Media Gateway 3200

H.248 User's Manual

Version SN09

Document # LTRT-72704 Rev 007

Contents

List of Figures

List of Tables

Reader's Notes

Introductory Matter

Note: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the **CTRL** and ¬ keys.

Notice

This User's Manual describes the installation and use of the MG 3200.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, Nortel cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered Technical Support customers at http://www.nortel.com under Support / Product Documentation.

Date Published: May 19, 2005 Date Printed: October 2, 2006

Trademarks

All other products or trademarks are property of their respective owners.

Customer Support

Customer technical support and service are provided by Nortel's Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from Nortel, contact mailto:support@nortel.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual. Hexadecimal notation is indicated by 0x preceding the number.

Related Documentation

The Nortel documentation package contains the following publications:

- **MG 3200 User's Manual** (this manual) - contains the boards' physical description, installation instructions, standard control protocols and management protocols description and general features of the board which are not control protocol specific (for example various networking issues)
- **LTRT-72904 MG 3200 Configuration Guide**
- **LTRT-73805 MG 3200 H.248-SIP Fast Track Installation Guide**

1 Overview of the MG 3200

The MG 3200 is the cost-effective, entry-level, market-ready, standards-compliant media server systems. Intelligently packaged in a 1U chassis, especially designed for small-scale deployments and smaller locations in the packet network, the MG 3200 is the correct solution size for small-scale needs. Incorporating best-of-breed Voice over Packet technology and based on field proven media technology, the MG 3200 enables Service Providers (SPs) rapid time-to-market and reliable cost-effective deployments of enhanced voice services in VoIP telephony networks. This compact device, is designed to be installed either as a desktop unit or installed in a 19-inch rack.

The MG 3200 contains the TP-1610 cPCI VoIP communication board, an ideal building block for deploying high-density, high availability Voice over IP (VoIP) enterprise systems.

The MG 3200 supports a broad selection of voice processing related algorithms, including G.711, G.723.1, and G.729A Vocoders, G.168-2002 compliant echo cancelation, T.38 real-time Fax over IP, a wide selection of In-band and Out-of-band tone detection and generation, as well as signaling protocol support, including ISDN PRI, SigTran (M2UA, IUA) and CAS.

The MG 3200 is suitable for VoIP gateways, IP-enabled call centers, large Telcos and next generation DLCs. Offering integrated voice gateway functionality capable of delivering up to 480 simultaneous calls, the MG 3200 supports all necessary functions for voice and fax streaming over IP networks.

The MG 3200 incorporates up to 8 or 16 E1, T1 or J1 spans for connection, either directly to PSTN telephony trunks, or to an enterprise PBX, and two 10/100 Base-TX Ethernet ports for redundant connection to the LAN.

Two packet processors handle packet-streaming functions through two redundant integral 10/100 Base-TX interfaces. Each processor implements the industry-standard RTP/RTCP packet-streaming protocol, advanced adaptive jitter buffer management, and T.38 fax relay over IP. An E1/T1 trunk interface module is provided for 16-T1, or 16-E1, or 16-J1 trunks, allowing for full gateway streaming functions in a single cPCI slot.

The TP-1610 board complies with industry-standard network control protocols including H.248. These protocols allow for the implementation of a distributed Media Gateway and media server architecture that separates call processing functions from media processing functions, resulting in better redundancy, scalability and higher system availability.

Enabling accelerated design cycles with higher density and reduced costs, the MG 3200 is an ideal building block for scalable, reliable VoIP solutions. With the MG 3200's comprehensive feature set, customers can quickly design a wide range of solutions for PSTN and VoIP networks.

1.1 General Features

The MG 3200 has the following features:

- Vocoder configuration options:
  - PCM/ADPCM, G.711, G.723, G.723.1, and G.729A

Note 1: G.729A and G.723 should not be used simultaneously on the same board.

Note 2: G.728 coder can be supported. For additional information, contact your Nortel representative.

