SCOPIA 400/1000 Gateway
version 5.6

User Guide

RADVISION
Delivering the Visual Experience

NOTICE

For further information contact RADVISION or your local distributor or reseller.

SCOPIA Gateway version 5.6, May 2008

Publication 10

http://www.radvision.com

CONTENTS

2 *Installing the SCOPIA Gateway*

3 *Configuring the SCOPIA Gateway*

About This Manual

The SCOPIA 400/1000 Gateway User Guide describes how to install, configure and monitor SCOPIA Gateway blades.

Related Documentation

The Gateway documentation set is available on the RADVISION Utilities and Documentation CD-ROM and includes manuals and online helps. The manuals are available in PDF format.

Note You require Adobe Acrobat Reader version 5.0 or later to open the PDF files. You can download Acrobat Reader free of charge from www.adobe.com.

Note For hardware-specific information relating to the SCOPIA Gateway, see the appropriate Platform Guide for the platform on which your Gateway is operating.

Conventions Used in this Manual

The SCOPIA Gateway blade is sometimes referred to as “the Gateway” throughout this manual.

Feedback

The team at RADVISION constantly endeavors to provide accurate and informative documentation. If you have comments or suggestions regarding improvements to future publications, we would value your feedback.

Please send your comments to doc_comments@radvision.com.

We thank you for your contribution.

1

FUNCTIONALITY

This section introduces the SCOPIA Gateway and includes the following topics:

- About SCOPIA Gateway Products
- About Gateway Features
- About SCOPIA Gateway Applications and Topologies
- About SCOPIA Gateway Functionality

ABOUT SCOPIA GATEWAY PRODUCTS

SCOPIA Gateway series consists of the following products:

- Gateway P20 SP (see About the Gateway P20 SP)
- Gateway S40 SP (see About the Gateway S40 SP)

ABOUT THE GATEWAY P20 SP

The Gateway P20 SP enables audio, video, and data communication between H.320 endpoints that connect through ISDN, and H.323 endpoints that connect through a packet-based network. For voice over IP, the Gateway enables PSTN voice callers to connect from the ISDN network to IP voice callers. The Gateway P20 SP supports two PRI ISDN ports.

ABOUT THE GATEWAY S40 SP

The Gateway S40 SP supports multimedia conferencing over IP by translating between H.323 and serial protocols. With the help of a V.35 Adtran Imux, the Gateway can also translate between H.323 and H.320 protocols.

The Gateway offers a serial leg for multimedia conferencing over IP by providing an interface for legacy endpoints with serial interfaces, encryption/decryption devices, satellite networks and leased line services.

About Gateway Features

Table 1-1 lists the major features of the SCOPIA Gateway.

Table 1-1 *Gateway Feature Summary*

Feature	Description
Interoperability	The Gateway provides a high degree of interoperability with other H.323 compliant gateways, gatekeepers, terminals, proxy, and Multipoint Control Unit (MCU) products by being based on the H.320 standard and H.323 protocol stack.
Web-based management	The Gateway features the Gateway interface. This is a web interface used to configure and monitor the Gateway. You can view and modify all aspects of the Gateway configuration from a remote location using a Java-enabled web browser.
SNMP management	The Gateway features Simple Network Management Protocol (SNMP) management that supports all aspects of monitoring, diagnostics, configuration, and trapping.
Diagnostics	The Gateway features front and rear panel LED indicators that display status for the unit. You can also access remote diagnostics of the unit through the Gateway interface, Telnet, SNMP, or a serial port.
Network load balancing	The Gateway supports load balancing on the network by communicating with a gatekeeper through H.323 RAI (Resource Available Indication)/RAC (Resource Available Confirmation) messages.
T.120 data collaboration	The Gateway supports data transfers in calls between ISDN and IP by using high speed T.120 in HMLP and VarMLP formats.
Quality of service (QoS)	The Gateway features configurable coding of media packets to achieve QoS routing priority on the Internet Protocol (IP) network. The Type of Service (ToS) bits of the IP datagram header can be configured for priority level.
Dial plan	The Gateway supports a simplified dial plan for outbound dialing using a single universal prefix. Using the dial plan, the Gateway automatically detects the capabilities received in the Setup message from the IP endpoint and sets the same bit rate for the ISDN (or serial interface) side of the call.

Table 1-1 *Gateway Feature Summary (continued)*

Feature	Description
Direct dialing and call routing	The Gateway dial plan supports the following direct dialing and call routing facilities: ■ Direct Inward Dialing (DID) □ Multiple Subscriber Network (MSN) □ Q.931 Sub-addressing Information Element Gateway S40 SP supports DID in DCE mode only. ■ Internal and External Interactive Voice Response (IVR) ■ TCS4 ■ Default extension
Access control	The Gateway features password-controlled access to the Gateway interface. Up to ten different administrator access profiles can be defined for the Gateway.
DTMF translation	The Gateway supports translation between in-band Dual Tone Multi-Frequency (DTMF) signals (on the ISDN side) and out-of-band H.245 messages (on the IP side). DTMF translation occurs for voice and video calls.
Dual video	The Gateway supports H.239 standard-based dual video and TANDBERG DuoVideo™ technology. Dual video streams enable a screen to carry video images from one source while simultaneously displaying images from a second source.
Hot swap	The Gateway features hot swap functionality that you can use to remove and replace Gateway blades under power.
Conceal caller ID	The Gateway supports a conceal caller ID feature that instructs the gatekeeper to conceal the identity of the calling endpoint on the IP or ISDN network, whether the presentation restricted feature is enabled or not.
H.323 fast start	The Gateway H.323 fast start feature enables endpoints to join a voice conference in the Gateway more quickly.
ISDN rollover (available in Gateway P20 SP only)	The Gateway features ISDN rollover. In this feature, the Gateway sends a “busy out” channel request to the PSTN switch when the current PRI connection is left with less than a predefined number of available B channels. The PSTN switch “rolls over” to the next available gateway.
Network Specific Facility (available in Gateway P20 SP only)	The Gateway provides support for Network Specific Facility Information Elements (NSF IEs) which enable system administrators to specify to service providers the equipment, service, or network through which they want a call routed.

Table 1-1 *Gateway Feature Summary (continued)*

Feature	Description
ISDN connection failure	The Gateway responds to ISDN connection failure events, by unregistering from its gatekeeper. 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 connection is restored.
Downspeeding	The Gateway features downspeeding functionality. In the downspeeding feature, the Gateway attempts to reconnect a disconnected video call either at a lower bandwidth or as a voice call. Downspeeding contributes to a higher percentage of call completion on the network. The Gateway supports downspeeding at call setup and in mid-call.
Multiple trap server support	The Gateway supports up to three SNMP trap servers.
H.239 support	The Gateway supports the H.239 protocol in ISDN-to-IP calls and in IP-to-ISDN calls.
Encryption support	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.
H.243 Conference Control support	The Gateway supports the H.243 protocol in ISDN-to-IP calls and in IP-to-ISDN calls. The Gateway identifies the protocol version that an IP endpoint uses and sends H.239 capabilities only to those endpoints working with protocol version 4.0 or later.
Peer-to-peer connectivity	The Gateway supports connectivity to the IP network through a gatekeeper, or directly to a peer device such as Cisco Unified Communications Manager.
IP network connections	The Gateway has one 10/100Base-T Ethernet IP port (on the front panel) and connects to an IP segment through a direct connection to a network switch.

Table 1-2 lists features for specific RADVISION Gateways.

Table 1-2 *Gateway Feature Specifics*

Feature	Gateway P20 SP	Gateway S40 SP
Supported ports	2 PRI ISDN ports	4 serial ports
Supported video conferencing protocols	H.320, H.323 (using RADVISION Stack v4.0)	

Table 1-2 *Gateway Feature Specifics (continued)*

Feature	Gateway P20 SP	Gateway S40 SP
Supported audio codecs	The term *audio transcoded video calls* refers to the process whereby an *audio* stream in a multimedia call can be transcoded from one codec type to another. Basic and advanced audio coding supported codecs: G.711, G.722, G.722.1, G.723.1, G.728	
Audio Transcoding	G.711 (ISDN) < > G.723.1 (IP) for up to 60 voice channels. G.711 (IP) < > G.728 (ISDN) for up to 20 audio transcoded video channels. The Gateway automatically performs A-Law G.711-to-µ-Law G.711 translation between the IP and ISDN sides if needed. **Note** When your RADVISION unit includes both a Gateway and an MCU, G.728 transcoding is supported on the MCU only.	Transcoding for the 4 supported multimedia calls.
Supported video protocols	H.261, H.263, H.263+ (Annexes F, J and N), H.263++ (Annex W), H.264	
Supported video resolutions	VGA, XGA, SVGA, SIF, 4SIF, CIF, QCIF, 4CIF, 16CIF	
Supported bandwidths (Kbps)	56, 64, 112, 128, 168, 192, 224, 256, 280, 320, 336, 384, 448, 512, 672, 768, 1288, 1472, 1680 and 1920 **Note** Bandwidth rates of 256 Kbps and up support the G.722 audio codec.	56, 64, 112, 128, 168, 192, 224, 256, 280, 320, 336, 384, 448, 512, 672, 768, 1288, 1472 and 1920

Table 1-2 *Gateway Feature Specifics (continued)*

Feature	Gateway P20 SP	Gateway S40 SP
Call handling capabilities	**For 1 x PRI T1 line:** 23 ports (voice) 23 ports 1B (video and data) 11 ports 2B (video and data) 3 ports 6B (video and data) **For 2 x PRI T1 lines:** 46 ports (voice) 30 ports 1B (video and data) 23 ports 2B (video and data) 7 ports 6B (video and data) **For 1 x PRI E1 line:** 30 ports (voice) 30 ports 1B (video and data) 15 ports 2B (video and data) 5 ports 6B (video and data) **For 2 x PRI E1 lines:** 60 ports (voice) 30 ports 1B/2B (video and data) 10 ports 6B (video and data)	1 call per serial connection, up to a maximum bandwidth of 1920 Kbps per port.
Line quality	Supports line echo cancellation, H.323 Fast Start and DTMF detection for voice and video calls.	Supports line echo cancellation and DTMF detection for voice calls.
IP network connection	I10/100Base-T Ethernet IP UTP connection (on the front panel).	
Serial control port (DB-9) connection	RS-232 DTE 9-pin D-type connection on front panel for connection to a PC terminal or an external modem.	
Supported media protocols	N/A	V.35, RS-449, EIA-530, EIA-530A
Supported signaling protocols	5ESS and 4ESS, DMS100, National ISDN, Euro-ISDN, VN6 Dialing (France), NTT (Japan), Hong Kong Dialing (Hong Kong), Support for Taiwan PRI system.	RS-366, Manual Control, Data Triggered.
Supported media + signaling combinations	N/A	RS-449 + RS-366 V.35 + RS-366 EIA-530 + RS-366 EIA-530A + RS-366

Table 1-2 *Gateway Feature Specifics (continued)*

Feature	Gateway P20 SP	Gateway S40 SP
Encryption interoperability	N/A	KIV-7, KG-194
PRI interface	Configurable E1/T1 PRI network interface. Support for fractional E1/T1 channel selection. Configurable as terminal side (TE) or network side (NT) device. Configurable Long Haul PRI module (supported in Japan only).	N/A
Switch information	Numbering Plan Identifier (NPI), Type of Number (TON) and Network Specific Facility (NSF) information elements are configurable per PRI port.	N/A
Bonding calls	Internal Imux providing calls at 128 Kbps (2B) up to full PRI of 1472 Kbps (23B) for T1 and up to full PRI of 1920 Kbps (30B) for E1 using bonding mode 1. Parallel dialing for bonded calls.	N/A
Internal IVR capacity	30 simultaneous calls	4 simultaneous calls

About SCOPIA Gateway Applications and Topologies

The SCOPIA Gateway supports multimedia conferencing by translating between H.323 and H.320 protocols. Examples of network applications that use the Gateway include:

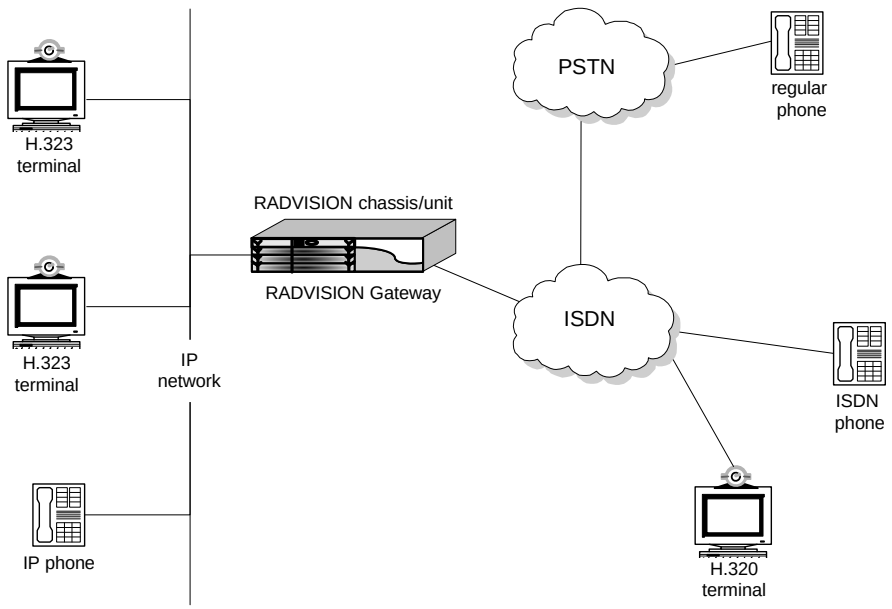
- Multimedia conferencing (see About Multimedia Conferencing on page 8)
- Point-to-Point conferencing (see About Point-to-Point Conferencing on page 9)
- Multipoint conferencing (see About Multipoint Conferencing on page 9)
- IP networking (see About Gateway IP Network Connections on page 10)
- ISDN networking (see About Gateway ISDN Network Connections on page 10)

- Encrypted videoconferencing (see About Gateway Encryption on page 12)
- Conferencing over leased lines (see About Conferencing via Leased Lines on page 13)
- Communicating with legacy MCU equipment (see About IP-to-Legacy MCU Conferencing on page 14)

About Multimedia Conferencing

The RADVISION PRI Gateway enables H.323 endpoints on the IP network to communicate with an H.320 terminal, an ISDN phone, or a regular phone on a circuit-switched public network without having to connect directly to these networks. The Gateway allows all IP network terminals to support video conferences without connecting every desktop computer to an ISDN line (see Figure 1-1).

Figure 1-1 *Multimedia Conferencing through the Gateway*



Typical multimedia conferencing applications include:

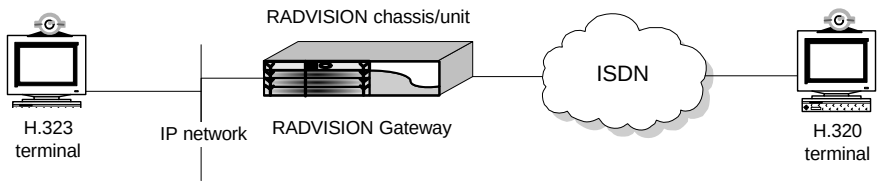
- Business video conferencing
- Distance learning

- Telemedicine
- Video-enabled call centers
- Telecommuting

About Point-to-Point Conferencing

The RADVISION PRI Gateway enables direct video, voice, and data communication between an H.320 (ISDN) terminal and H.323 (IP) terminals at bandwidths of up to 1472 Kbps (23B bonding for T1) and up to 1920 Kbps (30B bonding for E1) (see Figure 1-2).

Figure 1-2 *Point-to-Point Conferencing through the Gateway*

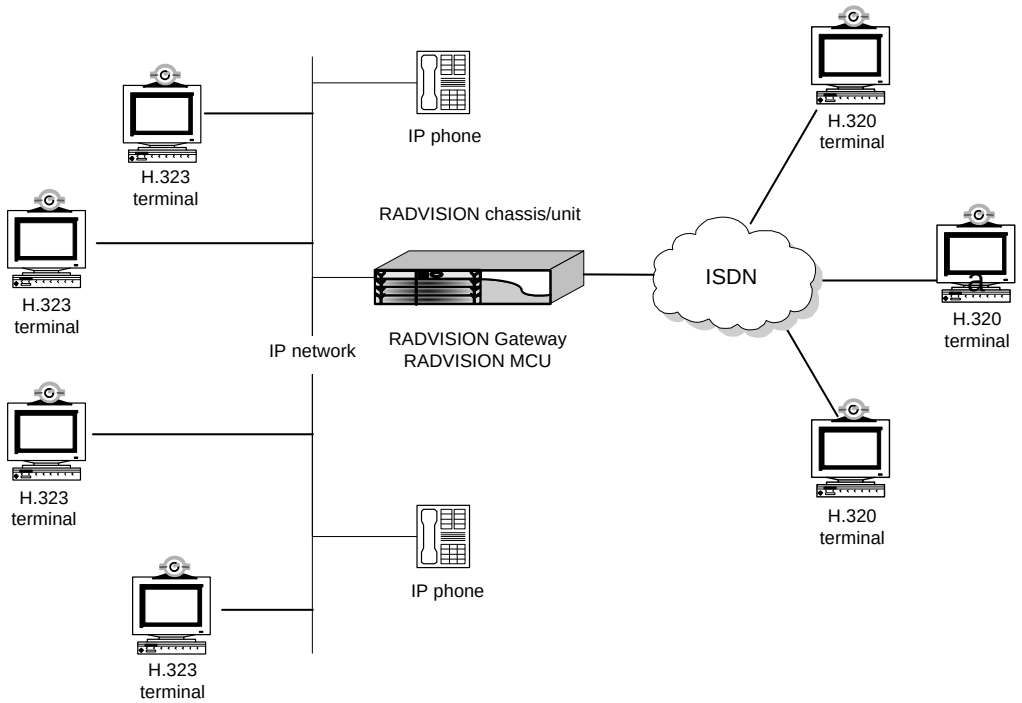


About Multipoint Conferencing

Together with the RADVISION MCU, the RADVISION PRI Gateway enables H.320 ISDN terminals to participate in a mixed ISDN-IP multipoint multimedia conference with IP network endpoints (see Figure 1-3).

For example, when an H.320 ISDN terminal wants to participate in a multipoint conference with H.323 IP endpoints, the H.320 ISDN terminal can either join the multipoint conference by dialing to the Gateway, or be invited into the conference by one of the participating IP endpoints. In either case, the Gateway connects the ISDN terminal to the RADVISION MCU, enabling it to participate in the multipoint conference.

Figure 1-3 *Mixed ISDN-IP Multipoint Multimedia Conference*



About Gateway IP Network Connections

The RADVISION PRI Gateway features one 10/100Base-T Ethernet IP port (on the front panel) and connects to an IP segment through a direct connection to a network switch.

About Gateway ISDN Network Connections

The RADVISION PRI Gateway features configurable E1/T1 PRI ISDN connections. When configured as an E1 connection, each port provides 30 B channels and one D signaling channel. When configured as a T1 connection, each port provides 23 B channels and one D signaling channel. The type of line available depends on your local ISDN provider. You configure the Gateway PRI port to an E1 or T1 interface accordingly. In addition, you can choose to activate only specific channels by using fractional channel selection.

PRI GATEWAYS

You can connect the PRI Gateway directly to a PRI line provided by your local ISDN provider (as shown in Figure 1-4), or to a local private branch exchange (PBX) that provides the PRI connection (as shown in Figure 1-5).

Figure 1-4 *Connecting the PRI Gateway Directly to a Central Office Switch*

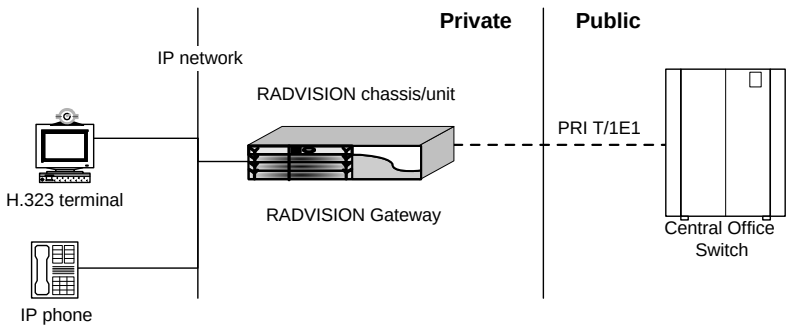
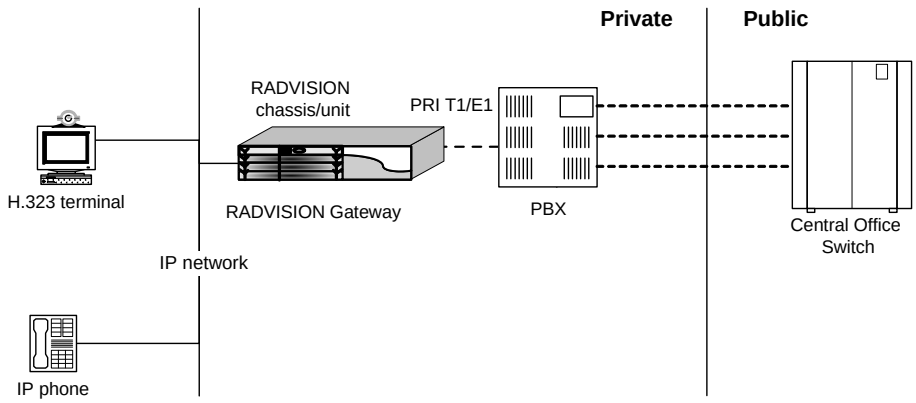


Figure 1-5 *Connecting the PRI Gateway to a PBX that Provides a PRI Line*



About Gateway Encryption

The Serial Gateway enables encrypted videoconferencing between H.323 endpoints on the IP network and endpoints on remote sites by connecting to external encryption/decryption devices via serial interfaces (as shown in Figure 1-6). The Serial Gateway also enables encrypted videoconferencing via satellite with or without RS-366 signaling (as shown in Figure 1-7).

Figure 1-6 *Encrypted Videoconferencing*

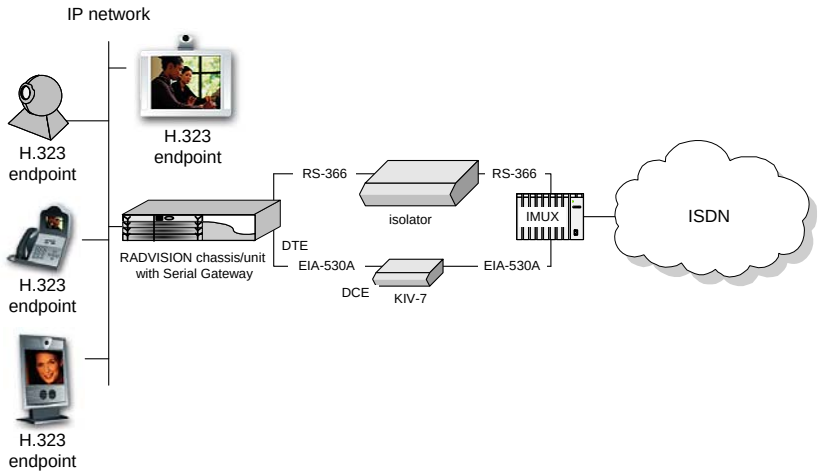
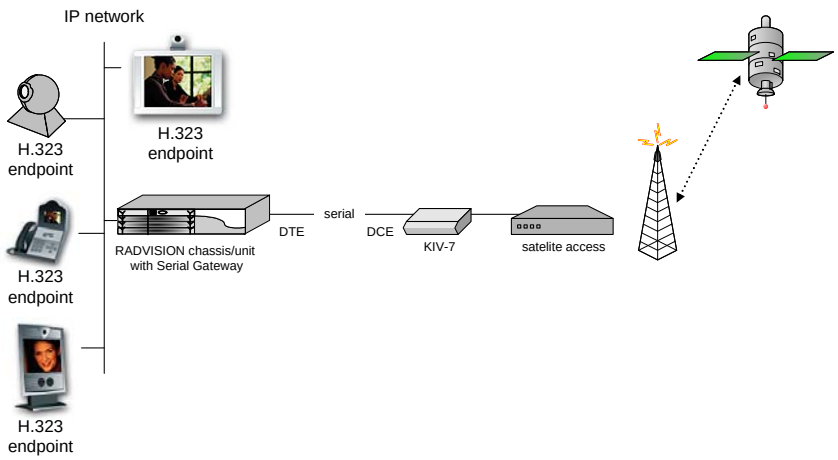


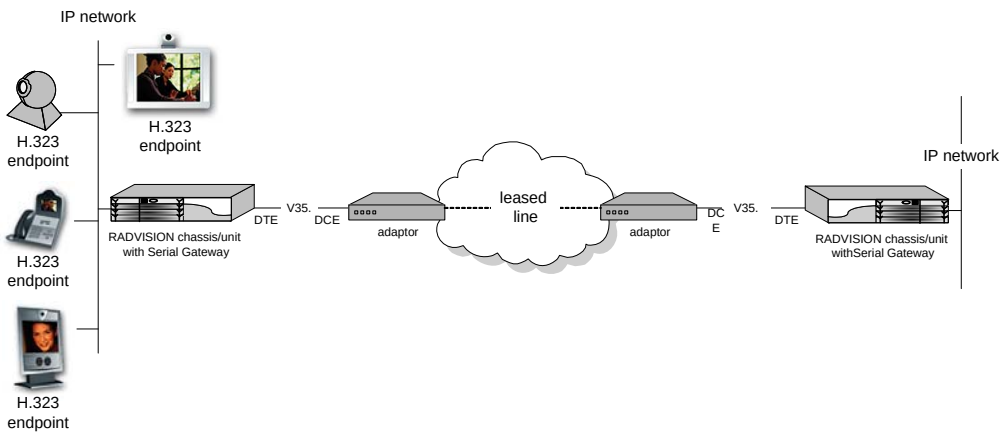
Figure 1-7 *Encrypted Videoconferencing via Satellite*



About Conferencing via Leased Lines

The Serial Gateway enables conferencing between H.323 endpoints on IP networks connected via a leased line (as shown in Figure 1-8).

