrupt or empty video packets are present in the gateway. Includes the ID number of the call during which the event occurs.	TRUE	Minor
		FALSE	Clear
Power-up	The gateway has started to operate.		Information
Power-down	The gateway is shutting down.		Information
Gatekeeper registration state change	A change occurs in the registration status of the gateway.	TRUE	Clear
		FALSE	Minor
Loss of Ethernet	The network returns after going down. Indicates the time at which the network was restored.	TRUE	Critical
		FALSE	Clear

Table 3-4 Cisco Unified Videoconferencing 3545 Serial Gateway SNMP Trap Event Types

Event Type	Trap is sent when ...	State	Severity
Max resource meter	A call could not be established because of a lack of one of the following resources—CPU, audio transcoder, DTMF detector or T.120 resources.		Warning
Network problem	A problem occurs on the network.	TRUE	Major
		FALSE	Clear
Card extract/Hot Swap	A card has been removed from the Cisco chassis under power or inserted into the chassis under power, or the when the gateway enters maintenance mode.	TRUE	Critical
		FALSE	Clear
Abnormal disconnect	A call has disconnected for a reason other than normal, busy or no answer.		Warning
Corrupt IVR messages on host	Corrupt IVR files are present in the gateway.		Warning
Corrupt WEB data	Corrupt web files are present in the gateway.		Major
Call to peer rejected - trying alternate	A call to a peer has been rejected and the gateway is searching for an alternate peer.		Warning
Call from peer rejected due to capacity	A call from a peer has been rejected because the gateway does not have enough resources available.		Warning
Call to peer rejected by all listed peers	A call to a peer has been rejected by all listed peers.		Major
Call to peer failed - peer list empty	A call to a peer has failed because the peer list is empty.		Major
Incompatible sw version install	An attempt to burn a version of the gateway software onto incompatible hardware occurs.		Warning
Call from non-peer H.323 entity rejected	The gateway has rejected an incoming IP call because the source does not appear in the peer list.		Warning
Call is out of synchronization	There is a loss of synchronization for data coming from the serial side (relevant only when the Signaling protocol field is set to Manual Control in the Physical Interface section of the Port tab).		Warning
Cables mismatch	A serial cable is not appropriate for the configured serial port settings.		Warning

Trap Severity Enumeration

Table 3-5 describes the proprietary Cisco gateway SNMP trap severity enumerations.

Table 3-5 Proprietary Cisco Gateway SNMP Trap Severity Enumerations

Trap Severity	Enumeration	Description
Cleared	0	One or more previously reported alarms have been cleared.
Information	1	Notification of a non-erroneous event.
Critical	2	A service-affecting event has occurred and immediate corrective action is required.
Major	3	A service-affecting event has occurred and urgent corrective action is required.
Minor	4	A non-service-affecting event has occurred and corrective action is required to prevent the condition becoming more serious.
Warning	5	A potential or impending service-affecting event has been detected, but no significant affects have been felt yet. Action should be taken to further diagnose and correct the problem to prevent the condition becoming more serious.

Configuring Gateway Resources for Calls

Note The Resources section is available in Cisco Unified Videoconferencing 3545 PRI Gateway only.

In the Resources section of the Settings tab, you can reserve gateway resources for T.120 enabled calls and for audio transcoded video calls. This section also displays the total number of calls that the gateway supports at specified bandwidths.

The gateway provides full end-to-end T.120 data collaboration sessions, provided that all terminals support the T.120 standard in their conferencing applications. In video calls with data transfer, the gateway accepts whatever bandwidth the ISDN connection defines for the data and dynamically adjusts the outgoing bandwidth used for data by using the MLP, HMLP and VarMLP formats.

You can also configure the gateway to prioritize the transcoding, giving preference to a particular codec that is applied to calls, thus optimizing the resource allocation utilized by each call.

The gateway supports up to 30 video calls on two B channels. If transcoding or T.120 capabilities are required, the gateway has to reserve resources for these. The gateway can differentiate between those calls that support T.120 and those that do not. When receiving calls, the gateway can check whether you are reserving resources for transcoding or for T.120 capabilities.

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 **Resources** button.

Step 4 In the Maximum number of T.120 calls field, enter the number of T.120 enabled calls that you want to reserve gateway resources for. The maximum number is 18.

Step 5 In the Maximum number of video calls with audio transcoding field, enter the number of audio transcoded video calls you want to reserve gateway resources for. The maximum number is 20.

Note The term *audio transcoded video calls* refers to the process whereby an audio stream in a multimedia call is transcoded from one codec type to another.

Step 6 In the Total call capacity: ***n*** calls of ***n*** Kbps field, choose a bandwidth.

Step 7 Click **Update total call capacity**.

The number of calls that the gateway can support at that bandwidth automatically appears.

Configuring Gateway Encryption

The gateway supports H.235-compliant AES 128 encryption for calls over IP networks, and H.233 and H.234-compliant AES 128 encryption for calls over ISDN networks.