- Up to 16 E1/T1 digital spans
- Independent vocoder selection per channel
- Extensive media processing functions
- RTP stream multiple destination connection (i.e. to TDM, other RTP channels and PCI channels (for recording))
- Packet telephony standard compliant
- PSTN protocol termination support
- Open architecture
- Flexible deployment and multiple density options
- NEBS Level 3 compliant
- Superior, high quality VoIP calls and FoIP transmissions
- Interchangeable IP/RTP or PSTN Endpoints
- VoIP packet streaming (RTP/ RTCP) per RFC 1889/1890
- Real-time Fax over IP/T.38 with superior performance (round trip delay of up to 9 sec)
- Integral Announcement support towards PSTN/TDM and IP
- IP to IP Mediation capabilities
- IP to IP Transcoding (G.711 to and from LBR)
- Tone detection and generation (MF, DTMF, RFC 2833)
- Packet interface: Dual 10/100 Base-TX link ports (for redundancy) or cPSB back plane (PICMG 2.16) interface
- G.168-2002 compliant Echo Cancelation with a 32, 64* or 128* msec tail
  (* May reduce channel density)
- Silence Suppression supporting VAD (Voice Activity Detection) and CNG (Comfort Noise Generation)
- Automatic Fax Bypass modes
- DTMF detection and generation according to TIA 464B

- DTMF Relay according RFC 2833
- PSTN Signaling: CAS, ISDN PRI
- Transport of SS7 signaling, with the use of SigTran; MTP-3 and higher layer messages are relayed using M2UA via SCTP over IP
- MFC-R2 and Call Progress Tone detection and generation
- PICMG 2.1 for Hot-swap support
- cPSB (PICMG 2.16) support
- Rear Transition Module (RTM)
- PICMG 2.5 for H.110 support
- Management Interfaces: SNMP V2, Embedded Web Server
- Compact, rugged 19-inch rack mount unit, 1U high (1.75" or 44.5 mm), with two compactPCI™ (cPCI) slots
- Optional dual redundant AC or single non-redundant DC power supplies

1.2 TP-1610 Software Overview

The MG 3200 software supports the following Protocols:

1.2.1 Call Control Protocols

- **H.248 Protocol** - H.248 is a standards-based network control protocol (based on the IETF's RFC 3015 and ITU-T: H.248). Since this is a standards-based control protocol, no special software library is provided. Users can choose from many such stacks that are generally available in the market to construct their own Call Agent. For more information, refer to "H.248 (Media Gateway Control) Protocol" on page 87.

1.2.2 Management Protocols

The MG 3200 software supports the following Management Protocols:

- **SNMP** - Refer to "Using SNMP" on page 123
- **Embedded Web Server** - Refer to "Embedded Web Server" on page 141
- **Telnet** - Refer to "Command Shell" on page 211

1.3 MG 3200 Applications

The MG 3200 can be used in a variety of applications, which exploit its unique advantages regarding compressing PCM voice channels to IP packets according to ITU and IETF standards.

Examples include:

- Next Generation Switches
- IP Services Platforms
- VoIP Access Gateways
- Carrier Grade Trunking Gateways
- IP-enabled Call Centers
- Cable Telephony Gateways

1.3.1 Available Configurations

The MG 3200 is offered in a variety of channel densities and rear I/O options. Most of the descriptions and illustrations in this manual refer to the full capacity board.