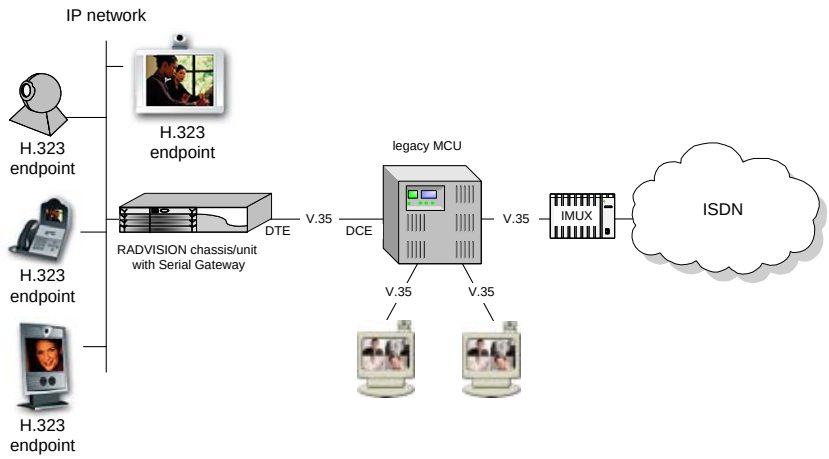
Figure 1-8 *Conferencing via Leased Lines*



About IP-to-Legacy MCU Conferencing

The Serial Gateway provides an IP-to-serial interface for communication with legacy MCU equipment (as shown in Figure 1-9).

Figure 1-9 *IP-to-Serial Interface Communication via Legacy MCU*



About SCOPIA Gateway Functionality

This section discusses the following topics:

- About PRI Gateway Call Handling Capacity on page 14
- About Gateway Call Bandwidth Overhead on page 15
- About Peer-to-Peer Connectivity on page 16

About PRI Gateway Call Handling Capacity

Table 1-3 lists the maximum call handling capacity of the PRI Gateway for different types of calls.

Table 1-3 *PRI Gateway Call Handling Capacity*

Call Type	Maximum Number of Calls Using 1 x E1 PRI Line	Maximum Number of Calls Using 1 X T1 PRI Line	Maximum Number of Calls Using 2 x E1 PRI Lines	Maximum Number of Calls Using 2 x T1 PRI Lines
voice (64 Kbps)	30	23	60	46
2B video (128 Kbps)	15	11	30	23
6B video (384 Kbps)	5	3	10	7

Table 1-3 *PRI Gateway Call Handling Capacity (continued)*

Call Type	Maximum Number of Calls Using 1 x E1 PRI Line	Maximum Number of Calls Using 1 X T1 PRI Line	Maximum Number of Calls Using 2 x E1 PRI Lines	Maximum Number of Calls Using 2 x T1 PRI Lines
12B video (768 Kbps)	2	1	5	3

Note Enabling ISDN-to-IP DTMF detection in the PRI Gateway for video calls reduces the number of supported calls by half.

About Gateway Call Bandwidth Overhead

According to the H.320 standard, the available bandwidth allocated to a call at any given bit rate will always be slightly less than the stated maximum for the following reasons:

- All stated maximum call bandwidths include provision for control, audio, video, and data traffic.
- Video traffic on the ISDN side contains additional bits for error correction purposes which also consume bandwidth. Video traffic on the IP side does not include this additional load.
- Opening an audio channel further reduces the bandwidth available to the video traffic.

For example, a call at 384 Kbps actually has only 363 Kbps available to it. Control and error correction account for the remaining 21 Kbps.

Resource Allocation across E1/T1 Lines

The Gateway can allocate bandwidth resources to calls across separate E1 or T1 connections to maximize bandwidth capacity in cases where there is not enough capacity for a call on a single E1 or T1 connection, but where sufficient capacity does exist when remaining capacity on both E1/T1 lines is combined.

For example, a Gateway using two T1 lines can support three 6B calls on each T1 line, with 320 Kbps spare capacity per line:

- Each T1 line provides 23 B channels.
- Each B channel supports 64 Kbps
- Each T1 line supports 23 x 64 = 1472 Kbps
- Each 6B call requires 6 x 64 = 384 Kbps
- Each T1 line supports 1472/384 = 3 6B calls + 320 Kbps spare

The Gateway processes an additional 6B call requiring a further 384 Kbps by taking bandwidth resources from each of the two T1 lines, both of which have 320 Kbps available. In this way, the Gateway spreads the call over both T1 lines.

About Peer-to-Peer Connectivity

The Gateway supports the following types of connectivity to the IP network

- Through a gatekeeper
- Directly to a peer device such as Cisco Unified Communications Manager without the need for a gatekeeper.

2

INSTALLING THE SCOPIA GATEWAY

This section provides information on installing, setting up and configuring the SCOPIA Gateway in the SCOPIA 400 chassis, and includes the following topics:

PHYSICAL DESCRIPTION

This section provides a physical description of the Gateway modules and their corresponding RTMs.

GATEWAY MODULE

The Gateway module has a 10/100BaseT Ethernet port on the front panel that uses an RJ-45 connector to connect to the network. There is an asynchronous, 9-pin serial port that you can use with a hyperterminal program to configure and monitor the module.

Figure 2-1 shows the front panel components of the Gateway module. Table 2-1 describes these components.

Figure 2-1 *Gateway Front Panel*

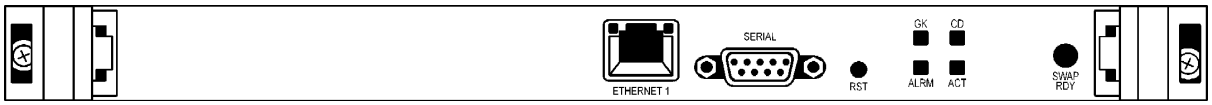


Table 2-1 *Front Panel Components*

Component	Description
ETHERNET connector	An RJ-45 connector that provides the primary Ethernet connection for the IP network port.
SERIAL connector	A DB-9 connector that allows you to connect a PC terminal for local configuration.
RST button	Allows you to reset the Gateway manually.
GK LED	Lights green when the Gateway is registered with a gatekeeper.
CD LED	Lights green when at least one Gateway port connection is online.
ACT LED	Lights green to indicate that there are active calls in the Gateway.
ALRM LED	Lights green to indicate that an error has occurred and the Gateway requires resetting.

Table 2-1 Front Panel Components (continued)

Component	Description
ETHERNET LEDs	The top part of the Ethernet connector contains two LED indicators. The left-hand LED lights green when the local IP network link is active. The right-hand LED lights green if the connection speed is 100 Mbps, and is off when the connection speed is 10 Mbps.
SWAP RDY LED	Hot Swap indication. Lights blue when the latches of a board are unlocked and it is safe to remove the board from the chassis. Goes off when the board is completely detached.

GATEWAY P20 SP RTM

The Rear Transition Module (RTM) provides the PRI line connections for the Gateway P20 SP.

Figure 2-2 shows the RTM panel components of the Gateway P20 SP module. Table 2-2 describes these components.

Figure 2-2 PRI Gateway: Rear Transition Module

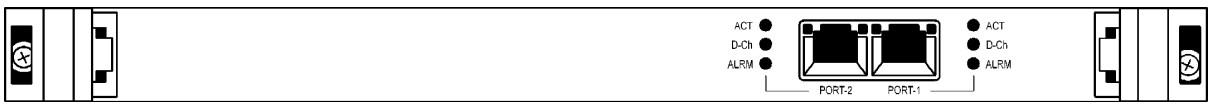


Table 2-2 PRI Gateway Rear Transition Module Components

Component	Description
ACT LEDs	Lights green to indicate that there are active calls in the Gateway.
D-Ch LEDs	Lights green to indicate that the PRI line is enabled and a carrier signal is detected.
ALRM LEDs	Displays alarm events for the PRI line. ■ YELLOW —Lights yellow when there is a loss of frame alignment at the remote side. ■ ORANGE—Lights orange when there is a loss of frame alignment in the Gateway.

Table 2-2 PRI Gateway Rear Transition Module Components (continued)

Component	Description
PRI LINE connectors	RJ-45 connectors that provide the PRI line connections for the specified Gateway ISDN PRI port.

GATEWAY S40 SP RTM

The Rear Transition Module (RTM) provides the serial line connections for the Gateway S40 SP.

Figure 2-3 shows the RTM panel components of the Gateway S40 SP module. Table 2-3 describes these components.

Figure 2-3 Serial Gateway: Rear Transition Module

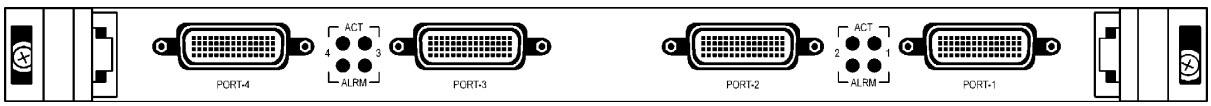


Table 2-3 Serial Rear Transition Module Components

Component	Description
PORT connectors	DB-60 connectors that provide the serial line connections for Gateway serial ports 1 to 4.
ACT and ALRM LEDs	ACT lights green to indicate that the specified serial line is currently in use. ALRM lights red to indicate an internal error related to the specified line.

PREPARING FOR INSTALLATION

This section describes the requirements for installing the RADVISION Gateway on the SCOPIA 400 platform and on the SCOPIA 1000 platform.

ON THE SCOPIA 400 PLATFORM

This section describes the requirements for installing the Gateway in the SCOPIA 400 chassis. For more information, see the SCOPIA 400 Platform Guide. The requirements are as follows:

Warning During this procedure, wear grounding wrist straps to avoid ESD damage to the blade. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

- SCOPIA 400 chassis
- Proper clearance at the sides of the unit to allow adequate ventilation, and at least 20 cm clearance at the back of the chassis to allow access to the boards and cable connections
- A PC with a serial port and terminal emulation software to assign the Gateway an IP address
- Dedicated IP address for the Gateway
- The IP address of the router the Gateway will use to communicate across the network
- The IP address of the H.323 gatekeeper with which you want the Gateway to register
- Available IP network ports on the switch for the SCOPIA 400 chassis
- A grounded AC power outlet
- A 10BaseT or 100BaseT LAN cable
- Ambient room temperature range of 32^{o} to 104^{o}F (0^{o} to 40^{o}C)
- Non-condensing relative humidity range of 5% to 85%

ON THE SCOPIA 1000 PLATFORM

This section describes the requirements for installing the Gateway in a SCOPIA 1000 chassis. For more information, see the SCOPIA 1000 Platform Guide. The requirements are as follows:

Warning This system contains board-level components that must be protected from static discharge and physical shock. Wear a wrist strap grounded through one of the system ESD ground jacks when handling system components. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

- SCOPIA 1000 chassis
- Ensure that all cover panels are in place
- Ensure that all component slots are populated with a component, filled with an air management blade (front), or covered with a blank filler panel (rear)

Warning Failure to cover open slots could cause overheating of power supplies, boards, or other components, and could damage the system.

- Proper clearance at the sides of the unit to allow adequate ventilation, and at least 20 cm clearance at the back of the chassis to allow access to the boards and cable connections
- PC with a serial port and terminal emulation software to assign the Gateway an IP address
- Dedicated IP address for the Gateway
- IP address of the router the Gateway uses to communicate across the network
- IP address of the H.323 gatekeeper with which you want the Gateway to register
- Available IP network ports on the switch for the SCOPIA 1000 chassis
- A grounded AC power outlet

- 10BaseT or 100BaseT LAN cable
- Ambient room temperature range of 41° F to 104° F (5° C to 40° C)

Note The hottest ambient temperature supported by RADVISION for the SCOPIA 1000 platform is 104° F (40° C). Any ambient temperature above 104° F (40° C) is considered a failure condition. Up to 104° F (40° C), the SCOPIA 1000 platform supports a single feed failure (leaving four power supplies operational), where the total chassis load (including the fans and positronic cable losses) does not exceed 1300W.

- Non-condensing relative humidity range of 5% to 85% (to 90% for 96 hours)

Note The SCOPIA 1000 platform also supports a severe conditions ambient temperature above 40° C, up to 55° C, with all eight power supplies operational, for 96 hours. Storage temperature -40° C to 70° C.

VERIFYING THE PACKAGE CONTENTS

Inspect the contents of the box for shipping damage. Report any damage or missing items to your distributor or reseller. Table 2-4 lists the package contents for an assembled Gateway shipped with a chassis.

Table 2-4 *Package Contents with Gateway*

Product	Contents
SCOPIA 400 chassis with Gateway	■ Gateway blade ■ Gateway Rear Transition Module ■ 2 power cables (depending on customer location) ■ Terminal cable ■ LAN cable ■ Rack mounting kit (two brackets and six screws) ■ Four rubber feet ■ SCOPIA 400/1000 Gateway User Guide (in PDF format only) ■ SCOPIA 400/1000 Gateway Quick Start ■ SCOPIA 400 Platform Guide (in PDF format only) ■ SCOPIA Gateway Release Notes ■ SCOPIA 400 Chassis Release Notes ■ RADVISION Utilities and Documentation CD-ROM containing product documentation, utilities and online help files.

Table 2-4 Package Contents with Gateway (continued)

Product	Contents
SCOPIA 1000 chassis with Gateway	■ Fully assembled 21-slot SCOPIA 1000 chassis with 18 air management blades including 18 rear filler panels, 2 Ethernet switches, 2 Intelligent Shelf Managers (ISMs) and 2 ISM RTM4820 Rear Transition Modules ■ Terminal cable ■ Terminal adapter cable (for the ISMs) ■ 2 switch terminal cables ■ 6 LAN cables (4 for switches, 2 for the ISMs) ■ SCOPIA 400/1000 Gateway User Guide (in PDF format only) ■ SCOPIA 400/1000 Gateway Quick Start ■ SCOPIA 1000 Platform Guide (in PDF format only) ■ SCOPIA Gateway Release Notes ■ SCOPIA 1000 Chassis Release Notes ■ Utilities and Documentation CD-ROM containing product documentation, utilities and online help files.

You can also order the following cables for the Gateway S40 SP:

- V.35/RS366-DTE cable
- EIA449/RS366-DTE cable
- EIA530/RS366-DTE cable
- EIA530/RS366-DTE-LOS cable
- EIA530A/RS366-DTE cable
- KIV7/RS366-DTE cable
- V.35/RS366-DCE cable
- EIA449/RS366-DCE cable
- EIA530/RS366-DCE cable

Related Topics

- Serial Gateway Cable Connections and Pin-outs on page 40

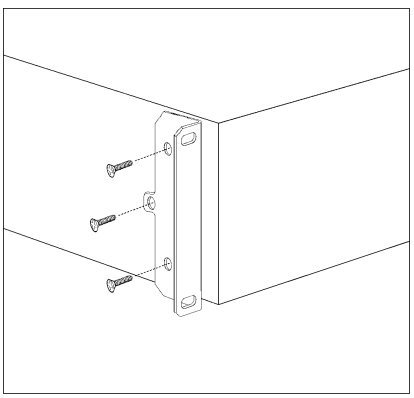
MOUNTING THE SCOPIA 400 CHASSIS IN A 19-INCH RACK

You can optionally mount the SCOPIA 400 chassis in a standard 19-inch rack. Two mounting brackets and a set of screws are included in the SCOPIA 400 chassis shipping box.

Procedure

1. Disconnect all cables including the power cables.
2. Place the SCOPIA 400 chassis right-side up on a hard flat surface, with the front panel facing you.
3. Position a mounting bracket over the mounting holes on each side of the SCOPIA 400 chassis, as shown in Figure 2-4.
4. Pass the screws through the brackets and tighten them into the screw holes on each side of the SCOPIA 400 chassis using a suitable screwdriver.

Figure 2-4 *Fitting a Bracket for Rack Mounting*



5. Insert the SCOPIA 400 chassis into the 19-inch rack.
6. Fasten the brackets to the side rails of the rack.
7. Make sure that the air vents at the sides of the SCOPIA 400 chassis are not blocked.

MOUNTING THE SCOPIA 1000 CHASSIS IN A 19-INCH RACK

This SCOPIA 1000 platform is intended for stationary mounting in a rack designed to meet the physical strength requirements of NEBS GR-63-CORE and NEBS GR 487. Be sure to mount the system in a way that ensures even weight distribution in the rack. Uneven mechanical loading can result in a hazardous condition. Secure all mounting bolts when installing the enclosure to the rack. For more information, see the SCOPIA1000 Platform Guide.

Note The SCOPIA 1000 chassis fits standard 19" EIA racks. Mounting flanges are attached to the front of the enclosure to facilitate front mounting. The flanges can be repositioned for center-mounting the enclosure.

Warning It takes more than one person to safely lift the SCOPIA 1000 chassis. Get assistance and use proper lifting techniques when moving the system. To prevent damage to the components, never use component handles or cables to lift or move the entire system.

Procedure

1. Disconnect all power sources and external connections and cables.
2. Select a position in the rack that does not interfere with other equipment and that provides safe weight distribution.
3. For efficient cooling, the area around the SCOPIA 1000 chassis intake and exhaust vents should be clear of obstructions. The intake should be away from other system exhausts. For more information, see the Cooling Subsystem chapter of the SCOPIA1000 Platform Guide.
4. Secure the mounting flanges to the front or middle of the enclosure.
5. Place the enclosure in its intended location and line up the mounting holes on the SCOPIA 1000 chassis flanges with the rack mounting holes.
6. Bolt the enclosure to the rack (rack hardware is not included).

INSTALLING THE GATEWAY

This section describes how to insert a Gateway into the SCOPIA 400 chassis and into the SCOPIA 1000 chassis.

Before You Begin

Note the following:

- The SCOPIA 400 chassis has four slots. You can install the SCOPIA Gateway in any of the slots.
- Insert the Gateway in the top slot at the front of the SCOPIA 400 chassis to view status and identification information via the **System** web user interface.
- The SCOPIA 1000 chassis has 18 payload slots. You can install the Gateway in any of slots 3-20.

The SCOPIA Gateway has two components that you must install in the chassis: the SCOPIA Gateway module and the corresponding Rear Transition Module (RTM), as indicated in Table 2-5.

Table 2-5 *Identifying RTM Boards*

Gateway	Corresponding RTM
Gateway [gw-P25/M]	Dual PRI RTM board
Gateway P20 SP	Dual PRI RTM board
Gateway S40 SP	Quad Serial RTM board

The Gateway module installs in the front of the chassis and provides ISDN or serial functionality. The RTM installs in the rear of the chassis and provides the physical interface for the ISDN or serial line. You must install these modules in corresponding slots in the chassis. That is, if you insert the Gateway module in the top slot in the front of the chassis, you must insert the RTM in the top slot in the rear of the chassis.

Warning

- During this procedure, wear grounding wrist straps to avoid ESD damage to the blade. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.
- Before opening the chassis, disconnect the telephone network cables to avoid contact with telephone network voltages.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- The telecommunications lines must be disconnected before unplugging the main power connector and/or while the housing is open.

INSTALLING THE RTM MODULE

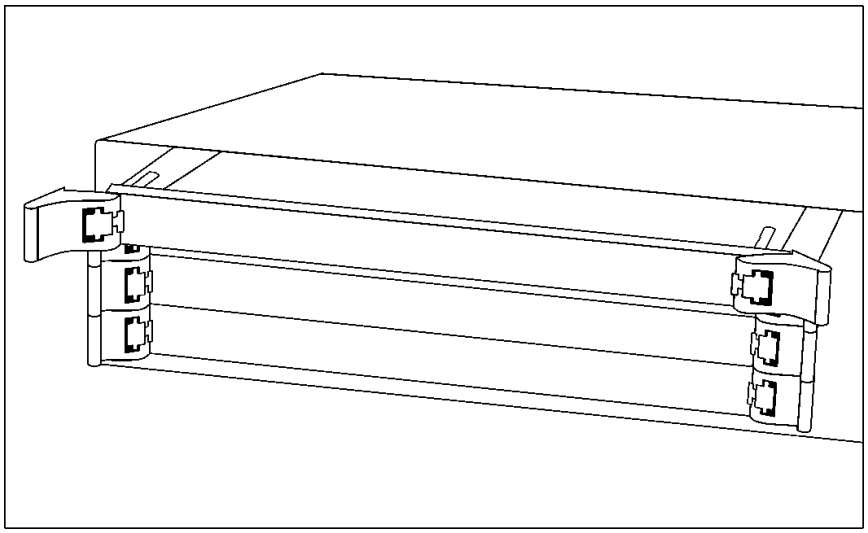
This section describes how to install the RTM module in the SCOPIA 400 chassis and in the SCOPIA 1000 chassis. The Rear Transition Module (RTM) provides the ISDN or serial line connections for the Gateway.

Warning You must install the RTM module before you install the Gateway module. Inserting an RTM module in the rear of the chassis when a Gateway module is already installed in the same position at the front of the chassis may damage the chassis.

Procedure

1. On the back of the chassis, loosen the screws of the blank panel covering the slot into which the RTM module is to be installed.
2. Remove the blank panel.
3. Remove the new RTM from the antistatic bag.
4. Press the red buttons and open the handles of the RTM module.
5. Align the edges of the RTM module with the chassis guide rails.
6. Slide the RTM module into the chassis until it stops (see Figure 2-5 for the SCOPIA 400 chassis).

Figure 2-5 *Inserting the RTM Module in the SCOPIA 400 Chassis*



7 Use even pressure to push the module further into the slot.

Caution Do not force the connection. Forcing the connection can bend or damage the pins in the connector inside the chassis.

8 Snap the handles forward to secure the RTM module in the slot.

9 Secure the RTM module screws.

Caution Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all blades, faceplates, front covers, and rear covers are in place.

INSTALLING THE GATEWAY MODULE

This section describes how to install the SCOPIA Gateway module in the SCOPIA 400 chassis and in the SCOPIA 1000 chassis.

Warning You must install the RTM module before you install the Gateway module. Inserting an RTM module in the rear of the chassis when a Gateway module is already installed in the same position at the front of the chassis may damage the chassis.

Procedure

1. On the front of the chassis, loosen the screws of the blank panel covering the slot into which the Gateway module is to be installed.
2. Remove the blank panel.
3. Remove the new Gateway module from the antistatic bag.
4. Press the red buttons and open the handles of the Gateway module.
5. Align the edges of the Gateway module with the chassis guide rails.
6. Slide the Gateway module into the chassis until it stops (see Figure 2-5 for the SCOPIA 400 chassis).
7. Use even pressure to push the module further into the slot.