Note (PRI gateways only) An encrypted call uses double the resources of a regular call for all bandwidth rates. Gateway capacity when encryption is supported is therefore half of regular gateway capacity, rounded up to the nearest whole call.

In the Security section of the Settings tab, you can configure gateway encryption settings.

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 **Security** button.

Step 4 In the Encryption mode field, choose one of the following settings:

- No Encryption (default)—Encryption support is disabled.
- Transparent—The gateway implements pass-through of the encryption capabilities from side to side and does not separately negotiate capabilities with each side of the call. This option ensures consistent encryption status of all call legs—all legs are either encrypted, or all legs are non-encrypted.
- Independent—The gateway negotiates encryption settings separately with each side of the call. This option enables you to define a separate connection mode (IP or ISDN, or IP or Serial) for each leg independently.

Step 5 If you selected Independent at step 4, you need to assign a mode of operation to each call leg, as follows:

In the ISDN (H.320) Mode and IP (H.323) Mode or Serial (H.320) Mode fields, choose one of the following settings:

- No Encryption—Encryption support is disabled.
- Best Effort—The gateway implements a “best effort” encryption algorithm. If an endpoint supports encryption, it connects in an encrypted way. If not, it connects without encryption.
- Encryption Required—The gateway connects only AES 128 encrypted calls.

Step 6 Click **Upload**.

Viewing Call Information

The Calls tab displays a list of the calls currently defined in the gateway and the basic details of each call. The Calls tab displays the following information in table format:

- Call ID—Displays the call identifier.
- Source Party Number—Displays the alias that identifies the source endpoint of the call.
- Destination Party Number—Displays the alias that identifies the destination endpoint of the call.
- Start Time—Displays the time at which the call began.
- Total Call Bandwidth—Displays the total bandwidth (in Kbps) used for this call on both sides.
- Encryption—Indicates the level of encryption currently in use for the specified participant: best effort, encryption required, or strong encryption required.
- Total—Field indicates the total number of calls currently defined in the gateway.

The following topics discuss the tasks you can perform in this tab:

- Refreshing Call Information, page 3-17
- Viewing Call Details, page 3-18
- Disconnecting Calls, page 3-19

Refreshing Call Information

You can configure the gateway interface to refresh information that appears in the Calls tab every ten seconds.

Procedure

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

Step 2 In the Calls tab, select the **Auto Refresh** check box.

Viewing Call Details

In the Calls tab, you can view detailed information for each call currently defined in the gateway.

Procedure

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

Step 2 In the Calls tab, select a call and click **Details**.

The Call Details window appears. Table 3-6 explains the information that this window provides.

Table 3-6 Call Details Window Fields

Field	Description
Start	Displays the time at which the call began.
Duration	Displays the length of time that the call has been in progress.
Bandwidth (Kbps)	Displays the total bandwidth (in Kbps) used for this call on both sides.
Source	
Source	Indicates whether the source endpoint of the call is located on an ISDN (or serial) or IP network.
Number	Displays the alias that identifies the source endpoint of the call.
B channels (not available in Cisco Unified Videoconferencing 35 45 Serial Gateway)	Displays the B channels currently in use for this call.
Resync B channels (not available in Cisco Unified Videoconferencing 35 45 Serial Gateway)	In mid-call, you can click this button to resynchronize B channels in cases of poor call quality. Use this option with extreme caution. Resynchronizing B channels can cause a call to disconnect.
Audio	Displays the audio transcoding protocol and the bandwidth of the voice calls in both directions between the source endpoint and the gateway.
Video	Displays the video transcoding protocol, the frame format, and the bandwidth of the video calls in both directions between the source endpoint and the gateway. **Note** The Video 2 stream is active when dual video streams for a single call are in use.
Data	Displays the bandwidth of the data calls in both directions between the source endpoint and the gateway.
Gateway	
Transcoded	Indicates that a call is transcoded.
Destination	
Destination	Indicates whether the destination endpoint of the call is located on an ISDN (or serial) or IP network.
Number	Displays the alias that identifies the destination endpoint of the call.

Table 3-6 Call Details Window Fields (continued)

Field	Description
Name	Displays the name that identifies the destination endpoint of the call.
IP	Displays the IP address of the destination endpoint of the call.
Packet Loss (%)	Displays the rate of packet loss in communication from the IP side of the call to the gateway, regardless of whether the source endpoint is located on an ISDN (or serial) or IP network.
Encryption	Indicates the encryption algorithm in use for the call (if any).
Audio	Displays the audio transcoding protocol and the bandwidth of the voice calls in both directions between the gateway and the destination endpoint.
Video	Displays the video transcoding protocol, the frame format, and the bandwidth of the video calls in both directions between the gateway and the destination endpoint. **Note** The Video 2 stream is active when dual video streams for a single call are in use.
Data	Displays the bandwidth of the data calls in both directions between the gateway and the destination endpoint.

Disconnecting Calls

In the Calls tab, you can disconnect a currently active call or disconnect all active calls.