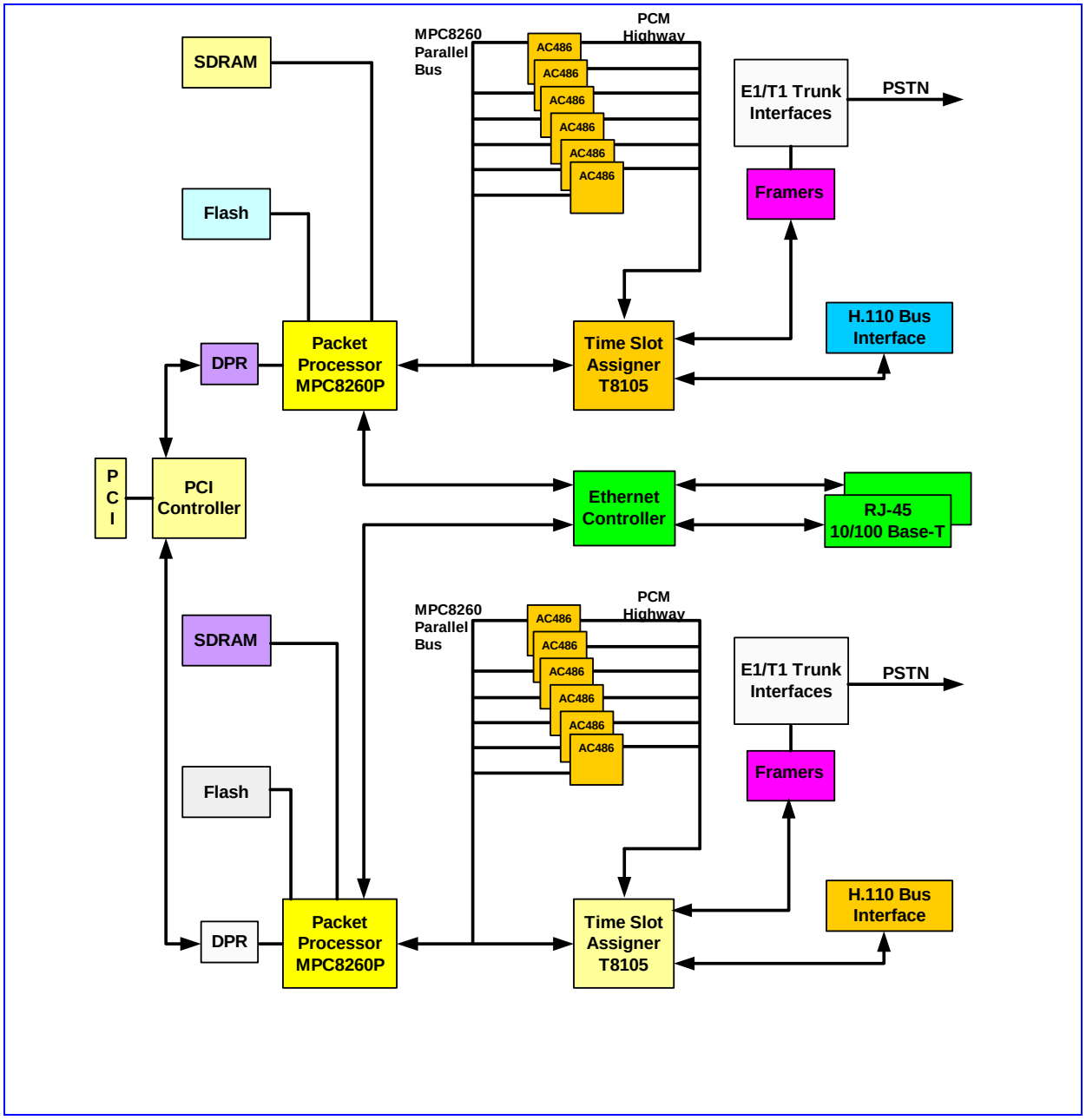
1.4 Benefits

- IP-enabled, cost-effective technology
- Low to high channel density, high performance board
- Concurrent toll quality voice and fax support
- Wide range of PSTN signaling protocols
- Fast time-to-market
- Flexible and easy migration to VoIP networks
- Extensive VoIP experience accumulated by Nortel
- All-in-one integrated board - Reduced inventory
- Scalable distributed architectures
- Shorter development cycle

1.5 Functional Block Diagram

The figure below illustrates the functionality of the TP-1610 board.