Caution Do not force the connection. Forcing the connection can bend or damage the pins in the connector inside the chassis.

Note If you are installing the Gateway module and the power to the chassis is on, the SWAP RDY LED on the module front panel turns blue when you slide the module into the chassis as far as it will go. This means that you can secure the module safely. The LED turns off when the handles are closed.

8 Snap the handles forward to secure the Gateway module in the slot.

9 Secure the Gateway module screws.

Caution Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all blades, faceplates, front covers, and rear covers are in place.

Removing a Module

This section describes how to remove the SCOPIA Gateway or the RTM module from the SCOPIA 400 chassis and from the SCOPIA 1000 chassis.

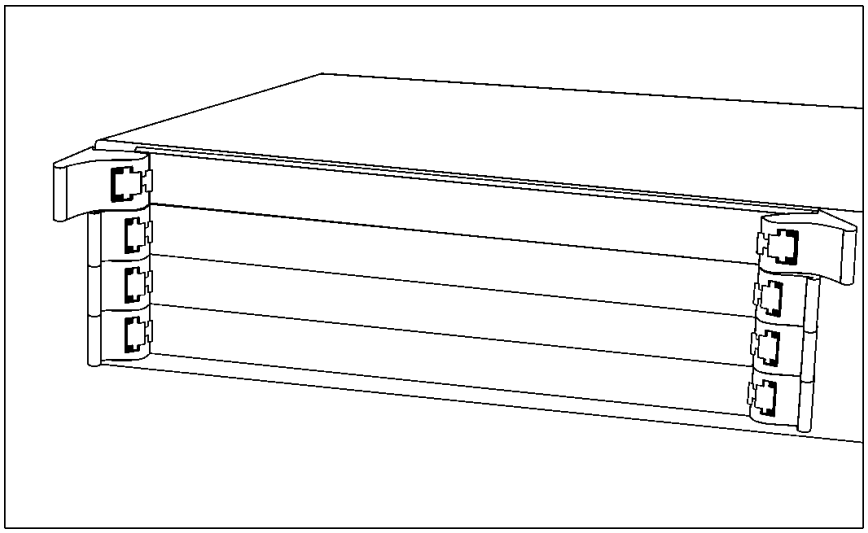
Warning You must remove the Gateway module from the slot at the front of the chassis before removing the corresponding RTM module from the same slot position at the rear of the chassis.

Procedure

1 Loosen the Gateway or RTM module screws.

2 Press the red buttons and open the handles of the Gateway or RTM module (see Figure 2-6 for the SCOPIA 400 chassis).

Figure 2-6 *Removing a Module from the SCOPIA 400 Chassis*



3 Wait for the blue SWAP RDY LED to light up. The SWAP RDY LED indicates that it is safe to remove the module.

Note It may take up to one minute for the LED to light up while the Windows operating system is shutting down.

The light goes out when the board is completely detached from the backplane.

4 Remove the module completely.

5 Insert a blank cover panel provided by RADVISION.

6 Secure the blank cover panel screws.

Caution Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all blades, faceplates, front covers, and rear covers are in place.

INITIAL GATEWAY CONFIGURATION

Initial monitoring and administration of the Gateway are performed from a remote PC via a serial connection. This allows you to access the boot configuration menu of the Gateway. At power-up, the Gateway goes through the following boot phases:

- **Auto-boot**—The embedded operating system initializes and displays basic information.
- **Configuration menu**—A 6-second countdown allows you to enter the configuration menu.
- **Initialization**—The Gateway completes its boot sequence and is ready for operation.

Note You can perform serial port configuration of the Gateway only at startup, during a short period indicated by a 6-second countdown. Once the initialization phase is complete, the only way you can access the configuration menu is by restarting the Gateway.

CONNECTING TO A PC

This section describes how to use the serial port connection to configure the Gateway with an IP address.

Procedure

1. Locate the terminal cable shipped with the Gateway.
2. Connect the end labeled **PC** to the serial port on the computer.
3. Connect the end labeled **Unit** to the serial port connector on the Gateway front panel.

Note The PC terminal should have an installed terminal emulation application, such as HyperTerminal.

SETTING THE IP ADDRESS

This section describes how to use the serial port to configure the unit with an IP address and other address information.

The serial port on the Gateway front panel is used to assign a new IP address to your Gateway. You must assign the IP address before you connect the Gateway to the network.

Before You Begin

Gather the items listed in Table 2-6 to assign an IP address to the Gateway.

Table 2-6 *Requirements for Setting the IP Address*

Requirements	Notes
Dedicated IP address for the Gateway	
IP address of the default router the Gateway uses to communicate over the network	
PC with available serial port and terminal emulator software installed	
RS-232 terminal cable (shipped with the unit)	

Procedure

1. Connect the supplied terminal cable to the PC terminal.
2. Connect the power cable.
3. Start the terminal emulation application on the PC.
4. Set the communication settings in the terminal emulation application on the PC as follows:
   - Baud rate: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
5. Turn on the power to the Gateway.
6. After the terminal emulator session starts, press the **RST** button on the Gateway front panel to reset the module.

   A log of the auto-boot events and a VxWorks banner scrolls across the computer monitor.

Note When the Gateway is started for the first time, two VxWorks banners appear. The configuration option appears after the second banner.

---

7. When the message “Press any key to start configuration” appears on the screen, press any key within 6 seconds.

   The network configuration **Main** menu displays:

```
Press any Key To start configuration...
Main menu
Enter <N> to configure default network port values
Enter <P> to change the configuration software password
Enter <A> to display advanced configuration menu
Enter <Q> to quit configuration menu and start GW
```

Caution If you do not press a key before the countdown ends, the device continues its initialization and you can only configure the device by pressing the **RST** button on the front panel.

---

8 At the prompt, type **N** to configure default network port values and press **Enter**.

9 At the **Enter IP address for default interface** prompt, type the IP address you want to assign to the Gateway and press **Enter**.

Caution Do not use leading zeros in the IP address.

10 At the **Enter Default Router IP Address** prompt, type the IP address of the router associated with the segment in which the unit will be installed and press **Enter**.

Caution Do not use leading zeros in the IP address.

11 At the **Enter IP Mask for default device** prompt, type the subnet mask without leading zeros, and then press **Enter**. If a subnet mask is not used, press **Enter**.

12 Allow the unit to complete the reboot process. A new emulator session begins.

13 Close the terminal emulator session.

Changing the Configuration Tool Login Password

You can use the terminal emulator to change the default password of the default login user before others can use the Gateway interface.

Procedure

1 Start a terminal emulator session for the Gateway.

2 Press the **RST** button on the front panel of the Gateway.

After 60 seconds, a new terminal emulator session begins on the computer monitor.

3 After the second VxWorks banner scrolls across the screen, the following message appears: “Press any Key to start the configuration.”

4 Press any key and then press **Enter**.

The default network properties screen appears.

5 At the prompt, enter **P** and press **Enter** to select “change the configuration software password.”

The **Enter user name** prompt appears.

6 Type the user login name for which you want to change the password and press **Enter**.

The default user name is admin. This is the user name that allows you to access the Gateway interface.

The **Enter new password** prompt appears.

7 Type the password you want the user to use to log in to the Gateway interface and press **Enter**.

There is no default password.

8 The network configuration **Main** menu re-appears.

9 Enter **Q** and press **Enter** to exit.

UPGRADING GATEWAY SOFTWARE

Software upgrades for the Gateway include the software components that are upgraded for the new version and a utility to upload the software to the unit. This section describes how to upgrade the software. For more information, see the Using the RADVISION Software Upgrade Utility chapter.

Procedure

1 Download the upgrade software to a host that can access the Gateway.

2 Unzip the upgrade file.

3 Double click the *upgrade.exe* file.

The RADVISION Software Upgrade Utility appears.

4 In the **Target IP** field, type the IP address of the Gateway for which you want to upload the software.

5 In the **User Name** field, type the software user name.

This is a global login name that the upload, upgrade, and Telnet utilities use to log in to the Gateway software. It can also be used to access the Administrator interface. The default user name is admin.

6 In the **Password** field, type the software password.

The default value is null.

Note To view the software components that will upgrade, click **Customize**. The **Customize** dialog box appears. If you do not want to upgrade a component, deselect it.

7 Click **Upgrade**.

The upgrade process takes a few minutes. After the upload completes, the **Upload Complete Message** dialog box appears.

8 Click **OK**.

CONNECTING THE GATEWAY TO THE NETWORK

The SCOPIA Gateway can connect to the LAN only through the front panel. The Gateway supports a 10/100BaseT, full-duplex Ethernet interface through an RJ-45 connector.

Procedure

1 Connect the supplied LAN cable from your network hub to the 10/100BaseT Ethernet port on the front panel of the Gateway. The 10/100BaseT port accepts an RJ-45 connector.

2 Connect a separate ISDN or serial line to each PRI or serial port in the rear panel of the Gateway. The port accepts an RJ-45 connector.

CONNECTING PRI LINES TO THE GATEWAY

You must connect a PRI line to at least one Gateway P20 SP port. The Gateway supports T1 and E1 PRI configurations.

Connecting Serial Lines to the Gateway

You can connect the Gateway S40 SP to four serial lines that may support different physical standards (V.35, RS-449 or EIA-530). The system is capable of recognizing the type of cable connected.

Procedure

1. Connect the DB-60 male connector of the cable to the DB-60 female connector of the unit.
2. Tighten the screws.
3. Connect the remote connectors (V.35, RS-449, EIA-530 and RS-366) to the connectors or the connecting cable of the remote equipment

Serial Gateway Cable Connections and Pin-outs

This section describes the DTE and DCE cables that you can use with the RADVISION Gateway S40 SP including the following topics:

Physical Description of DTE Cables

This section describes the following DTE cables supplied with the RADVISION Gateway S40 SP:

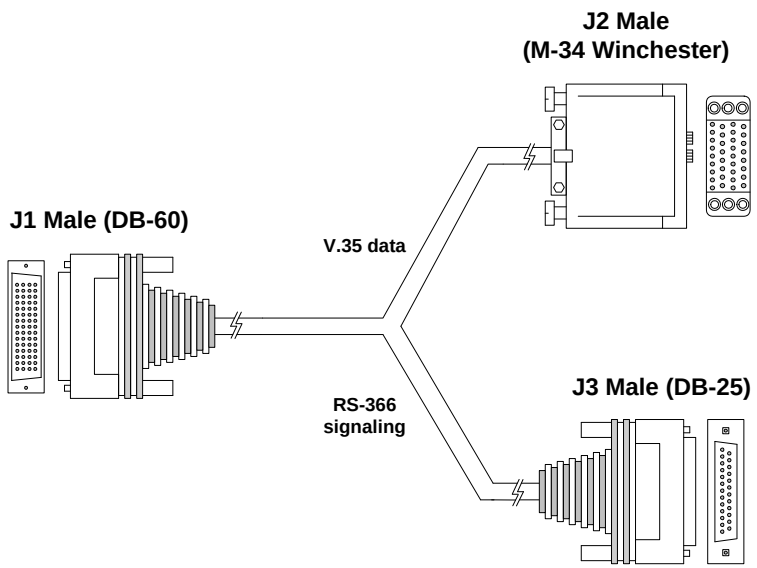
Note

- The **DB-25** connector provides the data interface for the EIA530/RS366-DTE and EIA530/RS366-DTE- LOS cables.
- The **DB-37** connector provides the data interface for the EIA449/RS366-DTE and KIV7/RS366-DTE cables.
- The **DB-25** connector provides the RS-366 signaling interface for all Gateway S40 SP cables.

V.35/RS366-DTE

Figure 2-7 shows the V.35/RS366-DTE cable.

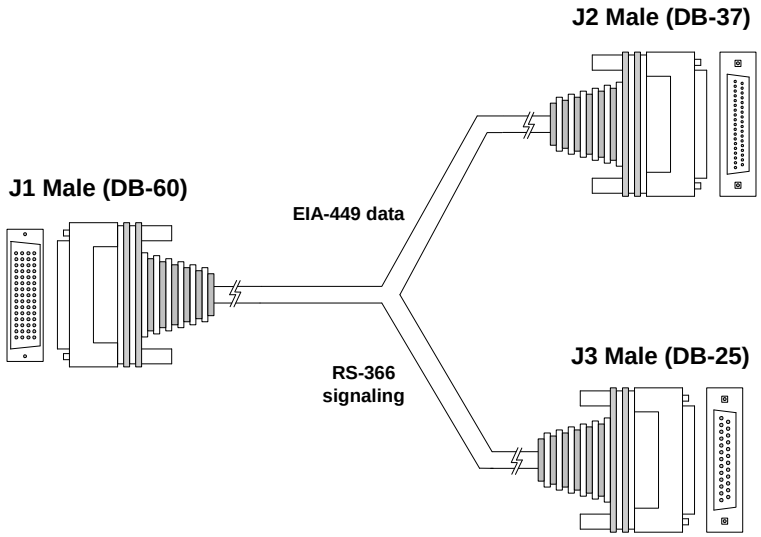
Figure 2-7 *V.35/RS366-DTE Cable*



EIA449/RS366-DTE

Figure 2-8 shows the EIA449/RS366-DTE cable.

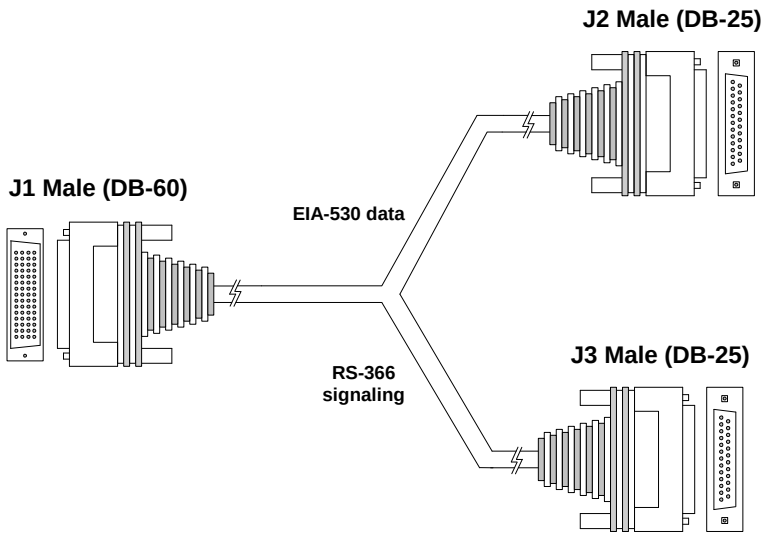
Figure 2-8 *EIA449/RS366-DTE Cable*



EIA530/RS366-DTE

Figure 2-9 shows the EIA530/RS366-DTE cable.

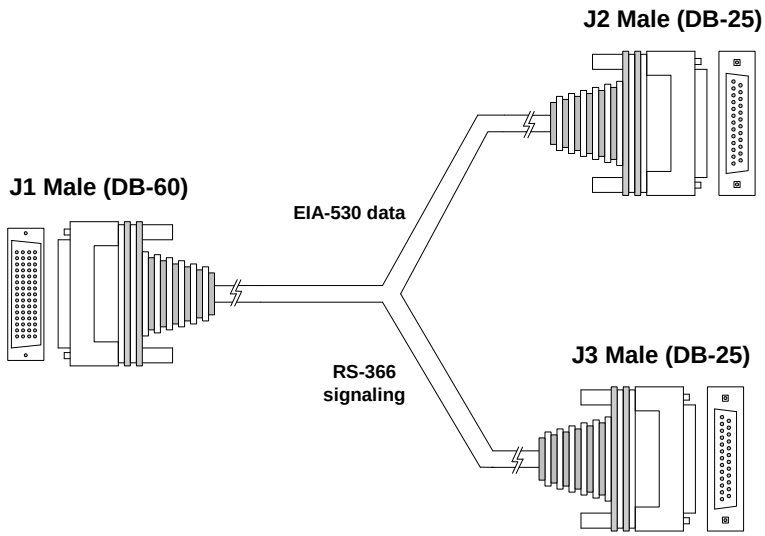
Figure 2-9 *EIA530/RS366-DTE Cable*



EIA530/RS366-DTE-LOS

Figure 2-10 shows the EIA530/RS366-DTE-LOS cable.

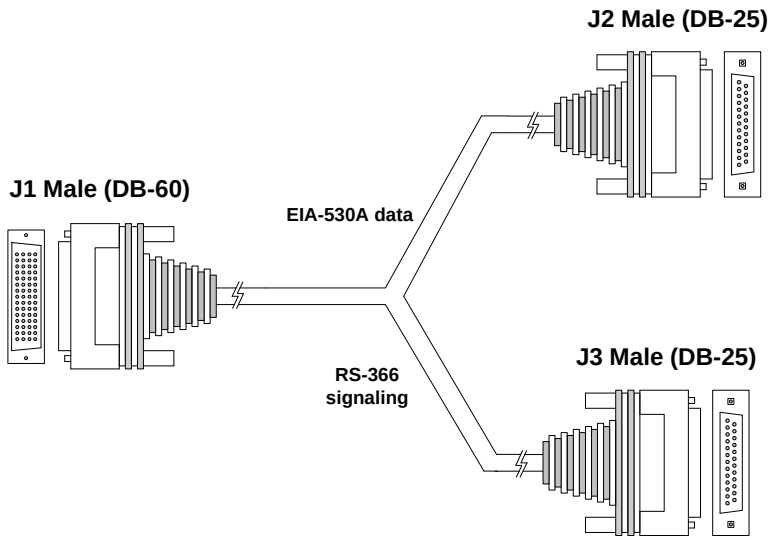
Figure 2-10 *EIA530/RS366-DTE-LOS Cable*



EIA530A/RS366-DTE

Figure 2-11 shows the EIA530A/RS366-DTE cable.

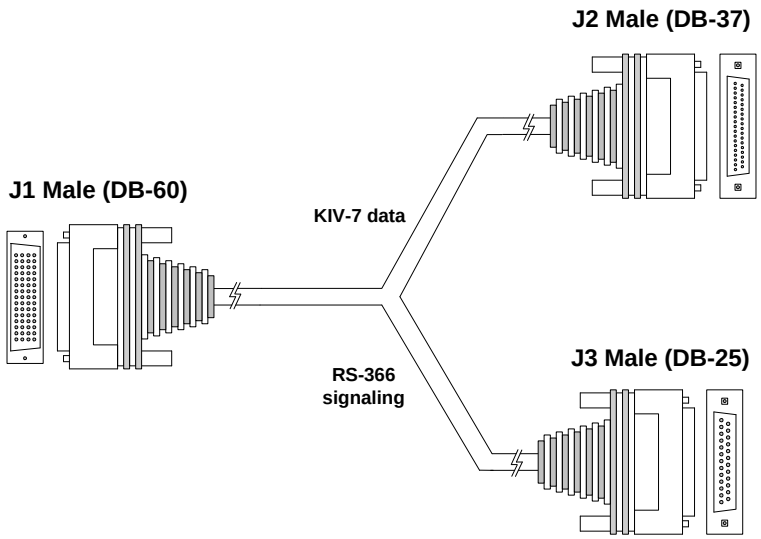
Figure 2-11 *EIA530A/RS366-DTE Cable*



KIV7/RS366-DTE

Figure 2-12 shows the KIV7/RS366-DTE cable.

Figure 2-12 *KIV7/RS366-DTE Cable*



PHYSICAL DESCRIPTION OF DCE CABLES

This section describes the following DCE cables supplied with the RADVISION Gateway S40 SP:

- V.35/RS366-DCE
- EIA449/RS366-DCE
- EIA530/RS366-DCE

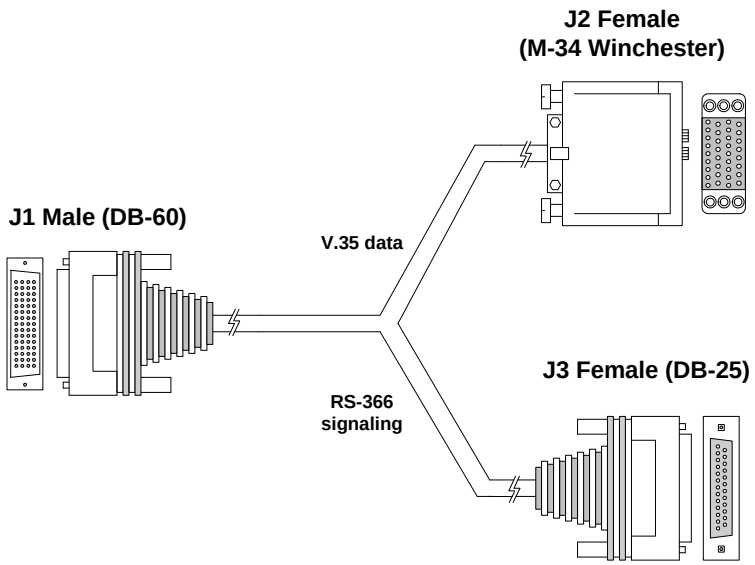
Note

- The **DB-25** connector provides the data interface for the EIA530/RS366-DCE cable.
- The **DB-37** connector provides the data interface for the EIA449/RS366-DCE cable.
- The **DB-25** connector provides the RS-366 signaling interface for all Serial Gateway cables.

V.35/RS366-DCE

Figure 2-13 shows the V.35/RS366-DCE cable.

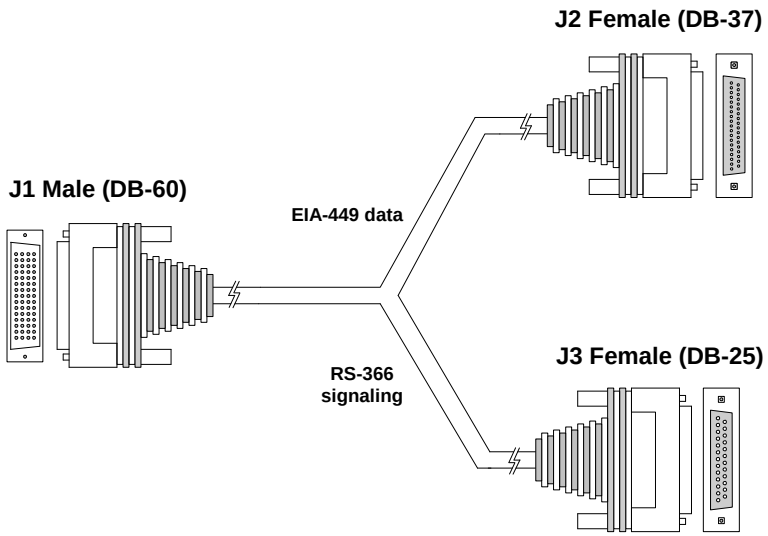
Figure 2-13 *V.35/RS366-DCE Cable*



EIA449/RS366-DCE

Figure 2-14 shows the EIA449/RS366-DCE cable.

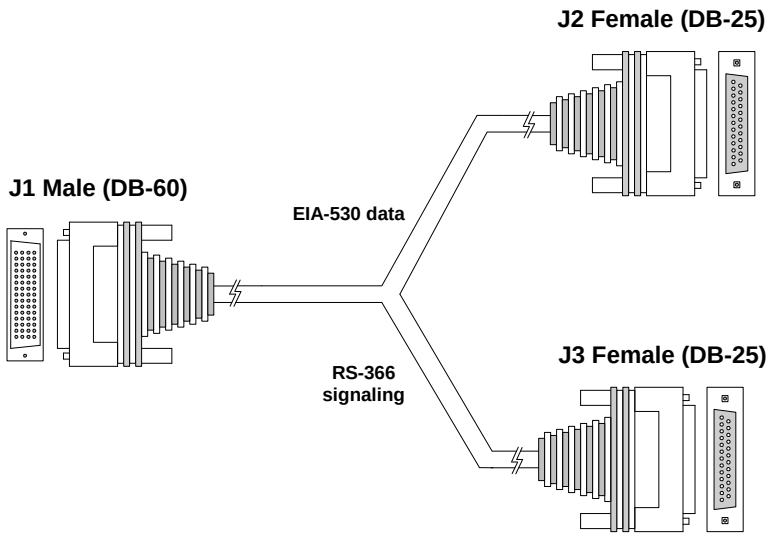
Figure 2-14 *EIA449/RS366-DCE Cable*



EIA530/RS366-DCE

Figure 2-15 shows the EIA530/RS366-DCE cable.