Procedure

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

Step 2 In the Calls tab, select a call and click **Disconnect**, or to disconnect all calls, click **Disconnect All Calls**.

Viewing Gateway Alarm Events

In the Event Log tab, you can view a list of reported alarm events. The Event Log tab displays the following information:

- Event ID—Displays the identifier for the specified alarm event.
- Type—Displays the type of event.
- Time—Displays the time at which the reported event occurred.
- Severity—Displays the severity of the reported event.
- Message—Displays the error message used to report the event.
- Total—Displays the total number of reported alarm events.
- Clear All—Click to clear all events from the Event Log tab.

See Table 3-3 for a list of PRI gateway SNMP events. See Table 3-4 for a list of serial gateway SNMP events.

Viewing Gateway Statistics

In the Statistics tab, you can view system-specific information such as call traces and debugging details. The Statistics tab displays the following:

- Gateway start-up counter—Displays the number of times that the gateway has reset.
- Details button—Click to display the Details window, which lists the last three reasons for gateway power failure.
- ISDN LOF event counter (PRI gateways only)—Displays the total number of ISDN Loss of Frame (LoF) errors recorded on both gateway PRI ports.
- CRC error/event counter on ISDN (PRI gateways only)—Displays the total number of CRC errors on the ISDN network recorded on both gateway PRI ports.
- ICMP-in-message counter—Displays the number of Internet Control Message Protocol (ICMP) packets received.
- UDP-in-datagram counter—Displays the number of User Datagram Protocol (UDP) packets received.
- Packet loss counter—Displays the number of lost packets.
- Packet late counter—Displays the number of late packets.
- (PRI gateways only) Accumulated time of B channel usage—Displays the total B channel usage (in minutes).
- Counter reset time—Displays the last time at which the counters were reset.
- Reset Counters button—Click to reset all counters to zero.

Configuring Gateway Maintenance Tasks

In the Maintenance tab, you can enter maintenance mode. In maintenance mode, you can perform maintenance work on the gateway, such as upgrading software. In maintenance mode, the gateway cannot accept new calls. You can disconnect all calls currently active in the gateway, or wait for them to disconnect. In maintenance mode, you can only modify the following configuration settings:

- Services
- Fractional B channel status
- Gatekeeper IP connectivity
- Resource allocation
- IVR

To enter maintenance mode, click **Enter Maintenance Mode**. To exit maintenance mode, click **Exit Maintenance Mode**.

Saving Configuration Settings

You can save Cisco Unified Videoconferencing 3545 Gateway configuration settings to a file and then export this file to a storage device on your network. You can use the saved configuration file to restore the settings to the current Cisco Unified Videoconferencing 3545 Gateway unit or to configure a similar Cisco Unified Videoconferencing 3545 Gateway unit.

An exported configuration file saves most of the current Board section settings and all of the current Gateway section settings.

Note You cannot save configuration settings in the System category.

You must use the Export button on the toolbar to save the configuration settings to a file. The Export button appears only when Gateway section settings are activated. When you save a configuration file, the current Board section settings are saved in the file. If you want to change these settings for export, click **Upload** on the toolbar to save these settings to configuration memory prior to saving the configuration file.

Procedure

Step 1 In the gateway interface, on the sidebar, click **Board**.

Step 2 Make sure that the settings in the Basics, Addressing, Web and Users tabs are correct.

Note Date parameters are not saved to the configuration file.

Step 3 Click **Upload** to save these settings.

Step 4 On the sidebar, click **Gateway**.

Step 5 Make sure that the settings in the Status, Settings, PRI or Serial Ports, Calls, Event Log and Statistics tabs are correct.

Step 6 Click **Upload** to save these settings.

Step 7 On the toolbar, click **Export**.

Note A dialog box appears indicating that you are navigating away from the page without saving the changes. Select the option to continue.

The File Download dialog box appears.

Step 8 Save the configuration settings file to your chosen location. The file extension *.ini* is automatically appended to the file name.

Importing Configuration Files

You can import the settings of a saved Cisco Unified Videoconferencing 3545 Gateway unit configuration file from a storage device on your network. You can use the saved configuration file to restore the settings to the current Cisco Unified Videoconferencing 3545 Gateway unit or to configure another Cisco Unified Videoconferencing 3545 Gateway unit.

Procedure

Step 1 In the gateway interface, on the sidebar, click **Gateway**.

Step 2 On the toolbar, click **Import**.

Step 3 Click **Browse** on the Import a Configuration Page.

Step 4 Navigate to and select the configuration file you want to import.

Note The file must have an *.ini* extension.

Step 5 Click **Open**.

Step 6 Click **Import**.

The file appears in the gateway category window, and the Upload button is active.

Note You can open and change settings in any of the gateway category options without losing the original settings in the configuration file. However, you must click **Upload** on the toolbar to retain these setting before selecting another category.

Step 7 Click **Upload** to save the settings in configuration memory.

Note Uploading the file resets the device.