Figure 1-1:1610 Functional Block Diagram

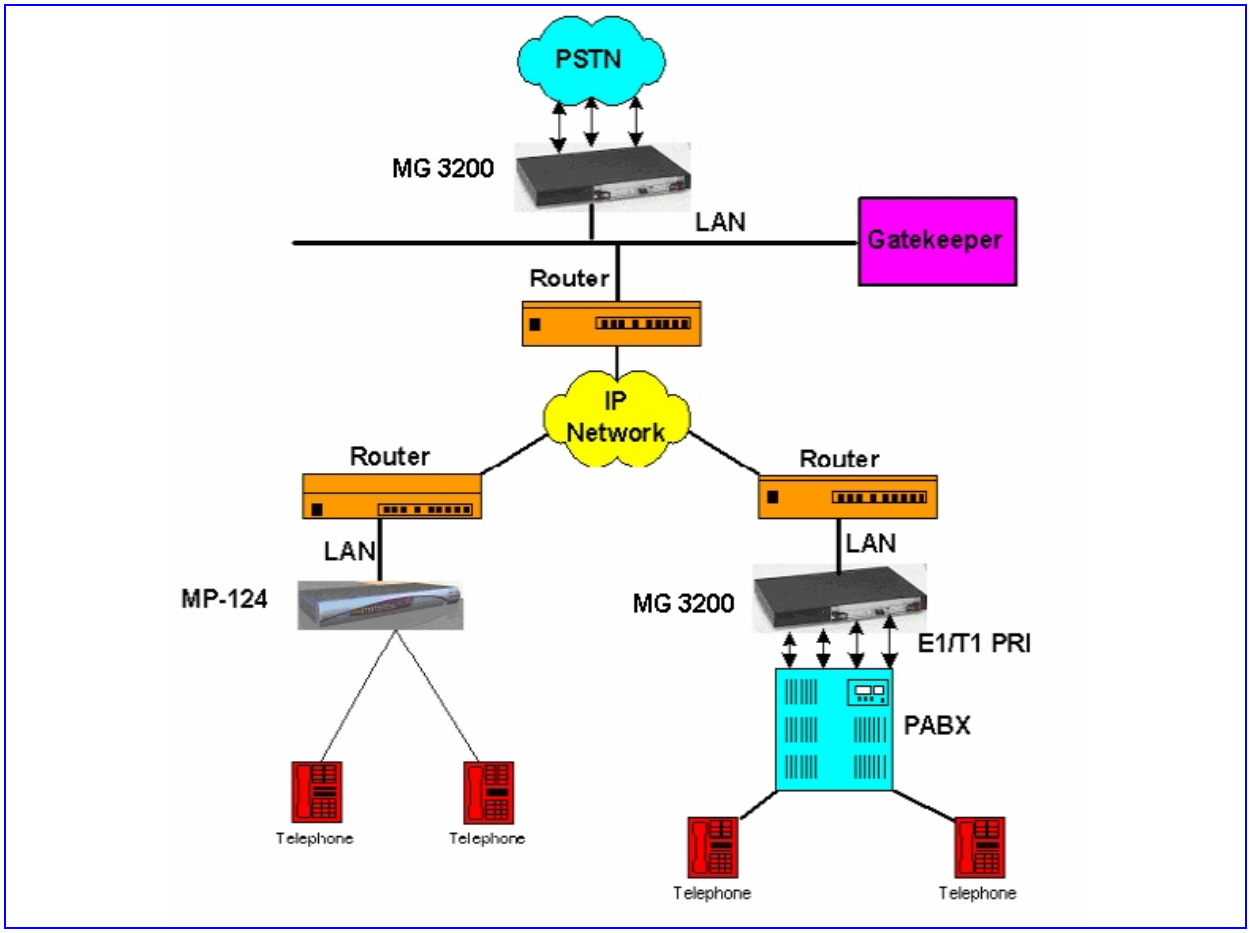


Note: The H.110 Bus Interface is not applicable to the MG 3200.

1.6 Typical Application Diagram

The diagram below illustrates a typical wireline application.

Figure 1-2: Typical MG 3200 Wireline Application



2 Hardware Equipment

This section provides details about the hardware equipment for the MG 3200. This section also describes the MG 3200's hardware features and details the various LED functions.