Figure 2-15 *EIA530/RS366-DCE Cable*



Data Interface Cable Pin-out Configurations

Table 2-7 describes the data interface pin-out configuration for the Serial Gateway cables.

Table 2-7 *Serial Gateway Data Interface Cable Pin-out*

Signal Name	Mnemonic	KIV-7 (DB-37) DTE only	EIA-449 (DB-37)	EIA-530 (DB-25)	EIA-530 LOS (DB-25) DTE only	EIA-530A LOS (DB-25) DTE only	V.35 (M-34)
Shield	—	1	1	1	1	1	A
Transmit Data	TXD A	2	4	2	2	2	P
Transmit Timing	TXC A	15	5	15	15	15	Y
Receive Data	RXD A	3	6	3	3	3	R
Request To Send	RTS A	4	7	4	4	4	C
Receive Timing	RXC A	17	8	17	17	17	V
Clear To Send	CTS A	5	9	5	5	5	D
Data Set Ready	DSR A	6	11	6	6	6	E
Data Terminal ready	DTR A	20	12	20	20	20	H
Carrier Detect	DCD A	8	13	8	8	8	F
Terminal Timing	TT A	24	17	24	24	24	U
Signal Ground	—	27	19	7	7	7	B
Transmit Data	TXD B	14	22	14	14	14	S
Transmit Timing	TXC B	12	23	12	12	12	AA
Receive Data	RXD B	16	24	16	16	16	T

Table 2-7 *Serial Gateway Data Interface Cable Pin-out (continued)*

Signal Name	Mnemonic	KIV-7 (DB-37) DTE only	EIA-449 (DB-37)	EIA-530 (DB-25)	EIA-530 LOS (DB-25) DTE only	EIA-530A LOS (DB-25) DTE only	V.35 (M-34)
Request To Send	RTS B	19	25	19	19	19	—
Receive Timing	RXC B	9	26	9	9	9	X
Clear To Send	CTS B	13	27	13	13	13	—
Data Set Ready	DSR B	22	29	22	22	—	—
Data Terminal ready	DTR B	23	30	23	23	—	—
Carrier Detect	DCD B	10	31	10	10	10	—
Terminal Timing	TT B	11	35	11	11	11	W
Local Loopback	LL	—	10	18	—	18	L, K
Remote Loopback	RLB	—	14	21	—	21	N
Loss of Sync	LOS unbalanced	31	36	—	—	—	—
Loss of Sync	LOS A	—	3	—	18	—	—
Loss of Sync	LOS B	—	21	—	21	—	—

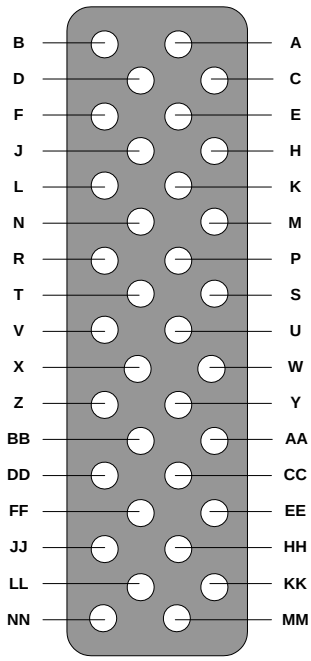
Data Interface Pin Layouts

This section illustrates the pin layouts for the Serial Gateway cable connectors.

M-34 Connector

Figure 2-16 shows the M-34 pin assignment.

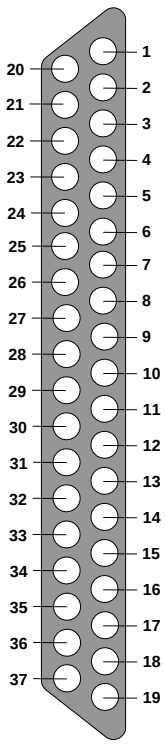
Figure 2-16 *M-34 Pin Layout*



DB-37 CONNECTOR

Figure 2-17 shows the DB-37 pin layout.

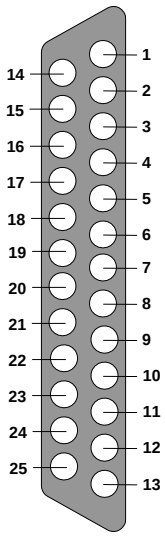
Figure 2-17 *DB-37 Pin Layout*



DB-25 CONNECTOR

Figure 2-18 shows the DB-25 pin layout.

Figure 2-18 *DB-25 Pin Layout*



Signaling Interface Cable Pin-out Configuration

Table 2-8 describes the signaling interface pin-out configuration for the Serial Gateway cables.

Table 2-8 *Serial Gateway Signaling Interface Cable Pin-out*

Signal Name	Mnemonic	RS-366 (DB-25)
Shield	—	1
Digit Present	DPR	2
Abandon Call & Retry	ACR	3
Call Request	CRQ	4
Present Next Digit	PND	5
Power Indication	PWI	6
Signal Ground	—	7
Distant Station Connection	DSC	13
Digit Signal Circuit 1	NB1	14
Digit Signal Circuit 2	NB2	15
Digit Signal Circuit 4	NB4	16
Digit Signal Circuit 8	NB8	17
Receive Common	RC	18
Send Common	SC	19
Data Link Occupied	DLO	22

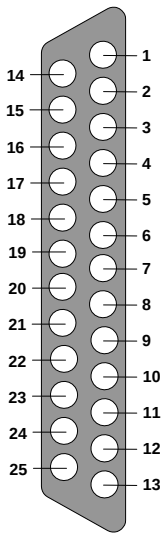
Signaling Interface Pin Layout

This section illustrates the pin layout for the Serial Gateway signaling cable connector.

DB-25 Connector

Figure 2-19 shows the DB-25 pin layout.

Figure 2-19 *DB-25 Pin Layout*



Connecting the Gateway to a Power Source

This section describes how to supply power to the Gateway. The Gateway is equipped with an autoswitching power supply that supports 100-240 VAC at 50/60 Hz.

Procedure

1. Plug a power cord into the power socket on the rear panel of the Gateway.
2. Connect the power cable to a grounded AC outlet.
3. Turn the power on.

ACCESSING THE GATEWAY ADMINISTRATOR INTERFACE

The Gateway Administrator is a web interface that allows you to view and configure the Gateway hardware and application parameters. You can use the Gateway interface to:

- Set administrative parameters to define access to the Gateway
- Set Gateway application parameters that specify how the Gateway processes incoming and outgoing calls
- Set chassis operating parameters for SCOPIA Gateway modules installed in the top slot of a SCOPIA 400 chassis

Before You Begin

The following requirements are necessary to access the Gateway Administrator web interface:

- A Java-compliant browser. Microsoft Internet Explorer version 5.5 or later is recommended.
- The Gateway IP address or a web link to the Gateway.
- Administrator level-access
- The required user name and password.

Note For first-time installation, you must assign an IP address to the Gateway using a serial port connection before you can access the web interface. For more information, see Setting the IP Address on page 35.

Procedure

1. Launch your browser and type the IP address or the name of the Gateway.

   For example, **http://125.221.23.44** or **board_name**.

   The Gateway login page appears.

2 Type the Administrator user name and password in the appropriate fields and click **Login**. The default global user name is *admin*. The default password is <null>.

The Gateway Administrator interface appears.

Note If you try to sign in as an Administrator and another Administrator is currently signed in, the Gateway signs you in as a **Read only** user and the words *Read Only* appear at the top of the window. **Read only** users cannot edit any of the Gateway settings.

REGISTERING THE ONLINE HELP

The online help files for the Gateway Administrator interface are shipped on the the RADVISION Utilities and Documentation CD-ROM. To use the online help, you must install the help files for the appropriate Gateway in a shared directory on your network and register the directory location in the Administrator interface.

If you wish to install the online help on a shared network location and link it to the Gateway Administrator, perform the following steps:

Procedure

1 Copy the online help library from the RADVISION Utilities and Documentation CD-ROM to a shared folder on a PC on your network.

2 Log in to the Gateway Administrator interface.

3 In the **Online help URL** field of the Board **Web** tab, type the directory path to the help files you installed on your PC.

The path must have the form:

`file://computerName/sharedDirectory`

where `computerName` is the name of the computer on the network and `sharedDirectory` is the path to the **Online Help** folder on the CD-ROM. For example:

`file://myComputer/Shared/Online Help`

4. Click **Upload** in the Gateway Administrator toolbar, followed by **Refresh**.
5. You may need to log out and log back in to the Gateway Administrator for the change to take effect.

NETSCAPE NAVIGATOR USERS

Online help files located on the local network and accessed using Netscape Navigator 4.x must be located on a mapped network drive.

3

CONFIGURING THE SCOPIA GATEWAY

This section describes what you can configure and how to configure RADVISION Gateways, and includes the following topics:

About Gateway Interface Users

Users must have the appropriate access level to log in to the Gateway interface. With Administrator-level access, a user can configure the Gateway and monitor Gateway activity. You can view and manage the list of Gateway users in the Users tab of the **Board** section of the Gateway interface. The Users tab displays all currently configured users and their access levels.

There are three types of Gateway interface users:

- **Administrator**—Full access to the Gateway interface to configure Gateway settings.
- **Operator**—User can monitor or disconnect calls but otherwise only has read-only access to the Gateway interface.
- **Read-only**—User has read-only access to the Gateway interface.

Adding Gateway Interface Users

In the Users tab of the **Board** section of the Gateway interface, you can add Gateway interface users.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the **Users** tab.
3. Click **Add** to add a new user.

   The Add User dialog box appears.
4. In the **User name** field, enter the user login name.
5. In the Access Level field, choose one of the following access levels: **Administrator**, **Operator** or **Read only**.
6. In the Password field, enter the password that the user uses to login to the Gateway interface.
7. In the Confirm Password field, re-enter the password.
8. Click **Upload**.

Editing Gateway Interface Users

In the **Users** tab of the **Board** section of the Gateway interface, you can edit Gateway interface users.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the **Users** tab.

3 Select an existing user and click **Edit**.

The Edit User dialog box appears.

4 In the **User name** field, edit the user login name.

5 In the Access Level field, choose one of the following access levels: **Administrator**, **Operator** or **Read only**.

6 In the Password field, edit the password that the user uses to login to the Gateway interface.

7 In the Confirm Password field, re-enter the password.

8 Click **Upload**.

Deleting Gateway Interface Users

In the **Users** tab of the **Board** section of the Gateway interface, you can delete Gateway interface users.

Procedure

1 In the Gateway interface, on the sidebar, click **Board**.

2 Click the **Users** tab.

3 Select a user and click **Delete**.

Viewing LED Information

In the **LED Monitoring** tab in the **Board** interface, you can monitor the status of all the Gateway front and rear panel LED indicators. The LEDs are displayed in diagrams reproducing the layout of the Gateway front and rear panels.

Procedure

1 In the Gateway interface, on the sidebar, click **Board**.

2 Click the **LED Monitoring** tab.

3 Place the mouse cursor over the required LED in the **LED Monitoring** tab to view a description of that LED.

VIEWING GENERAL INFORMATION ABOUT THE GATEWAY

In the **Basics** tab in the **Board** interface, you can view and configure general information about the hardware and software the Gateway uses.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the **Basics** tab.

   Table 3-1 describes the elements that appear in the **Basics** tab.

Table 3-1 *Board Basic Tab Elements*

Field	Description
Board name	Identifies the model number of the board or device.
Location	User-configured description about the device. Click this field to type a new description, and then click **Upload** on the toolbar.
Slot number	The number of the cPCI slot in the SCOPIA 400 chassis in which this SCOPIA MCU is inserted.
Serial number	The serial number that the factory assigned to the device.
License key	Your RADVISION license key for accessing SCOPIA 400 chassis devices. Click **Update** to modify your RADVISION license key. **Note** A separate license key is installed on each board in the SCOPIA 400 chassis.
Hardware version	The version number of the current hardware configuration.
Software version	The first two digits of the version number of the software installed on the device. Click the **Details** button to view details of the versions of software components installed on the device.
Date/Time	The date and time that the Gateway clock reports.

Related Topics

- Updating Your License on page 65
- Viewing Software Version Details on page 65
- Setting the Time and Date on the Gateway on page 66
- Setting the Gateway Location on page 67
- Resetting Default Board Basic Settings on page 67

Updating Your License

You use the **Basics** tab to update your Gateway license.

Procedure

1. On the sidebar, click **Board**.
2. Click the **Basics** tab.
3. Click **Update**.

   The Licensing and Registration dialog box appears.
4. Access the RADVISION web site to register before requesting a new license key by clicking the **Click here to register at the web site** link, or by copying the URL that appears in the lower half of the screen into your browser.
5. Enter your new license key in the New license key field and click **Upload** to activate the new license key.

Viewing Software Version Details

You use the **Basics** tab to view expanded software version information.

Procedure

1. On the sidebar, click **Board**.
2. Click the **Basics** tab.
3. Locate the Software version field and click **Details**.

   The Version Details dialog box appears.

Setting the Time and Date on the Gateway

You use the **Basics** tab to choose how your Gateway tracks the date and time.

Procedure

1. On the sidebar, click **Board**.
2. Click the **Basics** tab.
3. Locate the Date/Time field and click **Change**.

   The Change Time dialog box appears. The date and time the Gateway reports appear in the Set time to field.
4. In the Change field, select the unit of time that you want to change.

Note There is no unit to change AM and PM. This designation rolls automatically when the hour rolls past 12 backward or forward. Similarly, seconds roll minutes, minutes roll hours, hours roll days, and days roll months.

5. In the Set time to field, choose the up or down arrow to change that unit.

   The unit you choose changes in the direction you choose: higher (up) or lower (down).
6. Repeat step 4 and 5 for as many units as you want to change.
7. On the toolbar, click **Upload**.

Setting the Gateway Location

You can install the Gateway anywhere on your network including at a remote site. On the **Basics** tab, you can describe the current location of the Gateway.

Procedure

1. On the sidebar, click **Board**.
2. Click the **Basics** tab.
3. In the Location field, enter the location information about the Gateway that you want to display.

   The field displays up to 23 characters.
4. On the toolbar, click **Upload** to save to configuration memory.

Resetting Default Board Basic Settings

In the **Basics** tab, you can restore board basic settings to factory defaults.

Procedure

1. On the sidebar, click **Board**.
2. Click the **Basics** tab.
3. Select the **Reset to default settings** check box.

VIEWING ADDRESS SETTINGS

In the **Addressing** tab, you can view address information for the Gateway such as IP address information, Domain Name Server (DNS) information and Ethernet port speed and duplex. Table 3-2 describes the elements that appear on the **Addressing** tab.

Table 3-2 *Addressing Tab Elements*

Field	Description
IP Address	
IP Address	The IP address assigned to the Gateway.
Router IP	The address of the router that the Gateway uses.
Subnet Mask	The subnet address that the Gateway uses.
DNS	
DNS Server IP	The IP address of the Domain Name Server (DNS) that the Gateway accesses.
Device DNS name	The device name of the Domain Name Server (DNS) that the Gateway accesses (read-only).
Ethernet	
Port type	Displays information about the Ethernet connection (read-only).
Port settings	The Ethernet speed and duplex that the Gateway uses.
MAC address	Displays the Mandatory Access Control (MAC) code assigned to the Gateway (read-only).
Port status	Displays the actual Ethernet speed and duplex the Gateway uses on the network (read-only).

Related Topics

- Changing Address Settings on page 69

CHANGING ADDRESS SETTINGS

In the **Addressing** tab, you can change the following address information for the Gateway—IP address information, DNS information and the Ethernet port speed and duplex.

Procedure

1. In the Administrator interface, on the sidebar, click **Board**.
2. Click the **Addressing** tab.
3. To change an IP address setting, do any of the following steps:
   - In the IP Address field, type the IP address you want to assign to the Gateway.
   - In the Router IP field, type the IP address of the router you want the Gateway to use.
   - In the Subnet Mask field, type the subnet mask you want the Gateway to use.
4. In the DNS Server IP field, type the IP address of the DNS server that you want the Gateway to use.
5. In the Port settings field, choose the Ethernet port and duplex speed value you want to set.
6. On the toolbar, click **Upload**.

Related Topics

- Viewing Address Settings on page 68

CONFIGURING WEB SETTINGS

On the Web tab, you can set the web server port and configure enhanced web security settings.

This section describes the following topics:

CHANGING THE ADMINISTRATOR INTERFACE WEB SERVER PORT

Port 80 is the default Administrator interface web server port. For additional security, you can modify the web server port in the Web tab.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the **Web** tab.
3. In the Web server port field, enter the port number.
4. On the toolbar, click **Upload**.

ENABLING HTTPS

This section describes how to enable or disable Gateway HTTPS support.

Note HTTPS support is enabled when a certificate is installed or a certificate is self-signed.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the Web tab.
3. Check **Support Secure Communications (HTTPS)** to enable HTTPS support. Uncheck it to disable HTTPS.
4. Click **Upload**.

Logging into the Gateway when HTTPS is enabled

Proceed as follows when logging into the Gateway with HTTPS enabled.

Note When the Support Secure Communications (HTTPS) option is enabled, the Gateway URL automatically appears as an https:// URL. When the Support Secure Communications (HTTPS) option is disabled, the URL appears as a regular http:// URL.

Procedure

1. In your browser type the URL of the Gateway.

   If HTTPS is enabled, a Security Alert screen displays.
2. Click Yes to proceed and display the Administrator login screen. Click **No** to cancel the current operation.
3. Type a user name and password.
4. Click **Login**.

Managing Digital Certificates

The Certificate Management Wizard guides the administrator through the following digital certificate management processes:

- Generating a Certificate Request on page 72
- Deleting a Pending Certificate Request on page 73
- Loading a Certificate on page 73
- Removing a Certificate on page 73
- Renewing a Certificate on page 74
- Exporting a Signed Certificate on page 75
- Importing a Certificate on page 75

Note The tasks you can perform with the wizard depend on the certificate status. The status displays on the Welcome to the Web Server Certificate Wizard screen.

Generating a Certificate Request

You can generate a self-signed certificate or generate a request for an external certificate. The request for an external certificate must be sent to a Certificate Authority. The Certificate Authority will generate a certificate from the request.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the **Web** tab.
3. Click **Manage Certificate**.

   The Welcome to the Web Server Certificate Wizard screen appears.
4. Select **Create a new certificate request** and click **Next**.
5. To generate a certificate request using existing organization information, follow the procedure described at step 6.

   To generate a certificate request using new information, follow the procedure described at step 7.
6. Select **Using information from the existing certificate** and click **Next**.

   The Certificate Request Summary screen appears showing the existing organization and geographical information. Go to step 8.
7. Select **Using new information** and click **Next**.
   - Enter the required details in the Organization Information screen and click **Next**.
   - Enter the required details in the Geographical Information screen and click **Next**.
   - The Certificate Request Summary screen appears showing the configured organization and geographical information. Go to step 8.
8. Click **Next** to generate a certificate request.
9. Copy the generated request text to a file and send it to the certification authority, as described at Loading a Certificate on page 73.
10. Click **Finish**.

Deleting a Pending Certificate Request

You can delete a pending request for an external certificate which has not yet been loaded.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the **Web** tab.
3. Click **Manage Certificate**.

   The Welcome to the Web Server Certificate Wizard screen appears.
4. Select **Delete a pending request** and click **Next**.

   The Delete a Pending Request screen displays.
5. Click **Finish**.

Loading a Certificate

You load an external certificate that has been received from a certificate authority. The external certificate must match a pending request for it to be loaded properly.

Procedure

1. In the **Gateway Administrator** interface sidebar, click **Board**.
2. Click the **Web** tab.
3. Click **Manage Certificate**.

   The Welcome to the Web Server Certificate Wizard screen displays.
4. Select **Process the pending request and install the certificate** and click **Next.**

   The Process a Pending Request screen displays.

Removing a Certificate

You can remove a self-signed or an external certificate that has already been loaded.

Procedure

1. In the Gateway interface, on the sidebar, click **Board**.
2. Click the **Web** tab.

3 Select **Remove the current certificate** and click **Next**.

The Certificate Summary screen displays.

Note Removing a certificate disables HTTPS support and causes the Gateway to reset.

4 Select **Yes** and then **Finish** to remove the certificate,

–or–

Select **No** to cancel the operation.

Renewing a Certificate

Every certificate has an expiration date. You can renew it using existing information or new information.

Procedure

1 In the **Gateway Administrator** interface sidebar, click **Board**.

2 Click the **Web** tab.

3 Click **Manage Certificate**.

The Welcome to the Web Server Certificate Wizard screen displays.

4 To renew a certificate request using existing organization information, follow the procedure described at step 5.

To renew a certificate request using new information, follow the procedure described at step 6.

5 Select **Using information from the existing certificate** and click **Next**.

The Certificate Request Summary screen appears showing the existing organization and geographical information. Go to step 7.

6 Select **Using new information** and click **Next**.

- Enter the required details in the Organization Information screen and click **Next**.
- Enter the required details in the Geographical Information screen and click **Next**.
- The Certificate Request Summary screen appears showing the configured organization and geographical information. Go to step 7.

7 Click **Next** to generate a certificate request.

8 Copy the generated request text to a file and send it to the certification authority, as described at Loading a Certificate on page 73.

9 Click **Finish**.

Exporting a Signed Certificate

Exporting a signed certificate sends the certificate to a text file and the key material (known as the "keyblob") to the same text file.

Procedure

1 In the Gateway interface, on the sidebar, click **Board**.

2 Click the **Web** tab.

3 Click **Export Certificate**.

4 The **Certificate Export** screen displays.

5 Enter a password of up to 16 characters, and click **OK**.

The **File Download** screen displays.

6 Click **Save** and save the file to the directory where you wish to save the certificate.

The certificate is saved as *certific.csr*.

The Download Complete screen displays.

Importing a Certificate

You can import a certificate from a saved location.

Note The Administrator is responsible for the passwords. The system does not save import or export passwords.

Procedure

1 In the Gateway interface, on the sidebar, click **Board**.

2 Click the **Web** tab.

3 Click **Import Certificate**.

The **Import a Certificate File** dialog box displays.

4 Enter the certificate name.

–or–

Click **Browse** to allocate the certificate to import.

The Choose File dialog box displays. Double-click the certificate that you want to import.

5 Enter the same password that you used in the export certificate.

6 Click **Import** to import and install the new certificate.

CONFIGURING SECURITY

You can configure the access that external programs have to the Gateway. These external programs include Telnet, Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), and ICMP (Internet Control Message Protocol, or ping).

Procedure

1 In the Gateway interface, on the sidebar, click **Board**.

2 Click the **Security** tab.

3 From the Security mode field, choose the access level you want the Gateway to support:

- **Standard**—Enables SNMP, Telnet, FTP, and ICMP to access the Gateway.
- **High (no Telnet or Ftp)**—Enables access to the Gateway only through SNMP and ICMP.
- **Maximum (no Telnet, ftp, SNMP and ICMP)**—Disallows external programs to access the Gateway.

4 In the SNMP Read community and Write community fields, enter default strings used to enable SNMP communication between the Gateway and a external application.

5 On the toolbar, click **Upload**.

Configuring SCOPIA 400 Chassis Parameters

If your SCOPIA Gateway module is installed in the top slot of the SCOPIA 400 chassis, then the module also performs PCI bus functions for the chassis. In the Gateway interface, you can use the **System** section to monitor chassis functions remotely.

One of the functions the chassis performs is to monitor ambient temperature. You can set temperature thresholds in the **System** section. The chassis uses these thresholds to trigger a warning that the ambient temperature exceeds specification and when the temperature has returned to five degrees below the warning threshold.

Related Topics

- Viewing the System Section on page 77
- Setting Chassis Temperature Thresholds on page 79
- Refreshing the System Section on page 79

Viewing the System Section

You can view the **System** section by selecting it in the Gateway interface.

Procedure

1. Access the Gateway interface.
2. On the sidebar, click **System**.

   Table 3-3 lists the elements that appear in the **System** section.

Table 3-3 *System Elements*

Element	Description
Information section	This section provides the following information about the SCOPIA chassis hardware: ■ **Serial number—**Displays the serial number of the chassis. ■ **Part number—**Displays the part number of the chassis. ■ **System configuration—**Identifies the hardware configuration the chassis uses.
Temperature threshold	In this section, you can set the following temperature values that the chassis uses to trigger changes in the ambient temperature status: ■ **Low—**Enter the temperature value at which the Gateway module turns off the chassis temperature alarm. The value is measured in Celsius. ■ **High—**Enter the temperature value above which the Gateway module turns on the chassis temperature alarm. The value is measured in Celsius.
Status section	These LEDs provide information about chassis operation. ■ **Power**—This LED lights green for normal operation. It lights red when one power supply fails. ■ **Alarm**—This LED lights green for normal operation. It lights red when a system failure occurs. ■ **Fans**—This LED lights green for normal operation. It lights red when one or more fans fail. A message then appears indicating which fan has failed. ■ **Temperature**—This LED lights green for normal operation. It is red when the chassis determines that the ambient temperature rises above the high temperature threshold. The LED blinks when the falling ambient temperature crosses the high threshold to within five degrees of the high threshold.

Related Topics

- Setting Chassis Temperature Thresholds on page 79
- Refreshing the System Section on page 79

Setting Chassis Temperature Thresholds

You can set critical and safe threshold values for the SCOPIA chassis.

Procedure

1. In the Gateway Administrator interface sidebar, click **System**.
2. In the **High** field, enter a value in Celsius for the critical temperature threshold.

   The ALARM and TEMP LEDs illuminate red when the operating temperature inside the chassis rises above this value.
3. In the **Low** field, enter a value in Celsius for the safe temperature threshold.

   The TEMP LED illuminates green to indicate normal operation.

   The TEMP LED blinks green when the reading is inaccurate. If the LED blinks green for a few seconds and then illuminates continuously, no action is necessary. If the LED blinks green continuously, contact RADVISION Customer Support.
4. Click **Upload** to save the changes.
5. Click **Refresh** to refresh the **System** section.

Refreshing the System Section

You can refresh the information that appears in the **System** section to provide the latest Gateway status.

Procedure

1. In the Gateway interface, make sure that **System** is selected on the sidebar.
2. Click **Refresh**.

ABOUT THE GATEWAY ADMINISTRATOR INTERFACE

In the Gateway Administrator interface, you can view Gateway resource information, define the Gateway mode of operation, configure and edit Gateway services, configure physical line settings, monitor and disconnect calls, view reported alert events, and view debugging details. Table 3-4 explains the tabs that appear in the Gateway Administrator interface.

Note There may be slight variations between the configuration options described in this section and the options appearing in the Gateway you are working with.

Table 3-4 *Gateway Administrator Interface Tabs*

Tab Name	Description
Status	Displays Gateway resource usage information, number of calls currently in progress, and servicing gatekeeper details.
Settings	Defines the mode of Gateway operation.
Services	Defines services that the Gateway provides.
Port	Defines physical line settings for that particular PRI or serial port.
Calls	Displays details on current calls and disconnect calls.
Event Log	Displays reported alert events.
Statistics	Displays specific system information such as call traces and debugging details.
Maintenance	Provides access to maintenance mode, in which you can prevent the Gateway from accepting new calls, and perform software upgrades and other maintenance work.

Figure 3-1 and Table 3-5 display and list the elements in the Gateway Administrator interface.

Figure 3-1 *Gateway Administrator Interface*

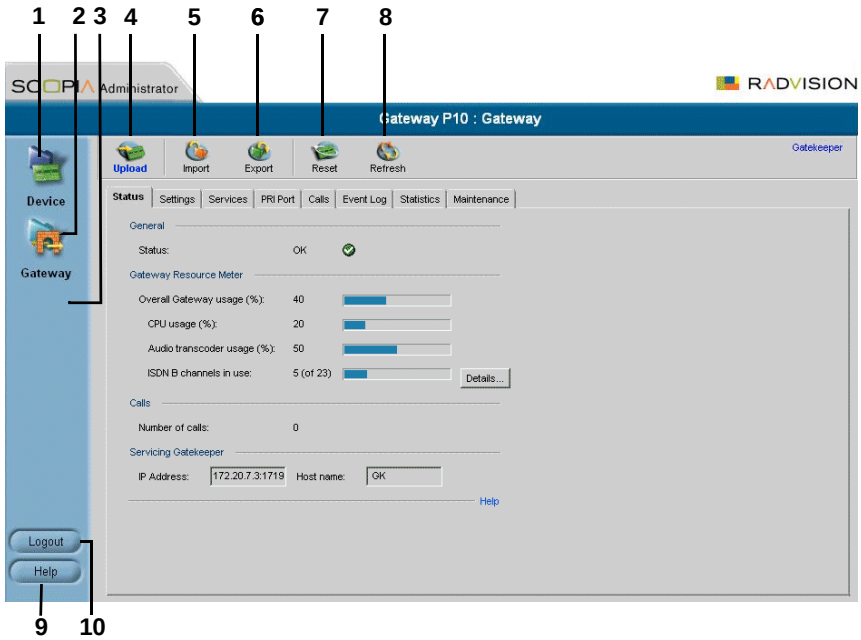


Table 3-5 *Gateway Administrator Interface Elements*

1	System button
2	Board button
3	Gateway button
4	Upload button
5	Import button
6	Export button
7	Reset button
8	Refresh button

Table 3-5 *Gateway Administrator Interface Elements*

9	Help button
10	Logout button

The Gatekeeper control on the right side of the toolbar provides a link to the Administrator web page of the RADVISION ECS Gatekeeper with which the Gateway registers. Enter the IP address of the ECS with which the Gateway registers in the Specify Gatekeeper address field in the IP Connectivity section of the Settings tab when the IP connectivity mode option is set to Using gatekeeper. For more information, see Configuring the Gateway to Register With a Gatekeeper on page 86

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 3-6 lists the information in the Status tab.

Table 3-6 *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 (Gateway P20 SP only).
Calls	■ **Number of calls**—Displays the total number of calls currently in progress in the Gateway.

Table 3-6 Status Tab Sections (continued)

Section Name	Description
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
- Refreshing Gateway Status

VIEWING B CHANNEL STATUS

This section applies only to Gateway P20 SP.

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

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Status** tab (if not already selected).
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

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Status** tab (if not already selected).
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:

Configuring Basic Gateway Settings

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

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **Basics** (if not already selected).
4. In the Gateway Identifier field, enter the Gateway identifier.

Configuring IP Connectivity Settings

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 Configuring the Gateway to Register With a Gatekeeper on page 86).
- **Peer-to-Peer**—The Gateway connects directly to a peer device without the need for a gatekeeper (see Configuring the Gateway for Peer-to-Peer IP Connectivity on page 88). Peer devices include RADVISION H.324/M Gateways for mobile applications.

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

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **IP Connectivity**.
4. In the IP connectivity mode field, choose **Using gatekeeper**.
5. Make one of the following selections:
   - Select the Gatekeeper auto discover and register option for the Gateway to automatically search for and attempt to register to a gatekeeper.
   - Select the Specify Gatekeeper address option to specify the gatekeeper to which the Gateway registers.
6. In the Gatekeeper address field, do one of the following:
   - Enter 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**.
7. In the Gatekeeper port field, enter the port number of the gatekeeper. The default setting is 1719.
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.

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.

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.

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 (see Serial Ports on page 131 for more information).

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.

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.

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

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

2 Click the **Settings** tab.

3 Click **IP Connectivity**.

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

Note Changing this setting causes the Gateway to reset.

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 About Peer-to-Peer H.323 Call Disconnect Reasons on page 91), 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 About Peer-to-Peer H.323 Call Disconnect Reasons on page 91), 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.

---

6 In the **Peer list** section, you can define 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, enter 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.”

---

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.

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.

9 (PRI Gateways only) In the Reject calls from peer devices when less than n B channels are free field, enter 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 3-7 lists the reasons for which the Gateway peer-to-peer hunting module might disconnect a call.

Table 3-7 *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.

Table 3-7 Disconnect Reasons (continued)

Number	H.323 Call Disconnect Reason
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.
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.

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

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click the **IVR** button.

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 9.

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.

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

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

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.

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>.

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.

---

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

11 In the Port field, enter 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

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

2 Click the **Settings** tab.

3 Click the **Delimiters** button.

4 In the Second number delimiter field, enter 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 Gateway S40 SP.

5 In the TCS4 extension delimiter field, enter 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 Codecs

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 Gateway P20 SP supports audio transcoding through the Audio Transcoder Module (TCM). Other RADVISION 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 the RADVISION Gateway and the RADVISION 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; the reallocation 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 CODECS

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

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if it is not already selected).
2. Click the **Settings** tab.
3. Click **Media Modes**.
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 the RADVISION Gateway and the RADVISION MCU, G.728 transcoding is supported on the MCU only.

---

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.
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.

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 Gateway S40 SP.

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

1 In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2 Click the **Settings** tab.
3 Click the **Bonding** button.
4 Select the **Enable bonding** check box to enable ISDN bonding support.
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 3-8.

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 3-8 *Downspeeding Policy Operation*

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

You can assign a Quality of Service (QoS) priority level to video and voice calls using either pre-configured system settings or by creating your own settings.

Quality of Service settings involve configuring the Gateway to add a Quality of Service (QoS) DiffServ Code Point value in the IP header of outbound packets. Routers on the network that support QoS can give preferential treatment for bandwidth, latency and jitter to such coded packets and facilitate the efficient transmission of packets. You can set QoS parameters on the Gateway for voice calls, video calls or both.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **Quality of Service**.
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 DiffServ Code Point value for each media type.
   - **Custom**—Select to assign your own DiffServ Code Point 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 DiffServ Code Point value 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 DiffServ Code Point value of voice packets that the Gateway sends out. The default value is 46.
     - In the Video Priority (0-63) field, enter a whole number from 0 to 63 to set the DiffServ Code Point value 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 DiffServ Code Point value 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 DiffServ Code Point value 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

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **Alert Indications**.
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.
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.
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 click **Upload**.

Related Topics

- Gateway Event Types on page 102
- Trap Severity Enumeration on page 108

Gateway Event Types

Table 3-9 lists proprietary RADVISION SNMP trap event types for the PRI Gateway, as detailed in the RvTrapEventType textual convention.

Table 3-10 lists SNMP trap event types for the 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 3-9 *PRI Gateway SNMP Trap Event Types*

Event Type	Trap is sent when:	State	Severity
Abnormal disconnect	A call has disconnected for a reason other than normal, busy or no answer.		Warning
Authentication failure (specific)	A login attempt to the web interface fails due to incorrect user name or password.		Warning
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
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 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 failed - peer list empty	A call to a peer has failed because the peer list is empty.		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

Table 3-9 *PRI Gateway SNMP Trap Event Types (continued)*

Event Type	Trap is sent when:	State	Severity
Call to peer rejected by all listed peers	A call to a peer has been rejected by all listed peers.		Major
Card extract/Hot Swap	A blade has been removed from the RADVISION chassis under power or inserted into the chassis under power, or the when the Gateway enters maintenance mode.	TRUE	Critical
Configuration changed	A configuration change is uploaded from the web interface.		Information
Configuration exported	Configuration is exported via the web interface.		Information
Configuration imported	Configuration is imported via the web interface.		Information
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
Gatekeeper registration state change	A change occurs in the registration status of the Gateway.	TRUE	Clear
		FALSE	Minor
ISDN downspeed	ISDN downspeeding to a lower rate is taking place.		Warning
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

Table 3-9 *PRI Gateway SNMP Trap Event Types (continued)*

Event Type	Trap is sent when:	State	Severity
Incompatible sw version install	An attempt to burn a version of the Gateway software onto incompatible hardware occurs.		Warning
Loss of Ethernet	The network returns after going down. Indicates the time at which the network was restored.	TRUE	Critical
		FALSE	Clear
Loss of ISDN	A state change occurs for each enabled ISDN line.	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
Power-down	The Gateway is shutting down.		Information
Power-up	The Gateway has started to operate.		Information
RAI status	A change in RAI status occurs.	TRUE	Warning
		FALSE	Clear
Snmp request with invalid community	An SNMP request uses community values that do not match those of the Gateway.		Warning
Snmp write request	An SNMP write request is sent to the Gateway.		Information
User account locked	A user account is disabled.		Warning
User logged in	A user successfully logs in to the system via the web interface.		Information

Table 3-9 *PRI Gateway SNMP Trap Event Types (continued)*

Event Type	Trap is sent when:	State	Severity
User logged out	A user logs out of the system via the web interface.		Information

Table 3-10 *Serial Gateway SNMP Trap Event Types*

Event Type	Trap is sent when ...	State	Severity
Abnormal disconnect	A call has disconnected for a reason other than normal, busy or no answer.		Warning
Authentication failure (specific)	A login attempt to the web interface fails due to incorrect user name or password.		Warning
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
Cables mismatch	A serial cable is not appropriate for the configured serial port settings.		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 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 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
Call to peer failed - peer list empty	A call to a peer has failed because the peer list is empty.		Major

Table 3-10 *Serial Gateway SNMP Trap Event Types (continued)*

Event Type	Trap is sent when ...	State	Severity
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 to peer rejected by all listed peers	A call to a peer has been rejected by all listed peers.		Major
Card extract/Hot Swap	A blade has been removed from the RADVISION chassis under power or inserted into the chassis under power, or the when the Gateway enters maintenance mode.	TRUE	Critical
		FALSE	Clear
Configuration changed	A configuration change is uploaded from the web interface.		Information
Configuration exported	Configuration is exported via the web interface.		Information
Configuration imported	Configuration is imported via the web interface.		Information
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
Gatekeeper registration state change	A change occurs in the registration status of the Gateway.	TRUE	Clear
		FALSE	Minor
Incompatible sw version install	An attempt to burn a version of the Gateway software onto incompatible hardware occurs.		Warning
Loss of Ethernet	The network returns after going down. Indicates the time at which the network was restored.	TRUE	Critical
		FALSE	Clear

Table 3-10 *Serial Gateway SNMP Trap Event Types (continued)*

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
Power-down	The Gateway is shutting down.		Information
Power-up	The Gateway has started to operate.		Information
RAI status	A change in RAI status occurs.	TRUE	Warning
		FALSE	Clear
Snmp request with invalid community	An SNMP request uses community values that do not match those of the Gateway.		Warning
Snmp write request	An SNMP write request is sent to the Gateway.		Information
User account locked	A user account is disabled.		Warning
User logged in	A user successfully logs in to the system via the web interface.		Information
User logged out	A user logs out of the system via the web interface.		Information

TRAP SEVERITY ENUMERATION

Table 3-11 describes the proprietary RADVISION Gateway SNMP trap severity enumerations.

Table 3-11 *Proprietary* RADVISION *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

The Resources section is available in PRI Gateways 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

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **Resources**.
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.
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.

---

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

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

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

2 Click the **Settings** tab.

3 Click **Security**.

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.

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.

6. Click **Upload**.

CONFIGURING ADVANCED SETTINGS

In the Advanced section of the Settings tab, you can configure, enable, and disable various advanced Gateway settings.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **Advanced**.

   Table 3-12 explains the IP-to-ISDN (or Serial) call settings you can configure in this section.

   Table 3-13 explains the ISDN (or Serial)-to-IP call settings you can configure in this section.

   Table 3-14 explains the IP call settings you can configure in this section.

   Table 3-15 explains the ISDN call settings you can configure in this section (available in PRI Gateways only).

   Table 3-16 explains the general call settings you can configure in this section.

Table 3-12 *Advanced Settings—IP to ISDN (or Serial) Calls*

Field or Check Box	Description
Conceal caller ID (unavailable in Gateway S40 SP)	Select to cause the Gateway to hide the identifier of the calling endpoint on the IP network, regardless of whether or not the Support Presentation Restriction advanced setting is selected. The *callerID* field of the Q.931 message is sent over the ISDN network empty.
Ignore caller bearer rate and force service rate	Select to configure the Gateway to ignore the incoming call bearer rate and to use instead the bandwidth specified for the service on the Services tab to process the call. If the service bit rate is set to **Auto**, the Gateway process the call at the bearer rate. Deselect to allow an administrator to limit a specific service to a maximum bit rate. When deselected and the bearer rate is greater than the service rate, the Gateway processes the call at the service rate. When deselected and the bearer rate is lower than or equal to the service rate, the Gateway processes the call at the bearer rate. If the bearer bit rate is set to Auto, the Gateway process the call at the bearer rate.

Table 3-12 *Advanced Settings—IP to ISDN (or Serial) Calls (continued)*

Field or Check Box	Description
Auto dial voice call in case of video call fail (unavailable in Gateway S40 SP)	Select to instruct the Gateway to attempt to reconnect video calls as voice calls after a video call has failed at call setup. The Gateway uses the auto-redial mechanism for outgoing video calls when any of the ISDN disconnect reasons listed below occur. When selected, the Gateway first tries to redial the call as a restricted video call at 56 Kbps. If the call fails for any of the reasons listed below, the Gateway tries to redial the call as a voice call. When deselected, the call disconnects. The Gateway log indicates both the disconnect reason and the Gateway attempt at redialing. **Note** The auto-redial mechanism operates independently of the downspeeding functionality. The ISDN disconnect reasons are: ■ 0x12—No user responding. ■ 0x39—Bearer capacity not authorized. ■ 0x3a—Bearer capacity not presently available. ■ 0x3f—Reports a “service or option not available” event only when no other cause in the “service or option not available” class applies. ■ 0x4f—Reports a “service or option not implemented” event only when no other cause in the “service or option not implemented” class applies. ■ 0x41—Bearer capability not implemented. ■ 0x45—Requested facility not implemented. ■ 0x58—Incompatible destination.
Use default service bit rate of n kbps for services defined to use ‘auto’ bit rate	Choose the default bit rate. When using a service with the bit rate set to Auto, the Gateway uses the default bit rate if the received bearer rate is not one of the supported bit rates.

Table 3-13 *Advanced Settings—ISDN (or Serial) to IP Calls*

Field or Check Box	Description
Conceal caller ID (unavailable in Gateway S40 SP)	Select to have the Gateway hide the identifier of the calling endpoint on the ISDN network, regardless of whether or not the Support Presentation Restriction advanced setting is selected. The *callerID* field of the Q.931 message is sent over the IP network containing the string "0000."
Enable T.120 capabilities in incoming IVR and TCS4 calls	Select to enable the Gateway to send T.120 capabilities messages to the ISDN endpoint upon receiving a call at the IVR-internal or TCS4 stage. The Gateway sends the T.120 messages before connecting to the IP network endpoint.
Support sub-address at Call Setup (unavailable in Gateway S40 SP)	Sub-addressing is a one-stage Direct Inward Dialing (DID) dialing mechanism in which a phone sends two numbers. One number is for routing on the circuit switched network. The other number is forwarded to the Gateway inside a Q.931 sub-addressing information element for IP address resolution by the gatekeeper. Sub-addressing can also be used for implementing ISDN fallback when not enough bandwidth is available for routing an IP-oriented call over IP. Select for the Gateway to take the E.164 number from the Q.931information element sub-address field and forward it to the gatekeeper for address resolution. Sub-addressing requires gatekeeper support.

Table 3-14 *Advanced Settings—IP Options*

Field or Check Box	Description
Support H.323 Fast Start in voice-only call setup (unavailable in Gateway S40 SP)	The H.323 fast start functionality enables endpoints that support the feature to join a voice conference in the Gateway more quickly. Standard call setup requires four round trips of messages between endpoints before the first media stream is exchanged between peers. The set of messages includes Setup/Connect (Q.931 procedure), Master/Slave Determination (H.245 procedure), Capability Exchange (H.245) and Open Logical Channel (H.245). H.323 fast start shortens the time it takes to start a call by skipping the H.245 phase and combining the call setup procedure into a single H.225 transaction. Select to encapsulate H.245 capabilities exchange and negotiation messages within Q.931 setup messages.
Enable packet handling (may increase call delay)	Select to configure the maximum rate of jitter tolerance in the Network jitter tolerance field. Jitter occurs when IP packets sent at a steady rate reach their destination at different speeds. Streams can also split on their way to the Gateway between different routers. This can cause a “later” packet B to arrive before an “earlier” packet A, even though A was sent before B.
Network jitter tolerance	If you selected the **Enable packet handling (may increase call delay)** check box, then enter the maximum rate of jitter tolerate in milliseconds. Packet loss occurs when jitter exceeds the configured rate.

Table 3-15 *Advanced Settings—ISDN Options*

Field or Check Box	Description
Request ISDN rollover when less than n B channels are available (available in PRI Gateways only)	Select to define when the Gateway uses the ISDN rollover feature (which is defined in advanced commands—see Configuring Advanced Commands on page 121 for more information). When the total number of available B channels in both PRI ports falls below the number specified in this field, the Gateway sends a “busy out” message to the PSTN switch for each of the remaining B channels. The switch application “busies out” the remaining B channels and diverts new calls to other gateways on the network with greater available resources. This setting is only active after you configure the Gateway to use a 4ESS PRI line. For example, you specify 10 in the Request ISDN rollover when less than n B channels are available field and the number of available B channels falls to 9. The Gateway sends a “busy out” request message to the PSTN switch. The PSTN switch application routes new calls through other gateways on the network. When the total number of available B channels returns to at least 10, the Gateway sends a “busy out” cancellation message to the PSTN switch indicating the restored ability to receive calls. The PSTN switch makes the “busied out” lines available and attempts attempt to route new calls through the Gateway.

Table 3-16 *Advanced Settings—General*

Field or Check Box	Description
Restrict Gateway use to MCU conferences only	Select for the Gateway to send and receive calls to and from the MCU only. This setting, together with a scheduling server, reserves resources for scheduled conferences only.
Support Presentation Restriction (unavailable in Gateway S40 SP)	Select to enable support for the presentation restriction feature. This feature responds to an instruction from the calling endpoint to forward or to conceal the endpoint identifier.

Table 3-16 Advanced Settings—General (continued)

Field or Check Box	Description
Support H.239	Select to enable support for dual video channels using the H.239 protocol. This setting is selected by default. When selected, the Gateway supports H.239 in ISDN-to-IP calls and in IP-to-ISDN calls. The Gateway identifies the protocol version that an IP endpoint uses and sends H.239 capabilities only to those endpoints working with protocol version 4.0 or later. H.239 support has no impact on Gateway capacity. We recommend that you do not enable this feature if you establish communication with endpoints that do not support H.245 generic capabilities (endpoints based on H.323 version 2 or earlier) as this might cause the endpoints to fail upon receiving these capability exchanges.

About DTMF Settings

The SCOPIA Gateway performs Dual Tone Multi-Frequency (DTMF) detection on IP-to-ISDN calls and on ISDN-to-IP calls. The Gateway can send DTMF tone information to the IP endpoint in-band only, or both in-band and out-of-band. The Gateway sends DTMF tone information to the ISDN endpoint in-band only.

Note For Gateway P20 SP, enabling DTMF detection for video calls reduces the number of supported calls at 128 Kbps from 30 to 22 when using an E1 connection. Capacities are lower when using a T1 connection

About DTMF

The signal generated by a DTMF encoder is a direct algebraic summation, in real time, of the amplitudes of time sine (or cosine) waves of different frequencies.

An example of the use of DTMF is in touch tone telephone dialing. DTMF tones are sent out as you dial. For example, pressing “1” sends a tone created by combining frequencies of 1209 Hz and 697 Hz.

The touch tone system uses pairs of tones to represent the various keys on the telephone. A “low tone” and a “high tone” are associated with each button (0-9, *, and #). The low tones vary according to the horizontal row in which the tone button is located in Table 3-17. The high tones correspond to the vertical column in which the tone is located. The local telephone company receives each pair of tones, decodes the number dialed and makes the connection.