The MG 3200 includes:

- 1U 19 inch chassis
- 1 TP-1610 board
- 1 TP-1610 Rear Transition Module (RTM)

2.1 The MG 3200 Chassis

The MG 3200 Media Gateway is comprised of a 19-inch 1U chassis with a dual 110/220 VAC power supply or a -48 VDC power supply. The MG 3200 is populated by a single compactPCI™ board, the TP-1610, and its Rear Transition Module (either up to, 8-span or 16-span) on which both PSTN trunks and the Ethernet interface are located.

The MG 3200 chassis' front cage, slot #1 - the lower slot, houses the TP-1610.

The MG 3200 chassis' rear cage, slot #1 - the lower slot, houses the TP-1610 RTM.

2.1.1 MG 3200 Diagram

Figure 2-1: MG 3200 Front View

The MG 3200 can be provided with the 1-Span, 2-Span, 4-Span, 8-Span or 16-Span RTMs

Figure 3-9 'Rear View with Connected Cables (8 Spans and DC)' on page 41 shows the MG 3200 chassis populated with the 8-span RTM. Figure 3-8 'Rear View with Connected Cables (16 Spans and Dual AC)' on page 40 shows the MG 3200 chassis populated with the 16-span RTM (featuring 2 Telco connectors and 2 RJ-45 connectors).

The physical difference between the 1-Span, 2-Span and 4-Span RTMs, and the 8-span RTM is that the RJ-48c ports are depopulated correspondingly.

2.1.2 Chassis LED Indicators

The table below details the LED indicators on the front panel of the chassis.

Table 2-1:Chassis Indicators

Placement	Color	Function
Right side of front panel	**Green**	Power is on
Right side of front panel	**Red**	Fan failure - indicates that any of the internal fans has significantly reduced its speed or has frozen
Left side of front panel	**Red**	Power supply failure - indicates that one of the two AC redundant power supplies is faulty (This LED is not relevant when there is a single AC connection only.)

2.2 The TP-1610 Board

The TP-1610 Board is the main component of the MG 3200. It is supplied within the MG 3200 Gateway.

The TP-1610 board panel is shown in the figure below. The section, "TP-1610 Board Panel LED Indicators" on page 29 provides details about the LED indicators and additional information.

The MG 3200 may be supplied with two types of TP-1610 RTM panels:

- TP-1610 RTM panel with two 50-pin Telco female connectors, shown in the figure, "1610 RTM - with Telco Connectors" below.
- TP-1610 RTM panel options for up to eight RJ-48c connectors, shown in the section,' 'TP-1610 RTM Panel Diagrams" on page 28.

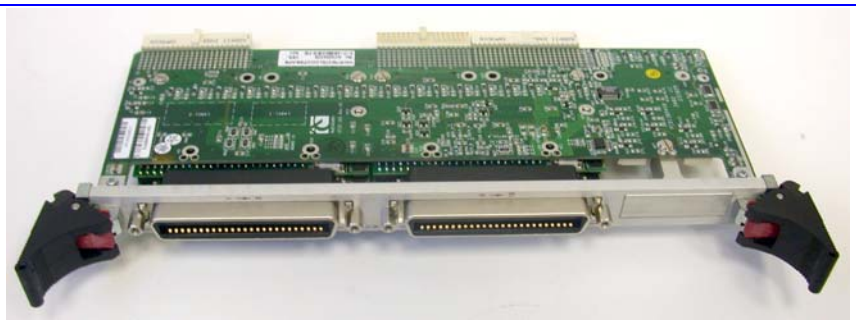
  Consult an Nortel representative for more information on the available configurations.

The figure below displays the TP-1610 board.

Figure 2-2: 1610 Board

The figure below illustrates the TP-1610 board's corresponding Rear Transition Module (RTM) with 50-Pin Telco Connectors.

Figure 2-3: 1610 RTM - with Telco Connectors



2.2.1 Board Hot-Swap Support

The TP-1610 board is hot swappable and can therefore be removed from a slot (and inserted into a slot) when the cPCI system is under power.

Figure 2-4: 1610 Board, Panel View

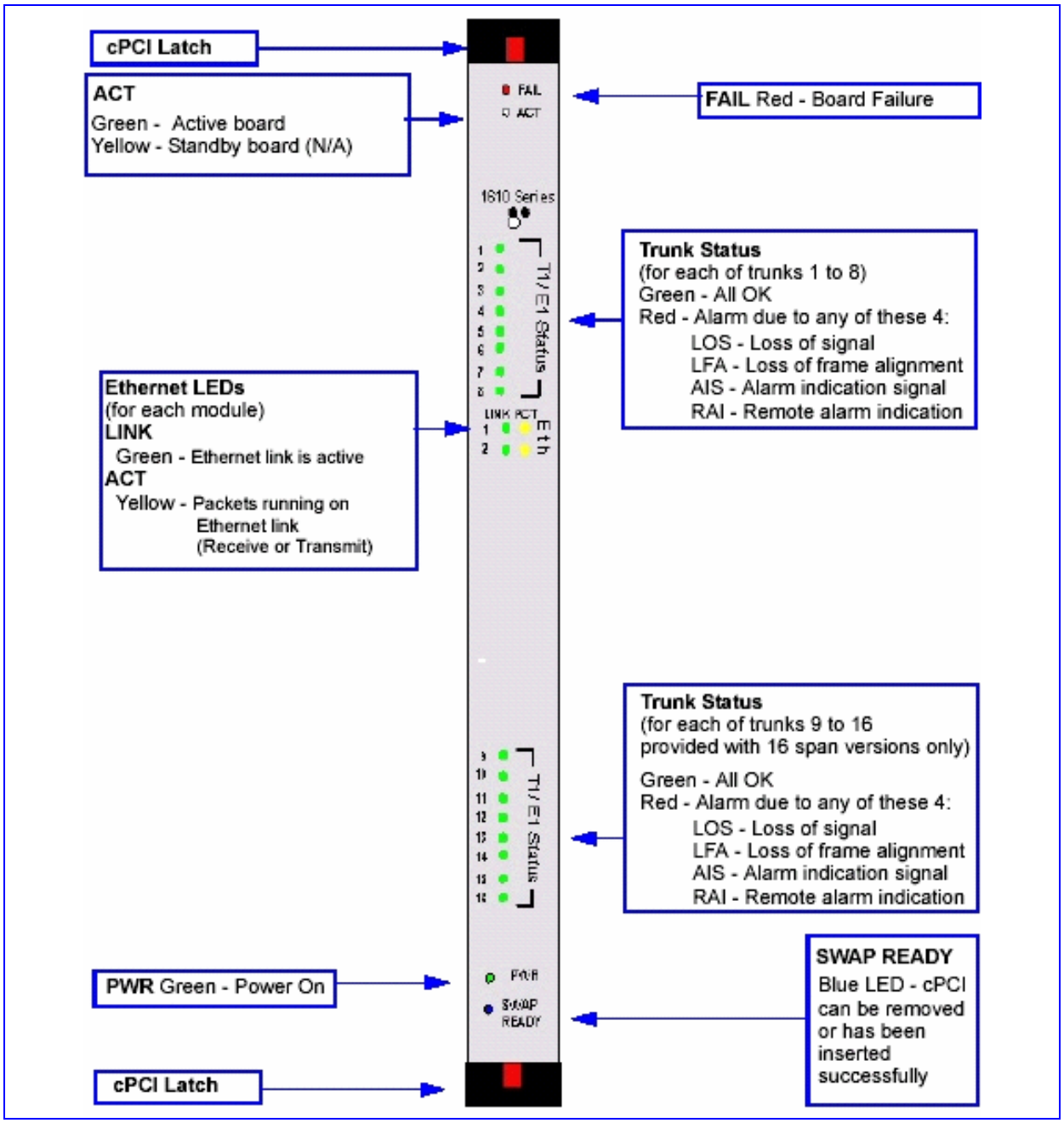