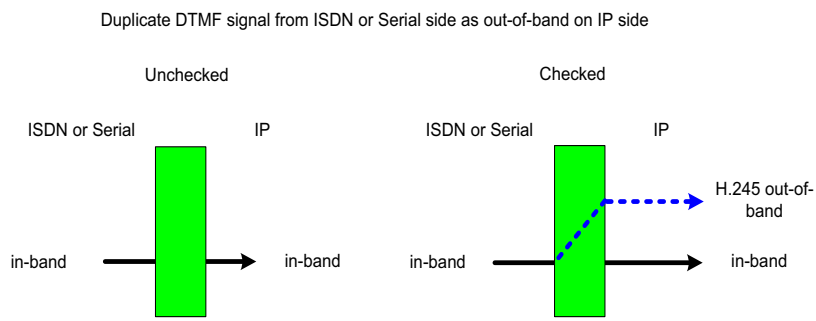
Table 3-17 *DTMF Tone Assignments*

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	ABC 2	DEF 3	A
770 Hz	GHI 4	JKL 5	MNO 6	B
852 Hz	PRS 7	TUV 8	WXY 9	C
941 Hz	*	oper 0	#	D

About DTMF Detection on IP-to-ISDN or Serial Calls

The Gateway passes incoming in-band DTMF signals to the ISDN or serial-side endpoint unchanged. In addition, you can configure the Gateway to convert H.245 out-of-band DTMF signals from the IP side to in-band signals on the ISDN or serial side. Figure 3-2 illustrates IP-to-ISDN or serial DTMF processing.

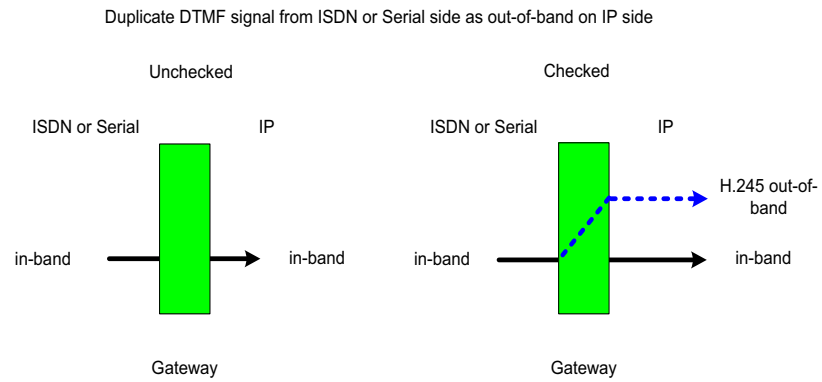
Figure 3-2 *IP-to-ISDN or Serial DTMF Processing*



About DTMF Detection on ISDN or Serial-to-IP Calls

The Gateway passes incoming in-band DTMF signals to the IP-side endpoint unchanged. In addition, you can configure the Gateway to convert in-band DTMF signals from the ISDN or serial side to H.245 out-of-band signals on the IP side. Figure 3-3 illustrates ISDN or serial-to-IP DTMF processing.

Figure 3-3 *ISDN or Serial-to-IP DTMF Processing*



Configuring DTMF Settings

You can enable DTMF detection and settings in the **Advanced** section of the **Settings** tab.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **Advanced**.
4. In the IP to ISDN Calls section of the PRI Gateway, you can select the **Translate DTMF from IP out-of-band (H.245) to ISDN in-band (G.711 only)** check box.

   In the **IP to Serial Calls** section of the Serial Gateway, you can select the **Translate DTMF from IP out-of-band (H.245) to Serial in-band (G.711 only)** check box.

   When selected, the Gateway performs the following:

   - Converts H.245 out-of-band DTMF signals coming from the H.323 IP-side endpoint to in-band signals on the ISDN side.

- Passes incoming in-band DTMF signals to the ISDN-side endpoint unchanged.

This setting is selected by default. If deselected, the Gateway passes in-band DTMF signals to the ISDN-side endpoint unchanged.

5 In the ISDN to IP Calls section of the PRI Gateway, you can select the **Duplicate DTMF signal from ISDN side as out-of-band on IP side** check box.

In the **Serial to IP Calls** section of the Serial Gateway, you can select the **Duplicate DTMF signal from Serial side as out-of-band on IP side** check box.

When selected, the Gateway performs the following:

- Converts in-band DTMF signals from the ISDN-side endpoint to out-of-band H.245 signals if the IP-side endpoint is located on an H.323 network.
- Passes incoming in-band DTMF signals to the IP-side endpoint unchanged.

This setting is selected by default. If deselected, the Gateway passes in-band DTMF signals to the IP-side endpoint unchanged. If you do select this setting, perform step 6.

6 In the Apply to field of the PRI Gateway, choose the type of calls to which ISDN-to-IP DTMF processing applies: Voice calls or Voice and video calls. Voice calls is the default setting.

Remember Enabling DTMF detection for PRI Gateway video calls reduces the number of supported calls at 128 Kbps from 30 to 22.

CONFIGURING ADVANCED COMMANDS

You can send text-based commands to the Gateway for enhanced control. You can use these advanced commands to change certain settings in real time and monitor information such as debug information. Advanced commands are not case sensitive.

Table 3-18 describes common advanced commands.

Table 3-18 *Advanced Command Settings*

Command	Description
AddService2SrcNum	Notifies the IP endpoint of the Gateway service number to which the ISDN-side endpoint has called. Parameters: disable/enable.
CallSignalPort	Notifies the gatekeeper to which the Gateway is registered on which port to communicate. Parameters: 1000 to 3000. Remarks: The number must be unique and not used for any other purpose.
DownSpeed (unavailable in Gateway S40 SP)	Instructs the Gateway to support downspeeding. Parameters: disable/enable.
EnhancedBillingForVoiceCalls (unavailable in Gateway S40 SP)	Instructs the Gateway to support the RADVISION ECS CDR *Real Connect Time* field. *Real Connect Time* indicates the actual time at which an IP-to-ISDN voice call connects to the ISDN terminal. When disabled, the ECS uses the *Connect Time* field for CDR billing purposes. *Connect Time* indicates the time at which the Connect message is sent to the source endpoint. Parameters: disable/enable. Remarks: Default value is disable. Relevant to voice calls only. Operational only when the Gateway is registered to an ECS working in Routed Mode.
ForceG711ForMcu	Instructs the Gateway to open only a G.711 channel in Gateway-to-MCU calls. Parameters: disable/enable.

Table 3-18 Advanced Command Settings (continued)

Command	Description
NotifyLevel	Changes the type and number of debug messages that are generated. Parameters: 0—Disables Gateway logs. 3 (default)—Fatal error (Gateway can no longer provide service), a problem affecting user functionality (for example, call connect failure or no resources available), or status prints for Customer Support use. 6—Debugging. 8—Extended debugging. Remarks: We recommend that you do not exceed a NotifyLevel of 6 as this might overload the system with a very large debug message output. Level 3 should be sufficient for normal usage.
Peer-to-Peer disconnect reason add	Instructs the Gateway under which circumstances to reroute a call to different peer device. Parameters: Enter a number representing the required H.323 call disconnect reason, as listed in Table 3-7.
Peer-to-Peer disconnect reason remove	Deletes the H.323 Call Disconnect Reason set by the Peer-to-Peer disconnect reason add advanced command. Parameters: ALL—Enter a number representing the required H.323 call disconnect reason, as listed in Table 3-7.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the **Settings** tab.
3. Click **Advanced**.
4. Click **Commands**.

   The Advanced Commands dialog box appears.
5. Configure an advanced command by one of the following methods:

- In the Command field, enter a command.
- In the Parameters field, enter the parameters for the command.

—or—

- In the Available commands field, select one of the advanced commands.
- In the Available parameters field, choose from one of the parameters that appears.

6 Click **Send**.

In the Response field, the Gateway indicates whether it received and executed the command. If you send an invalid command, an "Unknown Command" message appears.

About Gateway Services

Gateway services are the mechanism that allows IP network endpoints to choose the type of connection they want to establish with a terminal or telephone on a circuit-switched network. A Gateway service defines the maximum bit rate for each channel, the media content of the stream (voice or data), and the mode of the call (restricted or non-restricted).

A service prefix identifies a service. The service prefix is an identifier string that can have up to 31 characters. Valid characters are 0 to 9, pound (#), asterisk (*), or comma (,). You access a service by dialing the service prefix before the phone number of the destination. For example, 9* would be identified by the Gateway as a service prefix if you dialed 9*5673994.

Note If the Ignore caller bearer rate and force service rate setting in the Advanced section of the Settings tab is selected, a service uses the defined bit rate. If the Ignore caller bearer rate and force service rate setting is deselected, the bit rate defined in the service serves as the maximum limit for the service.

The Gateway has two types of services: default and user-defined. Default services come pre-configured on the Gateway. User-defined services are services that you can define at any time using the Gateway interface. Upon registration with a gatekeeper, the Gateway provides the gatekeeper with a list of Gateway services.

The following topics discuss how you can configure services on the Services tab:

Viewing Existing Services

The **Services** tab in the Gateway interface displays a list of currently defined services for the Gateway in a table format with the following columns and fields:

- **Prefix**—Displays the prefix that identifies the service.
- **Description**—Description of the service.
- **Call Type**—Media type of the call.
- **Bit Rate**—Total bandwidth requested for the service.
- **PRI Port 1** or **2**/Serial **Port 1** to **4**—Indicates whether or not the service is enabled for the specified port.
- **Total**—Displays the total number of services currently defined in the Gateway.

Adding or Editing Services

On the Services tab, you can add a new service or edit an existing one.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click **Services**.
3. To add a new service, click **Add**. To edit an existing service, select it and then click **Edit**.
4. In the Prefix field, enter or edit the prefix number of the service. The prefix can be up to 31 characters long. Valid characters are 0 to 9 and pound sign (#), asterisk (*), and comma (,).

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 prefix in Gateway fields.

5. In the Description field, enter or edit the description of the service (up to 31 characters in length).

6 In the Call type field, select the call type for this service: Video or Voice.

7 In the Bit rate field, select the maximum bit rate you want for this service. If you select **Auto**, the Gateway determines the ISDN or serial call rate according to the bearer capability received in the setup message from the IP network endpoint.

Note The Auto setting is for video calls only.

If the IP network endpoint has a configured bit rate that is not one of the options listed in this field, the Gateway uses the default bit rate configured in the Default Service Bit Rate field in the Advanced section of the Settings tab.

Note If the Ignore caller bearer rate and force service rate field is selected when you define a bit rate for a service, the service uses the defined bit rate. If the Ignore caller bearer rate and force service rate field is deselected, the bit rate you define serves as the maximum limit for that service.

Related Topics

- Bonding Synchronization

Bonding Synchronization

(PRI Gateways only) The Advanced dialog box enables you to configure a bonding synchronization setting for the specified service.

Procedure

1 Send the ServiceOption advanced command with a parameter of *enable to* activate the Advanced button.

For information on sending advanced commands, see Configuring Advanced Commands on page 121.

2 Click **Advanced** to configure bonding synchronization settings.

The Advanced dialog box appears.

3 In the Bonding Synchronization field, choose a bonding synchronization setting.

Note Choose **Prolong** only for endpoints that use non-standard synchronization mechanisms.

4 Click **OK** to save your setting and close the Advanced dialog box.

5 Click the **Port Specific** tab.

6 In the Enable service in ports section, select the PRI ports that are enabled for this service.

7 Click **OK**.

The Gateway interface uploads your settings to the services database.

DELETING GATEWAY SERVICES

In the **Settings** tab, you can delete existing services.

Procedure

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

2 Click the **Services** tab.

3 Select a service and click **Delete**.

Configuring Port Settings

On the PRI Port or Serial Port tabs, you can configure physical line settings for Gateway ports. The following topics discuss the settings you can configure.

Note Some configuration options are unavailable in Gateways that support only one PRI port.

Configuring Basic Port Settings

In the Basics section of the PRI Port or Serial Port tabs, you can configure basic settings for the specified port.

Note (PRI Gateways only) A frame alignment failure message will appear when you enable a port that is not in use (no cable is attached to the PRI line connector).

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the applicable PRI Port or Serial Port tab.
3. Select the **Port enabled** check box to enable this port. For PRI Gateways and Serial Gateways, if this setting is deselected, the CD LED light on the rear panel of the Gateway is disabled.
4. (PRI Gateways only) In the Port phone numbers section, choose one of the following option buttons:
   - **Single Number**—Defines a single number for this PRI port. Enter a phone number in the field.
   - **Range**—In the two fields, enter a range of numbers for this PRI line. If the line has a range of numbers, you only need to enter the digits necessary to indicate the range. For example, if the phone numbers assigned to this line are 6775380 to 6775411, enter 380-411. You can type a maximum of 31 digits in each text field.
5. (PRI Gateways only—optional) In the Local Area Code field, enter the local area code for the phone numbers. You can enter up to 16 digits.

6 (PRI Gateways only—optional) Select the **Strip Local Area Code** check box if you want the Gateway to strip local area codes for outbound calls to the ISDN network.

Note The type of line connected to this PRI port appears in the Physical standard field.

CONFIGURING PORT PHYSICAL INTERFACE SETTINGS

This section describes the available configuration options for Gateway ports.

- PRI Ports
- Serial Ports

PRI PORTS

Note This section applies only to Gateway P20 SP.

In the Physical Interface section of the PRI Port tabs, you can configure the physical line properties of the specified PRI port.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the applicable PRI Port tab.
3. Click **Physical Interface**.
4. Select the **Same as Port** check box if you want to duplicate physical interface settings from another PRI port that you choose from the field. When selected, you cannot modify any settings in this section.

Note This option is not available in Gateways that support only one PRI port.

5. In the Interface field, choose the line interface: **T1** or **E1**.
6. In the Country field, choose the nation where the ISDN service is installed.

7. In the Signaling protocol field, choose the signaling protocol used to set up and tear down the calls through the signaling (D) channel. Depending on the interface used, different signaling protocols are available.
8. In the Network access field, choose the Gateway national access type: **TE** (Terminal Equipment) or **NT** (Network Terminator) device.
9. In the Clock source field, choose the Gateway clock source:
   - **Master** (the Gateway provides the clock signal)
   - **Slave** (the Gateway receives the clock signal)
10. In the Line Build Out field, choose **Long Haul** or **Short Haul**.

Note You can configure this setting only if you select **Japan** in the Country field. Skip to step 4 otherwise.

Related Topics

- Configuring Fractional Channels
- Configuring Line Coding, Framing and Signaling Type

CONFIGURING FRACTIONAL CHANNELS

In the Physical Interface section of the PRI Port tabs, you can configure fractional channels as part of the physical line properties of the specified PRI port.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the applicable PRI Port tab.
3. Click **Physical Interface**.
4. Click **Fractional** to select fractional channels.

   The Fractional dialog box appears.
5. Select the **Fractional line** check box to enable the fractional selection of channels.

6 In the Select the channels field, define individual channels you want to use for fractional E1 or T1 distribution. The table contains 24 check boxes for T1 or 31 check boxes for E1.

Note You cannot select channel 24 of the T1 settings and channel 16 of the E1 settings. These are reserved as the signaling (D) channels that are essential for communication.

Note Click **Select All** to select all fractional channels or **Deselect All** to deselect all fractional channels.

7 Click **OK** to close the Fractional dialog box.

Configuring Line Coding, Framing and Signaling Type

In the Physical Interface section of the PRI Port tabs, you can configure coding, framing, and signaling type settings as part of the physical line properties of the specified PRI port.

Procedure

1 In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2 Click the applicable PRI Port tab.
3 Click **Physical Interface**.
4 Click **Advanced** to configure line coding, framing, and signaling type.
The Advanced dialog box appears.
5 In the Line coding field, choose the type of modulation used to encode the data.
6 In the Framing field, choose the framing and error detection method.

Note The ESF CRC6JT framing option is available only if you select **Japan** in the Country field and **Long Haul** in the Line Build Out field.

7 In the Signaling type field, choose the signaling type.

8 Click **OK** to close the Advanced dialog box.

SERIAL PORTS

This section applies only to Gateway S40 SP.

In the **Physical Interface** section of the Serial **Port** tabs, you can control the properties of the cable connected to the specified serial port. When a cable is connected to a serial port, the Gateway identifies the type of the cable and displays the information in the **Interface** and **Physical standard** fields of the **Physical Interface** section. In such cases, you cannot modify these fields. If the Gateway does not detect a connected cable, you can modify the **Interface** and **Physical standard** fields. For changes to settings in these fields to take effect, the system should be rebooted.

Gateway line cables are attached to the Gateway via a DB-60 connector that provides the serial line connection for the Gateway serial ports. The cables are Y-type with split leads at the remote end. On one side is either a V.35, RS-449, EIA-530, or EIA-530A connector. On the other side is an RS-366 connector.

Gateway terminal adapter cables have either a DTE or a DCE interface.

The Gateway can identify which type of cable has been connected to its DB-60 serial ports. Cable configuration settings are automatically displayed in the **Physical Interface** section of the **Port** tabs. The automatically configured settings are shown in Table 3-19 on page 132.

Procedure

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

2 Click the applicable Port tab.

3 Click the **Physical Interface** button.

4 In the **Interface** field, select the DTE or DCE cable interface (disabled after you have connected a cable).

The **Physical standard** field displays the type of line connected to the serial port.

5 In the **Terminal adapter** field, select the required terminal adapter type. Enabled only when **DTE** is selected in the **Interface** field. When **DCE** is selected in the **Interface** field, the **Terminal adapter** option is set to **Common** and disabled.

6. In the **Signaling protocol** field, select a signaling protocol for use in call setup from the following list:
   - **RS-366—**Carries signaling information only.
   - **Data Triggered**—Enables the Gateway to connect a call when it detects valid incoming data from an endpoint on the serial network.
   - **Manual Control**—Enables an Administrator to manually connect a call via the Gateway web user interface.

   Different signaling protocols are available depending on the interface and terminal adapter that you select, as shown in Table 3-19.

   The **Signaling protocol** field is enabled only you select **DTE** in the **Interface** field. The **Signaling protocol** field is set to **RS-366** and disabled when you select **DCE** in the **Interface** field.
7. In the **Incoming default bandwidth** field, set the rate to which the Gateway forces the bandwidth of an incoming call. Available only when **DCE** is selected in the **Interface** field.
8. (Optional) Click **Connect Call/Disconnect Call** to connect or disconnect the specified call. Available only when **Manual Control** is selected in the **Signaling protocol** field.
9. Click **Reset**.

Table 3-19 *DTE/DCE Interface Configuration Options*

Interface Selected	Terminal Adapter Options	Signaling Protocol Options
DTE	Common	RS-366, Manual Control, Data Triggered
	KG-Device	RS-366, Manual Control, Data Triggered
DCE	Common	RS-366

Related Topics

- Configuring Signal State and Loopback Control Options
- Viewing Connection Status

Configuring Signal State and Loopback Control Options

In the **Advanced** dialog box, you can configure non-standard signal state and loopback control options.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the applicable Port tab.
3. Click the **Physical Interface** button.
4. Click the **Advanced** button to configure non-standard signal state and loopback control options:
   - **Force Signal State**—Enables separate control over signals. When you uncheck a specific signal option, signaling control is defined by the standard logic of the Gateway. When you check a specific signal option, you can force the signal to the on or off state. Signals can be on all the time or off all the time.
   - **Enable Local Loopback**—Enabled for non-**KG-Device** terminal adapters only. When checked, instructs the Gateway to perform loopback locally to the specified port without the involvement of a remote entity. The Gateway raises an LL control signal to request that the DCE device moves to loopback mode.
   - **Enable Remote Loopback**—Enabled for non-**KG-Device** terminal adapters only. When checked, sends a loopback command via the specified port to an endpoint on the remote side of the serial interface. The Gateway raises an RLB control signal to request that the DCE device moves to loopback mode.

- **LOS support**—Enables LOS control over the synchronization signal towards a KG-Device. Enabled for **KG-Device** terminal adapters only. When checked, allows sending of a synchronization signal to the KG-Device if the Gateway needs to update the video image coming from the serial port.

Note When you select **DCE** in the **Interface** field, the **Advanced** button is disabled and signal state and loopback control settings are defined by the standard logic of the Gateway.

5 Click **Upload**.

VIEWING CONNECTION STATUS

In the **Connection Status** screen you can view the configured signal state and loopback control settings.

Procedure

1 In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2 Click the applicable Port tab.
3 Click the **Connection Status** button.
   - When **DTE** is selected in the **Interface** field, the **Connection Status** screen displays the signal state and loopback control settings you have configured in the **Advanced** dialog box.
   - When **DCE** is selected in the **Interface** field, the **Connection Status** screen displays the signal state and loopback control settings defined by the standard logic of the Gateway.

Note Blue lines indicate that the specified signal is on. Gray lines indicate that the specified signal is off.

Table 3-20 lists connection status and loopback control signals.

Table 3-20 Connection Status and Loopback Control Signal Descriptions

Signal	Description
CTS	Clear To Send
DSR	Data Set Ready
CI	Call Indication
DCD	Data Carrier Detected
DTR	Data Terminal Ready
RTS	Request To Send
LL	Local Loopback
RLB	Remote Loopback
DPR	Digit Present
CRQ	Call Request
ACR	Abandon Call & Retry
PND	Present Next Digit
DSC	Distant Site Connected
DLO	Data Line Occupied

About Advanced ISDN Settings for PRI Gateways

This section applies only to Gateway P20 SP.

In the Advanced ISDN section of the PRI Port tabs, you can view and configure ISDN settings for Gateway P20 SP. Table 3-21 explains the information that this tab displays.

Table 3-21 Advanced ISDN Tab Details

Column or Field	Description
Prefix	Displays the prefix of the advanced ISDN entry.

Table 3-21 Advanced ISDN Tab Details (continued)

Column or Field	Description
Description	Displays a brief description of the advanced ISDN entry.
NPI	Displays the Numbering Plan Identification (NPI) classification for the ISDN phone number.
TON	Displays the Type of Number (TON) code for the advanced ISDN entry.
NSF	Indicates whether the Network Specific Facility feature is enabled or disabled for the Advanced ISDN entry.
Max Digits	Displays the maximum number of digits allowed for outbound dialing.
DN Manipulation	Indicates whether advanced ISDN prefix number is enabled. For default prefix entries where TON is local, this field indicates whether the DN Manipulation setting is set to Append Local Area Code in the Add or Edit ISDN Information Elements dialog box (see Adding or Editing ISDN Information Elements on page 142 for more information).
Total	Displays the total number of ISDN information elements currently listed in the Gateway database.

The following topics discuss how you can configure Advanced ISDN Settings:

- About NSF Settings on page 136
- Adding or Editing ISDN Information Elements on page 142
- Deleting ISDN Information Elements on page 145

Note You can select the **Same as Port** check box and select another PRI port to duplicate advanced ISDN settings from that port. When you select this option, you cannot make any edits to the configuration settings. This option is unavailable in Gateway that support only one PRI port.

About NSF Settings

The NSF Information Element (IE) feature enables system administrators to coordinate network and service requirements with service providers. Service providers supply the information that you enter in the **NSF Configuration** dialog

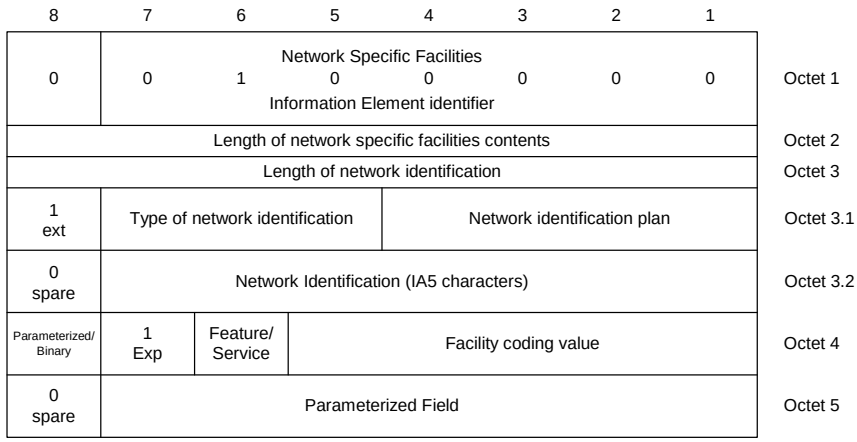
box. System administrators can either select any of the pre-configured NSF settings, or choose to configure their own NSF Information Element using service provider information.

You can specify the following information in the NSF:

- The service providers with which you want their network to work.
- The specific network plan and equipment with which you want your network to work (for example, switches and bandwidth).
- The specific services available to their network (for example,1-800 phone numbers).

Instructions are contained in the NSF IE fields of outgoing Q.931 setup messages in the format shown in Figure 3-4.

Figure 3-4 *Network Specific Facility Information Element Format*



NSF Information Elements contain a number of configurable **Octet** fields. The values entered in these fields represent instructions contained in outgoing Q.931 Setup messages. Figure 3-4 represents the format of such instructions. Table 3-22 describes the function of each of the **Octet** fields.

Table 3-22 *Octet Field Functions*

Octet	Function
Octet 3	Octet 3 represents the total number of Octet 3.X fields required for the specific information element, including the Octet 3 field itself.
Octet 3.1	Octet 3.1 is used to hold Numbering Plan Identification (NPI) and Type of Network (TON) values. The octet contains eight bits numbered from 1 to 8 and from right to left, so that Bit 1 is rightmost and Bit 8 is leftmost. The bits contain binary values representing the following functions: ■ Bits 1-4 = NPI ■ Bits 5-7 = TON ■ Bit 8 is always set to 1 when Octet 3.1 is used and populated. **Note** The **Numbering Plan Identification (NPI)** and **Type of Network (TON)** fields appear in the **Add ISDN Information Elements** dialog box The standard NPI values are: ■ For an NPI setting of Unknown, the standard integer value is 0 and the standard binary value is 0. ■ For an NPI setting of ISDN/Public, the standard integer value is 1 and the standard binary value is 0001. ■ For an NPI setting of Private, the standard integer value is 9 and the standard binary value is 1001. The standard TON values are: ■ For a TON setting of unknown, the standard integer value is 0 and the standard binary value is 0. ■ For a TON setting of International, the standard integer value is 1 and the standard binary value is 0001. ■ For a TON setting of National, the standard integer value is 2 and the standard binary value is 0010. ■ For a TON setting of Network, the standard integer value is 3 and the standard binary value is 0011. ■ For a TON setting of Local, the standard integer value is 4 and the standard binary value is 0100.

Table 3-22 *Octet Field Functions (continued)*

Octet	Function
Octet 3.2	Octet 3.2 is used to hold information including Carrier Identification Codes (CIC). A CIC is three-digit number used to access the switched services of a particular long-distance carrier from a local exchange line. All long-distance carriers, and many long-distance resellers, have their own unique CIC. One or more CIC codes are assigned to each carrier. Some examples of CIC are: ■ MCI VNET: 222 ■ AT&T Communications: 288 ■ Sprint: 333
Octet 4	Octet 4 is used to hold information representing coding values for features and services. Service providers supply the coding values. The octet contains eight bits numbered from 1 to 8 and from right to left, so that Bit 1 is rightmost and Bit 8 is leftmost. The bits contain values representing the following functions: ■ Bits 1-5=The binary Facility Coding Value for the specified feature or service. ■ Bit 6 indicates whether the facility is a feature or a service: □ 0=The requested facility is a feature. □ 1=The requested facility is a service. ■ Bit 7 is always set to 1 ■ Bit 8 indicates whether the requested facility has associated parameters or is binary: □ 0=There are parameters associated with the requested facility and they are specified in Octet 5. □ 1=The requested facility is a binary facility. There are no parameters.
Octet 5	Octet 5 is used to hold information representing coding values for parameterized facilities. The octet contains eight bits numbered from 1 to 8 and from right to left, so that Bit 1 is rightmost and Bit 8 is leftmost. The bits contain values representing the following functions: ■ Bits 1-7 represents the parameterized field coding value. ■ Bit 8 is for future use.

Table 3-23 shows Octet 4 binary facility coding values for specified features when Bit 6 is set to 0. Table 3-24 shows binary facility coding values for specified services when Bit 6 is set to 1.

.

Table 3-23 *Feature Binary Facility Coding Values*

Bits					Feature
5	**4**	**3**	**2**	**1**	
0	0	0	0	1	Calling party number preferred
0	0	0	1	0	Billing number preferred
0	0	0	1	1	Calling party number only
0	0	1	0	0	Billing number only
0	0	1	0	1	Operator
0	0	1	1	0	Pre-subscribed Common Carrier Operator
0	0	1	1	1	Reserved
0	1	0	0	1	Call-Associated Temporary Signaling Connection (TSC)
0	1	0	1	0	Notification of Call-Associated TSC clearing
0	1	0	1	1	Reserved
0	1	1	0	0	Reserved
1	0	0	0	0	Reserved

Table 3-24 *Service Binary Facility Coding Values*

Bits					Feature
5	**4**	**3**	**2**	**1**	
0	0	0	0	1	Software Defined Network (SDN). Includes Global SDN)
0	0	0	1	0	AT&T Megacom

Table 3-24 *Service Binary Facility Coding Values*

Bits					Feature
5	**4**	**3**	**2**	**1**	
0	0	0	1	1	AT&T Megacom
0	0	1	0	0	Reserved
0	0	1	0	1	Wide Area Telecommunications Service (WATS)
0	0	1	1	0	AT&T Accunet Switched Data Video Gateway (SDVG)
0	0	1	1	1	Long Distance Service
0	1	0	0	0	International 800 (1800)
0	1	0	0	1	Reserved
0	1	0	1	0	Reserved
0	1	0	1	1	Reserved
0	1	1	0	0	Reserved
1	0	0	0	0	Multiquest
1	0	0	0	1	Reserved
1	0	0	1	0	800
1	0	0	1	1	Test call
1	0	1	0	0	Inward Wide Area Telecommunications Service (INWATS)
1	0	1	0	1	SDN-K (Key Service Protection)
1	0	1	1	1	Call Redirection Service

Table 3-25 shows Octet 5 parameterized facility coding values.

Table 3-25 *Parameterized Field Binary Coding Values*

Bits							Parameterized Field
7	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	1	Alternate handling on Ring/No Answer
0	0	0	0	1	1	0	Sponsor Flexible Rating (SFR)
0	0	0	1	1	0	0	Out-of-band triggers allowed—data allowed
0	0	0	1	1	0	1	Out-of-band triggers allowed—data not allowed
0	0	0	1	1	1	0	Network Managed Data
0	0	0	1	1	1	1	Switched Data Video Gateway (SDVG) Service

Adding or Editing ISDN Information Elements

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the applicable **PRI Port** tab.
3. Click **Advanced ISDN**.
4. Click **Add** to add a new ISDN information element or select an existing one and click **Edit** to modify it.

   The Add or Edit ISDN Information Elements dialog box appears.
5. In the Prefix field, enter or edit the prefix for the ISDN information element. If you set this field to **Default**, it cannot be edited after you create the element.

6. In the Description field, enter or edit the description of the ISDN information element. If you set this field to **Default**, it cannot be edited after you create the element.
7. In the Numbering Plan Identification (NPI) field, choose an NPI code for the ISDN information element.
8. In the Type of Number (TON) field, choose a TON code for the ISDN information element.
9. In the Maximum digits send field, enter the number of digits (up to a maximum of 32) allowed for outbound dialing.
10. In the DN Manipulation field, you can configure the stripping of the ISDN information prefix number from the outbound dialed number.

    The options in this field vary according to the options set in the Prefix and Type of Number (TON) fields. Table 3-26 details the possible variations

Table 3-26 *DN Manipulation Option Variations*

Prefix Field	Type of Number (TON) Field	DN Manipulation Options
Default	Local	None, Append Local Area Code
Default	Any except Local	None
Any except Default	Any	None, Strip Prefix

You are now ready to configure your required Network Specific Facility settings (see Configuring Network Specific Facility Settings).

Configuring Network Specific Facility Settings

This section describes how to complete the procedure that you began in Adding or Editing ISDN Information Elements.

You can choose one of the pre-configured settings or choose **None** to not configure any NSF information elements. Table 3-27 lists the pre-configured settings.

Table 3-27 *Pre-configured NSF Settings*

Pre-configured Setting	Information Element (IE) Octets								
	IE 1 Octets						IE 2 Octets		
	3	3.1	3.2	3.2	3.2	4	3	4	5
AT&T Accunet	4	A1	32	38	38	E6			
AT&T Megacom	4	A1	32	38	38	E3			
AT&T Megacom 800	4	A1	32	38	38	E2			
AT&T SDDN	4	A1	32	38	38	E1			
AT&T Accunet + SDVG	4	A1	32	38	38	E6	0	49	0F
AT&T Megacom + SDVG	4	A1	32	38	38	E3	0	49	0F
AT&T Megacom 800 + SDVG	4	A1	32	38	38	E2	0	49	0F
AT&T SDDN + SDVG	4	A1	32	38	38	E1	0	49	0F
MCI VNET	4	A9	32	32	32	E1			
Sprint VPN	4	A9	33	33	33	E1			

Procedure

1. In the Network Specific Facility (NSF) field, choose **Custom**.
2. Click **Configure**.

   The NSF Configuration dialog box appears. You can configure up to four NSF information elements.

Note You can only configure the NSF information elements (NSF IEs) if you set the Interface field in the Physical Interface section of the PRI Port tabs to **T1** and set the Country field to **US**. All outgoing Q.931 setup messages will contain the NSF IE.

3 Select the **Enable** check box.

4 In the Octet 3 field, choose a value. When the value is greater than 0, that number of fields appears beneath the Octet 3 field. If this field is set to 0, the Octet 3.1 and Octets 3.2 fields are not available. If this field is set to 1, only the Octet 3.1 field is available.

5 In the Octet field(s), choose settings.

6 In the Type field, choose **Binary feature** or **Binary service** and then in the Facility Coding Value field, enter a value.

—or—

In the Type field, choose **Parameterized** and then in the Parameterized Field field, enter a value.

—or—

In the Type field, choose **Custom** and then in the Octet 4 and Octet 5 fields (if applicable), enter a value.

Note When you select **Binary feature** or **Binary service** in the Type field, the Facility Coding Value field is for Octet 4, Bits 5-1. When you select **Parameterized** in the Type field, the Parameterized Field field is for Octet 5, Bits 7-1. When you select **Custom** in the Type field, the values entered in the Octet 4 or Octet 5 fields are not subject to bit restriction.

7 Repeat step 1 for as many additional NSF information elements as necessary.

Deleting ISDN Information Elements

In the Advanced ISDN section of the PRI Port tabs, you can delete an ISDN information element.

Procedure

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

2 Click the applicable **PRI Port** tab.

3 Click **Advanced ISDN**.

4 Select an ISDN information element and click **Delete**.

CONFIGURING PORT CALL POLICIES

In the Call Policies section of the PRI Port or Serial Port tabs, you can configure the incoming call routing methods available in the Gateway for each specified port. You can define each port with different settings.

Procedure

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

2 Click the applicable PRI Port or Serial Port tab.

3 Click **Call Policies**.

4 Select the **Same as Port** check box to duplicate call policies settings from another Gateway port that you choose from the field. When selected, you cannot modify any settings in this section.

Note This option is unavailable in Gateways that support only one PRI port.

5 In the Enable inbound routing methods section, you can select incoming call routing methods in the following order of priority:

- **DID**—When selected, enables Direct Inward Dialing to an endpoint.
- **TCS4**—When selected, enables TCS4 dialing. This setting does not apply to voice calls.
- **IVR**—When selected, enables the Interactive Voice Response operator.
- **Default extension**—When selected, enables the use of the default extension number that you enter in the field.

6 (PRI Gateways only) Select the **Overlap Receiving** check box to enable overlap receiving functionality. In this functionality, the Gateway can receive consecutive digits until the dialing is complete, instead of receiving the entire phone number as a block of digits. The Gateway recognizes that an overlap receiving dialing is completed when it receives a fixed, predefined, incoming number of digits. If the Gateway receives a complete indication notification from the switch (PSTN) or a

timeout before all the digits have been dialed, the call might connect to a different address or rejected. If you select this setting, perform step 7, otherwise skip to step 8.

7. (PRI Gateways only) In the Incoming number of digits field, enter the number of digits you want the Gateway to expect during overlap receiving. The Gateway waits until this number of specified digits is received and then processes the whole number. You can enter any value up to 32.
8. (PRI Gateways only) In the Outgoing Calling Party Number field, enter a number that the Gateway automatically provides if the calling IP network endpoint does not provide a calling party number. Valid digits are 0 through 9 You can enter up to 11 digits.
9. (Serial Gateways only) In the **Display name for incoming calls** field, enter an alias for this serial port. The Gateway sends this alias to the IP endpoint in serial-to-IP calls.

Configuring Port Supported Services

In the Supported Services section of the PRI Port or Serial Port tabs, you can enable or disable specific Gateway services on each port. The Supported Services section displays the following information in table form:

- **Prefix**—Displays the prefix for this service.
- **Description**—Displays a brief description of the service.
- **Call Type**—Displays the call media type: Voice or Video.
- **Bit Rate**—Displays the maximum total bit rate allowed for this service.
- **Support**—Displays the status of the service: enabled or disabled.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. Click the applicable PRI Port or Serial Port tab.
3. Click **Supported Services**.

4 Select the **Same as Port** check box if you want to duplicate settings from another Gateway port that you choose from the field. When selected, you cannot modify any settings in this section.

Note This option is unavailable in Gateways that support only one PRI port.

5 To enable or disable a service for this port, select it and click **Enable** or **Disable**.

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 call leg.
- **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 on page 149
- Viewing Call Details on page 149
- Disconnecting Calls on page 152

Refreshing Call Information

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

Procedure

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

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
2. In the Calls tab, select a call and click **Details**.

   The Call Details window appears. Table 3-28 explains the information that this window provides.

Table 3-28 *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 Gateway S40 SP)	Displays the B channels currently in use for this call.
Resync B channels (not available in Gateway S40 SP)	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.
Encryption	"Encryption: AES 128" displays when the call leg is encrypted.
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.

Table 3-28 *Call Details Window Fields (continued)*

Field	Description
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.
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	"Encryption: AES 128" displays when the call leg is encrypted.
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

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

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway** (if not already selected).
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 3-9 for a list of PRI Gateway SNMP events. See Table 3-10 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.
- **Accumulated time of B channel usage** (PRI Gateways only)—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

On 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 (see About Gateway Services on page 123 for more information)
- Fractional B channel status (PRI Gateways only) (see Viewing B Channel Status on page 83 for more information)
- Gatekeeper IP connectivity (see Configuring IP Connectivity Settings on page 85 for more information).
- Resource allocation
- IVR (see Configuring IVR Settings on page 92 for more information)

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

Saving Configuration Settings

You can save 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 Gateway unit or to configure a similar 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

1. In the Gateway interface, on the sidebar, click **Board**.
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.

---

3. Click **Upload** to save these settings.
4. On the sidebar, click **Gateway**.
5. Make sure that the settings on the Status, Settings, PRI or Serial Ports, Calls, Event Log and Statistics tabs are correct.
6. Click **Upload** to save these settings.
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.

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 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 Gateway unit or to configure another Gateway unit.

Procedure

1. In the Gateway interface, on the sidebar, click **Gateway**.
2. On the toolbar, click **Import**.

   The Import a Configuration File page appears.
3. Click **Browse**.

   The Choose file dialog box appears.
4. Navigate to and select the configuration file you want to import.

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

---

5. Click **Open**.

   The file path appears in the File Name field.
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.

---

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

Note Uploading the file resets the device.

4

USING THE SCOPIA GATEWAY

This section provides sample scenarios for using the SCOPIA Gateway with configuration details and dialing examples, including the following:

- About Dialing Out to the ISDN Network via the Gateway
- About Dialing In to the IP Network via the Gateway

ABOUT DIALING OUT TO THE ISDN NETWORK VIA THE GATEWAY

This section describes how to dial between IP and ISDN networks using the Gateway.

Note References to the ISDN network refer also to the serial side of the Serial Gateway. The references to B-channels refer also to the equivalent bandwidth for the Serial Gateway. To obtain the actual serial call rate, multiply the number of channels by 64 Kbps (56 Kbps for restricted calls).

When you dial out from an IP network to an ISDN network, you dial a service prefix followed by a string that usually includes the destination area code, the destination phone number and any required extra characters such as an asterisk (*), pound sign (#) or delimiter. The service prefix indicates that the call is to go through the Gateway, and also indicates the properties of the call such as the call type or bandwidth requirements.

About Gateway Service Prefixes

Gateway services define different call types and bandwidths for IP network endpoints. The services are identified by service prefixes. The network administrator in charge of the H.323 network is responsible for defining services and informing users of available services. See About Gateway Services on page 123 for more information.

Note A service prefix should not be the same as the first digits of an IP endpoint phone number.

Dialing Example 1: Voice calls (PRI Gateway and Serial Gateway only)

The number string 912015294300 is a voice call from an IP network terminal to an H.323 endpoint on another IP network or to a terminal on the ISDN network. This number string consists of:

- 9—The service prefix for a voice call.
- 12015294300—The destination phone number including the area code.

Dialing Example 2: Voice calls with the auto bit-rate setting service (PRI Gateway and Serial Gateway only)

The number string 712015294300 is a voice call from an IP network terminal to an H.323 endpoint on another IP network or to a terminal on the ISDN network using a service with the bit rate setting of auto. This number string consists of:

- 7—The auto bit-rate setting service prefix for a voice call.
- 12015294300—The destination phone number including the area code.

The bit rate of the call is fixed according to the setting in the source IP network terminal.

Dialing Example 3: 1B video calls

The number string 821816455318 is a 1B video call from an IP network terminal to an H.323 endpoint on another IP network or to a terminal on the ISDN network. This number string consists of:

- 82—The service prefix for a 1B video call.
- 1816455318—The destination phone number including the area code.

About Second Number Delimiters

Note Second number delimiters are available in PRI Gateways only.

To dial an outgoing 2B call, you dial the service prefix for 1B calls and the two B channel phone numbers. Because some H.323 endpoints do not support dialing long number strings or two phone numbers, you can use a delimiter to indicate to the Gateway the end of one number and the beginning of the other. See Configuring Outgoing Call Delimiters on page 94 for more information.

Dialing Example 4: 2B video calls

The number string 821816455318* is a 2B video call from an IP network terminal to an H.323 endpoint on another IP network or to a terminal on the ISDN network. Both B channels have the same number. This number string consists of:

- 82—The service prefix for a 2B video call.
- 1816455318—The destination phone number including the area code.
- *—The second number delimiter. The second number delimiter tells the Gateway to dial the destination phone number a second time.

Dialing Example 5: 2B video calls

The number string 821816455318*1816455319 is a 2B video call from an IP network terminal to an H.323 endpoint on another IP network or to a terminal on the ISDN network. The B channels have different numbers (or your endpoint does not have two phone number fields). This number string consists of:

- 82—The service prefix for a 2B video call.
- 1816455318—The destination phone number including the area code.
- *—The second number delimiter.
- 1816455319—The second B channel number including the area code.

Dialing Example 6: 6B bonded high quality video calls

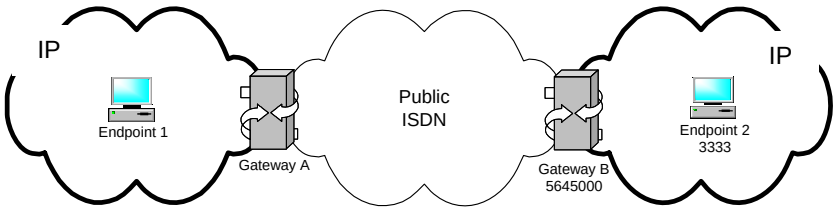
The number string 867455001 is a 6B bonded high quality video call from an IP network terminal to an ISDN network terminal. This number string consists of:

- 86—The service prefix for 6B bonded calls.
- 7455001—The phone number of the destination terminal.

Dialing Example 7: IP-ISDN-IP direct dialing—Gateway supports TCS4

The number string 9825645000^3333 is a call from an IP network endpoint (Endpoint 1) to an IP network endpoint in another zone (Endpoint 2), through a public ISDN network, as shown in Figure 4-1. Gateway A dials using TCS4, while Gateway B is set to receive calls in TCS4 mode.

Figure 4-1 *TCS4 Dialing*



This number string consists of:

- 9—The voice call service prefix in Gateway A in Zone A.
- 82—The service prefix for a 2B video call in Gateway A in Zone A.
- 5645000—The number of the destination Gateway B on the public ISDN network.
- ^—The TCS4 delimiter configured in Gateway A.
- 3333—The E.164 number of the destination IP Endpoint 2.

About Dialing In to the IP Network via the Gateway

The Gateway is responsible for routing incoming calls to the requested H.323 endpoints on the IP network.

When a terminal or phone on the ISDN network wants to reach an IP endpoint, it has to dial at least one of the phone numbers assigned to the ISDN line connected to the Gateway PRI ISDN port.

About Incoming Call Routing

When a call originating on the ISDN or serial network reaches the Gateway, the Gateway routes it to an IP network endpoint. This is achieved through one of several incoming call routing methods that the Gateway supports. You can enable any number of routing methods for each port, but at least one method must be enabled for incoming calls to be routed through that port. The Gateway routes an incoming call from the ISDN or serial network according to the routing methods enabled for the ISDN or serial port, following this order of priority: DID –>TCS4 –>IVR–>Default Extension.

If a routing method fails, the Gateway automatically tries to route the call through the next routing method in line. If all methods fail, the call is rejected. The call might also be rejected if the Gateway routes the call to an endpoint that is busy or not available.

Table 4-1 explains the routing methods.

Table 4-1 *Routing Methods*

Routing Method	Explanation
DID	The Gateway supports two forms of DID (Direct Inward Dialing): Multiple Subscriber Network (MSN) and sub-addressing. ■ MSN—The telephone company assigns a group of phone numbers to a particular ISDN line by the telephone company. PRI ISDN lines are usually assigned multiple numbers in the US and in Europe. When MSN is used, an ISDN terminal or phone can dial directly to an IP network endpoint. The call is still routed through the Gateway but the Gateway is transparent to the person dialing from an ISDN terminal. An H.323 endpoint on the IP network registers with the gatekeeper using one of the MSN numbers. When an ISDN terminal dials the MSN number, the call routes through the Gateway ISDN port connected to the line with the MSN service to the endpoint that registered using the requested number. ■ Sub-addressing (PRI Gateways only)—Sub-addressing is a one-stage DID dialing mechanism in which a phone sends two numbers. One number is for routing on the circuit switched network. The other number is forwarded to the Gateway inside a Q.931 sub-addressing information element for IP address resolution by the gatekeeper. Sub-addressing can also be used for implementing ISDN fallback when not enough bandwidth is available for routing an IP-oriented call over IP. Implementing ISDN fallback requires the support of the gatekeeper.

Table 4-1 *Routing Methods (continued)*

Routing Method	Explanation
TCS4	TCS4 is a special routing method for incoming H.320 video calls. TCS4 allows direct inward dialing to an endpoint on the IP network through the Gateway when DID is not available. H.323 endpoints on the IP network register with the gatekeeper using extension numbers. When an ISDN terminal dials one of the Gateway phone numbers followed by a TCS4 extension, the call is routed directly to the corresponding IP endpoint registered with that extension.
IVR	IVR (Interactive Voice Response) is a widely deployed automated call answering system that responds with a voice menu allowing you to make choices for routing the call. The Gateway can operate with its own internal IVR or an external IVR located in another device. When an incoming call activates the IVR system, it initiates an interactive session with the caller. The caller directs the call to its destination endpoint by responding with the dialer to prompts from the IVR system. If the caller appropriately enters the destination endpoint phone number, the IVR connects the caller to the requested IP network endpoint. Otherwise, the call can be forwarded to an operator. The IVR call transfer is enabled by a proprietary mechanism that the Gateway uses to transfer a call from one IP network endpoint to another. The Gateway supports call transfer for incoming calls from the ISDN network to an IP network endpoint whether you are using the RADVISION gatekeeper or a third-party gatekeeper. The Gateway internal IVR can handle up to 30 simultaneous incoming calls. With the Gateway, you can define an endpoint on the IP network as an IVR operator (see Configuring IVR Settings on page 92 for more information). This provides an alternative if the requested destination endpoint is not available.
Default Extension	Any endpoint on the IP network can be defined as a default destination for calls using the default extension number (including the Gateway prefix plus the H.320 or PSTN phone number) that is registered with the gatekeeper. All calls not routed through one of the above incoming call routing methods are forwarded to this endpoint.

About the IVR Operator

You can define an IP network endpoint as an IVR operator and configure the Gateway ports accordingly. See Configuring IVR Settings on page 92 for more information.

Dialing Example 8: Direct dialing to an IP network endpoint (Gateway supports DID)

The number string 5645001 is a call from an ISDN network terminal to an IP network endpoint. This number string consists of:

- 5645001—The destination endpoint phone number.

The call is routed to the requested endpoint according to its registration identity in the gatekeeper.

Dialing Example 9: Direct dialing to an IP network endpoint (Gateway supports TCS4 but not DID)

The number string 5645000^5776 is a call from an ISDN terminal to an IP network endpoint. The dialing endpoint must also support TCS4. This number string consists of:

- 5645000—The Gateway phone number.
- ^—The TCS4 delimiter of the dialing endpoint (if required).
- 5776—The extension number of the requested endpoint.

Note TCS4 only routes H.320 video calls.

About Dialing through the IVR

When the Gateway does not support DID or TCS4, you can reach an endpoint using the Interactive Voice Response (IVR) routing mechanism.

When IVR is enabled, you are answered by a recorded message prompting you to enter the destination endpoint phone number followed by the pound (#) sign. If you enter the number of an endpoint that is online and currently not busy, the IVR connects the call to the requested endpoint.

Dialing Example 10: Dialing to an IP network endpoint through the IVR

The number string 5645000 <wait for the IVR to respond> 5561# is a call through an IVR routing mechanism. This number string consists of:

- 5645000—The Gateway phone number.
- 5561—The number of the requested endpoint.
- #—This is required by the IVR for call completion.

About Dialing Indirectly through an Operator

If you do not dial the number of a destination endpoint when requested to do so by the IVR, the IVR automatically passes you to an operator. You can define any endpoint on the IP network as the IVR operator (see Configuring IVR Settings on page 92 for more information).

When IVR is enabled, you are answered by a recorded message prompting you to enter the destination endpoint phone number. If you do not know the destination endpoint number, the IVR routes the call from the Gateway using ISDN to the IP network endpoint that is defined as the IVR operator.

Dialing Example 11: Dialing to an IP network endpoint through an operator

The number string 5645000 <wait for the IVR to respond>* is a call to an IP network through an IVR operator. This number string consists of:

- 5645000—The Gateway phone number.
- *—This character is optional.

5

TROUBLESHOOTING THE SCOPIA GATEWAY

This section covers problems you might encounter when configuring, operating and managing the SCOPIA Gatewayand provides suggested actions you can perform to solve the problems.

This section describes the following topics:

Checking Your Gateway Environment

This section describes how to verify that your system status is operational and whether or not the Gateway is registered to a gatekeeper.

Verification Steps

- Check the Status screen in the Gateway, and table of endpoints in the gatekeeper.
- Check that the Gateway PRI/BRI synchronization is correct (the CD LED is green on the Gateway board).
- Check the ISDN connectivity to the public ISDN switch or the PBX/PABX.
  - Verify at Gateway > Board (or Device) > LED Monitoring that the far/near (red/yellow) LEDs are off. If they are on, contact the ISDN provider.
  - (Serial Gateways only) Verify that the Serial cables are properly connected to the RTM.
- Check that the Gateway LAN interface is working at 100Mb/Full Duplex. If not, hard code it on both sides (switch and Gateway) to 100Mb/Full Duplex and restart both devices.

Checking Your LAN Environment

This section describes how to verify that your LAN network connection is operating correctly.

Verification Steps

- Check that your H.323 entities are properly registered to the gatekeeper.
- Make a call between two LAN endpoints and verify the video and audio quality.
- Verify that the LAN interface performance is satisfactory (no packet loss, jitter or delay issues occur). Check with the network administrator if necessary.

Checking Your ISDN Environment

This section describes how to verify that your ISDN network connection is operating correctly.

Verification Steps
■ Check that the video endpoint is ISDN enabled and has ISDN lines connected and properly configured for bonding calls. ■ Make an ISDN-to-ISDN call and verify the video and audio quality. ■ At Gateway > Port verify that all necessary ISDN ports are enabled. ■ At Gateway > Board (or Device) > LED Monitoring verify that the CD LED is steady green. If it is off, check the ISDN physical layer setting. ■ At Gateway > Port > Physical Interface confirm proper country selection, signaling protocol and network access settings (TE is most commonly used). ■ Some Central Switches/PBXs/PABXs require Double Framing or Extended CRC4 framing. At Gateway > Port > Physical Interface > Advanced confirm proper framing selection.

Resolving IP-to-ISDN Call Failure

This section describes what to do if IP-to-ISDN calls fail to connect.

Possible Causes	Verification Steps
The Gateway is not registered to the gatekeeper.	■ Verify at Gateway > Settings > IP Connectivity that the Gateway is in Using gatekeeper mode and not in Peer-to-Peer mode. ■ Verify at Gateway > Settings > IP Connectivity that the gatekeeper IP address is correct. ■ When using more than one Gateway, verify that each Gateway has a unique registration name.
The LAN endpoint dialed the wrong Gateway access prefix.	Confirm that the correct Gateway service prefix is used.
The H.320 endpoint is unavailable or busy, or there is an ISDN connection problem.	Make a direct video call to the ISDN endpoint from another ISDN endpoint to identify whether the source of the problem is the ISDN endpoint or the Gateway.

Possible Causes	Verification Steps
The LAN endpoint made the call while set to ISDN call mode, instead of LAN call mode.	Change the endpoint dialer to LAN mode and try calling again.
The ECS table of services does not include the Gateway services because the Gateway is set to H.323 version 1 mode registration	■ At Gateway > Settings > IP Connectivity set the Gateway registration mode to Version 2 and try to make the call again, –or– ■ Add the Gateway services manually to the ECS table of services.
The ECS is set not to accept calls.	Set the ECS to accept calls at ECS > Settings > Calls.
The Gateway service is a substring of an ECS service, endpoint E.164 number, or MCU service.	Check the ECS table of endpoints. ■ Look for an E.164 number that begins with the specified service prefix. ■ Double click each network MCU, and look for a service that begins with the specified service prefix.
The ISDN endpoint does not support the call bandwidth.	Check the ISDN endpoint supported bandwidth. Dial again with an appropriate bandwidth.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

Resolving ISDN-to-IP Call Failure

This section describes what to do if ISDN-to-IP calls fail to connect.

Note In this section we assume that the LAN endpoint is an H.323 endpoint.

Possible Causes	Verification Steps
The LAN endpoint does not appear in the gatekeeper list of registered H.323 endpoints.	Make sure that the LAN endpoint is properly registered with the gatekeeper, and make the call again.
ISDN Central Switch/PBX/PABX call routing problem.	■ Open a Telnet connection to the Gateway. ■ Make an ISDN-to-IP call. ■ Verify whether the call reaches the Gateway. ■ If the call does not reach the Gateway, ask the ISDN provider to check the ISDN Central Switch/PBX/PABX call routing rules.
The Gateway DID option is checked but there is no endpoint with such a DID number on the LAN.	■ Check that a LAN endpoint with the same DID number is registered with the gatekeeper. ■ Check the Gateway log and make sure that the ISDN network delivered the correct Called Party Number to the Gateway. ■ You may need to redefine the LAN endpoint E.164 number accordingly (sometimes the ISDN network is set to deliver only the last 3-5 digits). ■ Make a call to another properly registered endpoint to see if the source of the problem is the Gateway or the endpoints.

Possible Causes	Verification Steps
The Gateway TCS4 option is checked and the dialing delimiter is not a legal TCS4 delimiter.	■ Ensure that the initiating endpoint uses the correct TCS4 delimiter (see the endpoint users guide). ■ Verify that the endpoint you are using supports TCS4.
The Gateway IVR option is checked but there is no endpoint with such an E.164 number on the LAN.	■ Check that a LAN endpoint with the same E.164 number that you dialed during the IVR phase is registered with the gatekeeper. ■ You may need to register the LAN endpoint to the gatekeeper with a correct E.164 number. ■ Check that the ISDN endpoint DTMF generation works properly: ■ Open a Telnet connection to the Gateway. ■ Make a call to the Gateway IVR. ■ Dial the E.164 number using DTMF tones. ■ Check the Telnet log for correct DTMF digit detection. ■ Make a call to another properly registered endpoint.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

RESOLVING PEER-TO-PEER CALL FAILURE

This section describes what to do if peer-to-peer calls (both IP-to-ISDN and ISDN-to-IP calls) fail to connect.

Note In this section we assume that the LAN endpoint is an H.323 endpoint.

Possible Causes	Verification Steps
One of the peers does not exist.	Check that the peer is configured in the peer list at Gateway > Settings> IP Connectivity.
Ports configuration mismatch.	In the peer list at Gateway > Settings> IP Connectivity, check that: ■ The LAN endpoint is configured with the correct signaling port number. ■ The Gateway Q.931 port is identical to the port configured in the Gateway (using the Advanced Commands).
The wrong dial plan is in use—the destination number does not begin with a Gateway service.	Change the destination number.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

Resolving Intermittent Call Failure

This section describes what to do if calls intermittently fail to connect.

Possible Causes	Verification Steps
PRI/E1 line is fractional.	Check with the PRI line provider if the PRI/E1 line is a fractional line (Economy PRI/E1 in the UK). If so, At Gateway > Port > Physical Interface set the Fractional button to use the correct channels only.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

Resolving IP Video Quality Issues

This section describes what to do if you encounter poor video quality on the IP endpoint on your LAN.

Possible Causes	Verification Steps
The LAN port of the unit is not synchronized with the LAN switch.	Hard code both the Gateway and the switch to 100Mb/Full Duplex at Gateway > Board (or Device) > Addressing > Port settings
Call rate problem.	■ In LAN-to-ISDN calls, verify that you are using the correct service prefix set with correct bit rate in the Gateway. ■ In Gateway > Settings > Advanced, verify that the Ignore bearer rate and force service rate option setting is not the cause.
Packet loss and packet reordering, re-transmission, jitter or delay.	Verify that the LAN interface performance is satisfactory (no packet loss, jitter or delay issues occur). Check with the network administrator if necessary.

Possible Causes	Verification Steps
The LAN network is suffering from massive packet loss.	At Gateway > Settings > Advanced, verify that Enable packet handling is checked, and increase the value of the Network jitter tolerance parameter if necessary.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log. ■ Gateway media recording. ■ Ethereal trace of the Gateway.

RESOLVING ISDN VIDEO QUALITY ISSUES

This section describes what to do if you encounter poor video quality on the ISDN endpoint.

Possible Causes	Verification Steps
The ISDN connection is not stable, and the orange/yellow panel LEDs are steady or flickering.	■ Call your operator for help. ■ Check your PABX.
ISDN endpoint problem.	Make a call to other ISDN endpoints (from the same vendor and from different vendors). If the video quality is good, there may be an interoperability problem with the specific endpoint.
LAN endpoint problem.	Make a call from another LAN endpoint. If the video quality on the ISDN endpoint is good, the problem lies with the LAN endpoint you are calling from.
LAN problems.	Make a LAN-to-LAN call and verify that the LAN interface performance is satisfactory (no packet loss, jitter or delay issues occur). Check with the network administrator if necessary.

Possible Causes	Verification Steps
Video bit rate sent from the LAN side is too low.	Check the LAN endpoint bearer capabilities/call rate settings for the LAN-to-ISDN call.
ISDN Downspeeding occurs due to dropped ISDN lines.	If the problem recurs, check with the ISDN provider at both ends of the connection.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

RESOLVING VIDEO CHANNEL ISSUES

This section describes what to do if video channels fail to open on the ISDN or LAN endpoint.

Possible Causes	Verification Steps
The LAN endpoint or ISDN endpoint does not support the required video codecs.	At Gateway > Calls> Details check that the video channels are open to the ISDN and to the LAN side.
Some of the media modes in the Gateway configuration are disabled.	At Gateway > Settings > Media Modes verify that all the relevant video codecs are checked.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

RESOLVING DTMF ISSUES

This section describes what to do if DTMF is not operating correctly.

Possible Causes	Verification Steps
DTMF is not enabled in the Gateway.	IP-to-ISDN calls ■ At Gateway > Settings > Advanced verify that Translate DTMF signal from IP Out-of-band (H.245) to ISDN in-band (ISDN G.711 only) is checked. ■ If this is a video call, verify that this option is checked for both voice and video calls. ISDN-to-IP calls ■ At Gateway > Settings > Advanced verify that Duplicate DTMF Signal from ISDN side as Out of band on IP side is checked.
The Gateway does not properly identify DTMF tones.	Open a Telnet connection to the Gateway and verify that you see the DTMFs in the Gateway log. If not, verify that the ISDN endpoint generates the DTMF tones.
An incorrect audio codec is used.	Verify that the G.711 audio codec is used in the call is G.711 (the Gateway supports DTMF detection for G.711 only). If another audio codec is used, force the call to G.711 mode by disabling all the audio media modes at Gateway > Settings > Media Modes.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

RESOLVING CALLER ID ISSUES

This section describes what to do if an incorrect caller ID is used in IP-to-ISDN calls.

Possible Causes	Verification Steps
The calling LAN endpoint is set in the ECS to use a fixed Calling Party Number.	Delete the LAN endpoint line from the ECS Endpoints table and let it register again.
The ECS is set to use a fixed Calling Party Number.	At ECS > Settings > Advanced uncheck Use Fixed Calling Party Number.
If the problem is not resolved, contact RADVISION Customer Support.	Provide the following information to RADVISION Customer Support: ■ Gateway traces with level 6. ■ H.323 stack log.

6

USING THE RADVISION AUDIO MESSAGE UTILITY FOR IVR MESSAGING

This section describes the RADVISION Audio Message Utility, and includes the following topics:

INTRODUCTION

The RADVISION Audio Message Utility is an interactive GUI that enables you to record and replace messages and upload new messages to the call routing mechanisms in RADVISION devices.

Default built-in messages are in English. The RADVISION Audio Message Utility allows you to record new messages in a different language or with different content to suit your requirements. The RADVISION Audio Message Utility also enables you to replace and upload new messages to the target RADVISION device.

There are two ways of using the RADVISION Audio Message Utility. The standard utility functions enable you to play, record or replace messages. The Express Setup guides you through the recording, replacing and upload procedure for each message.

Before You Begin

Before you can record, play and upload messages to the target RADVISION device, you must

- Save recorded messages as WAV files.
- Know the IP address of the target device.

ABOUT GATEWAY CALL ROUTING

The RADVISION Audio Message Utility provides audio messages for the call routing mechanism in RADVISION Gateways. The call routing mechanism initiates a series of voice messages that allow you to make choices and respond via the keypad through dial tones (DTMF).

The routing mechanism enables you to dial through the RADVISION Gateway to an IP network-based H.323/SIP/RTSP terminal when you do not know the extension number of the destination terminal.

Launching the RADVISION Audio Message Utility

This section describes how to install and launch the RADVISION Audio Message Utility.

Procedure

1 Copy the Audio Message Utility folder from the RADVISION Utilities and Documentation CD-ROM to your local computer.

Note You cannot run the Audio Message Utility from the RADVISION Utilities and Documentation CD-ROM.

2 To run the utility, double-click the *IvrRecordingUtility.exe* file.

Playing a Message

This section describes how to play an audio message. Available messages depend upon the device selected in the **Target Type** field.

- Gateway Messages

Note The devices available in the **Target Type** drop-down list vary according to the RADVISION devices included in your installation.

Procedure

1 In the **Target Type** field, choose the device that uses the message you want to play.

Note The options available in the **Target Type** drop-down list vary according to the RADVISION devices included in your installation.

The **Audio Recordings** window displays the messages currently uploaded to the target device.

2 Ensure the message type you wish to play is enabled in the **Audio Recordings** window.

3 Click on the message type you wish to play in the **Audio Recordings** window.

4 From the **Message** menu, select **Play Message**.

The **Play Recording** dialog box appears. You can stop or replay the message you have selected to play.

GATEWAY MESSAGES

The following Gateway messages are available.

Table 6-1 *Gateway Audio Messages*

ID	Message Name	Recorded Message	Played when ...
0	Opening Sound	Sound.	the call connects
1	Welcome	Thank you for calling. If you know your party's extension, please dial the number, followed by the pound sign now. To speak to an operator, please press star.	the call connects after the opening sound
2	Transfer to extension	Thank you, please hold.	you dial an extension after the welcome message
3	Transfer to operator	Please hold. Your call is being transferred to an operator.	you press * after the welcome message
4	Busy	The number you have dialed is busy.	the dialed extension is busy
5	No answer	No answer from this extension.	there is no answer from the dialed extension
6	Unreachable	The number you have dialed is unreachable.	the dialed extension is unreachable
7	Disconnecting	Could not connect your call. Disconnecting.	the transfer to the operator or the default extension fails.

Table 6-1 *Gateway Audio Messages*

ID	Message Name	Recorded Message	Played when ...
8	Please dial a number	Dial a number followed by the pound sign. To speak to an operator, press star.	an attempt to connect to an extension fails (busy, no answer or unreachable). The user is allowed to dial the extension number again.
9	Transfer to default extension	Please hold.	the call is being transferred to the default extension.

RECORDING A MESSAGE

This section describes how to record a new audio message.

Note There is no limit on the length of individual message files, but the total length of all WAV files should not exceed 250 seconds. An FLS file should not exceed 2000 KB.

Procedure

1. From the **Message** menu, select **New Recording**.

   The **New Recording** confirmation box appears and the MSsound recording utility is invoked.

Note MSsound is invoked by default. You can use any recording software that supports the WAV format.

   The new message must be recorded in the following formats:

   - WAV file
   - G.711 (CCITT)
   - µ-Law
   - 8-bit
   - Sampling rate 8kHz

2. Use the recording software, to record a new message and save it to the RADVISION Audio Message Utility directory.

REPLACING A MESSAGE

This section describes how to replace an audio message.

Procedure

1. In the **Target Type** field, choose the device that uses the message you want to replace.

Note The options available in the **Target Type** drop-down list vary according to the RADVISION devices included in your installation.

---

2. The **Audio Recordings** window displays the messages currently uploaded to the target device. Click the message type in the **Audio Recordings** window you wish to replace.
3. From the **Message** menu, select **Properties**.

   The **Properties** dialog box appears showing the name of the message you selected in the **Message Type** field.
4. (Optional) Enter the text that you want to appear in the **Message Type** field in the **Audio Recordings** window.
5. In the **Video message** field, enter video message text.
6. Click **Browse** to choose the audio message file you wish to use.

   The **Replace Recording** dialog box appears.
7. Select the file with which you wish to replace the current message and click **Open** to confirm your selection.
8. Click **OK** in the **Properties** dialog box.
9. The new message appears in the **Audio Recordings** window.

UPLOADING A MESSAGE TO A DEVICE

This section describes how to upload audio messages from the Audio Message Utility to a target device.

Procedure

1. From the **Actions** menu, select **Upload Messages To Target**.

   The **Upload** dialog box appears.
2. In the **General Information** section, enter the IP address of the target device.
3. In the **Login Information** section, enter the user name and password of the target device, as configured in the device network configuration settings.
4. (Optional) Modify the read and write community settings for the target device as follows:
   - Click **Customize SNMP Settings**.

     The **Customize SNMP Settings** dialog box displays.
   - Enter the required read community and write community values and click **OK**.

   The default read and write community settings are RVGET2 and RVSET2 respectively.
5. Click **Upload Messages**.

   The **Upload in progress** window appears, and the message files are uploaded and burned onto the target device.

Viewing Message Details

You can view the file name and length of the audio messages listed in the **Audio Recordings** window.

Procedure

1. Click the **Target Type** drop-down list.
2. Choose the device that uses the message you want to replace.

Note The options available in the **Target Type** drop-down list vary according to the RADVISION devices included in your installation.

The names of audio message files currently uploaded to the target device appear in the **Recorded Message** field of the **Audio Recordings** window.

The lengths of audio message files currently uploaded to the target device appear in the **Message Length (sec)** field of the **Audio Recordings** window.

Exiting the Utility

This section describes how to exit the Audio Message Utility.

Procedure

1. Open the **Actions** menu.
2. Select **Exit**.

About Express Setup

The Express Setup is an alternative way of recording, replacing and uploading messages. The Express Setup guides you through the recording, replacing and uploading procedure for each audio message.

You proceed through the Express Setup sequentially for each message type. You are alternately prompted to select to record a new message and to navigate a path to a new message file with which you wish to replace a current file.

As you proceed through the Express Setup, the dialog box displays the name the current message type and the associated message file.

Note You can skip the recording and replacing sequence for each message by clicking **Next** at each step in the Express Setup. You can return to any step in the procedure to change the setup for a particular message by clicking **Back**.

Using Express Setup

This section describes how to use the Express Setup.

Procedure

1. Click **Express Setup** in the **Tools** menu.

   The **Express Setup** dialog box is displayed informing you of the name of the first message file in the selection and provides a check box for indicating whether you wish to create a new recording for the message.

2. Check **Create a new recording** and click **Next**.

   The **Express Setup** dialog box displays the required format settings for the new message and the MSsound recorder is displayed. Use the MSsound recorder or other recording software to record the new message and save it to the Audio Message Utility directory.

3. When you have finished recording a new message, click **Next**.

   The **Express Setup** dialog box displays the path of the current file for the specified message type and the **Replace** button.

4. Click **Replace**.

   The **Replace Recording** window appears showing the directory containing the current sound files for the device.

5 Select the required file and click **Open** to replace this file with the current message file for the specified message.

When you have completed the recording and replacement procedure, the **Express Setup** dialog box displays the new list of message types and message files associated with each type.

6 Click **Upload**.

The **Upload** dialog box appears.

7 Type the IP address of the target device.

8 Type the user name and password as defined in the network configuration settings of the RADVISION device.

9 Click **Upload Messages** to complete the upload procedure.

The **Upload in progress** window displays. The message files are uploaded and burned onto the target device.

7

USING THE RADVISION SOFTWARE UPGRADE UTILITY

This section describes the RADVISION Software Upgrade Utility, and includes the following topics:

INTRODUCTION

The RADVISION Software Upgrade Utility is an interactive GUI interface that enables you to upgrade RADVISION software installed on RADVISION devices.

The RADVISION Software Upgrade Utility enables you to select files to be uploaded via a network or modem connection to the RADVISION device. You can select either to perform a typical upgrade which includes all the new files or a customized upgrade which enables you to select which files to upload.

The upgrade files are uploaded and then burned into the memory of the RADVISION device.

Before You Begin

RADVISION devices automatically save configuration settings before a software upgrade takes place. However, it is recommended that you save all configuration information using the Export button in the RADVISION device web interface toolbar. You can retrieve all these settings after the software upgrade is complete by using the Import button in the RADVISION device web interface toolbar.

LAUNCHING THE UTILITY

This section describes how to install and launch the RADVISION Software Upgrade Utility.

Procedure

1. Download the UpgradeUtility.exe file from the RADVISION Utilities and Documentation CD-ROM.
2. Double click the UpgradeUtility.exe file to run the Software Upgrade Utility.

   The upgrade files are extracted and the **Upgrade Utility** dialog box appears.

UPGRADING SOFTWARE

This section describes how to use the Software Upgrade Utility to upgrade RADVISION software installed on RADVISION devices.

Procedure

1. In the **General Information** section of the **Upgrade Utility** dialog box, enter the IP address of the device you want to upgrade.
2. In the **Login Information** section, enter the administrator user name and password for the target device, as configured in the device network configuration settings.
3. (Optional) Modify the read and write community settings for the target device as follows:
   - Click **Customize SNMP Settings**.

     The **Customize SNMP Settings** dialog box displays.
   - Enter the required read community and write community values.

   The default read and write community settings are RVGET2 and RVSET2 respectively.

Note We recommend that you modify the default settings for security purposes.

- Click **OK** to return to the **Upgrade Utility** dialog box.

4 (Optional) Select the components of the target device you want to upgrade as follows:

- Click **Customize**.

  The **Customize** dialog box appears.

- Check the device components you want to upgrade in the **Select the components you want to upgrade** list.

Note The components displayed vary according to the RADVISION device upgraded.

- Click **OK** to return to the **Upgrade Utility** dialog box.

5 Click **Upgrade** to upgrade all components of the RADVISION device software (or only those components you manually selected via the **Customize** option).

The RADVISION Software Upgrade Utility informs you whether or not the upgrade is successful.

Note When the upgrade is complete, the RADVISION device automatically resets itself and starts operation with the new software version.

INDEX

D

M

N

O

P

Q

R

S

T

U

V

W