Figure 2-5: 1610 RTM Panel with 2 Telco Connectors

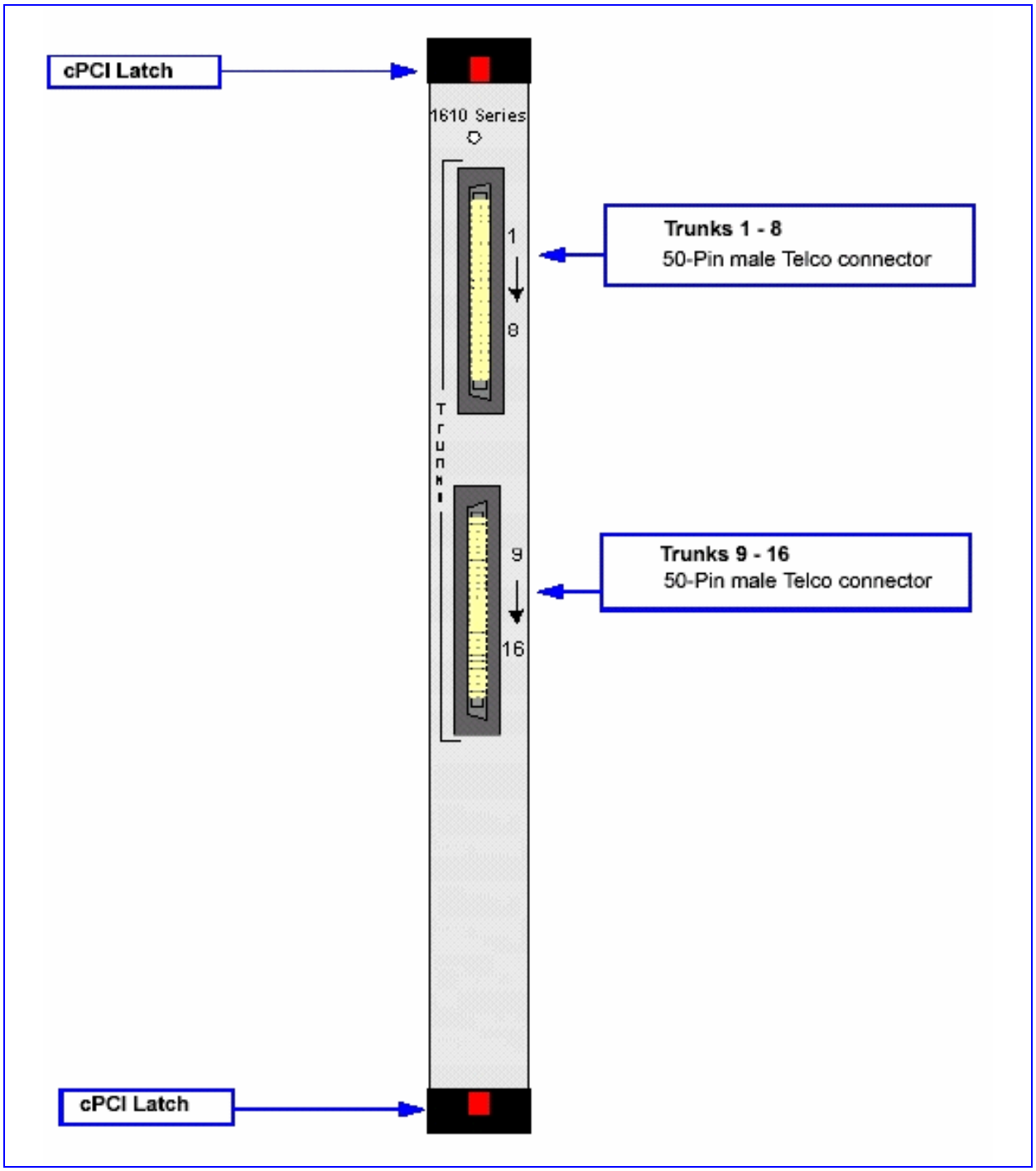
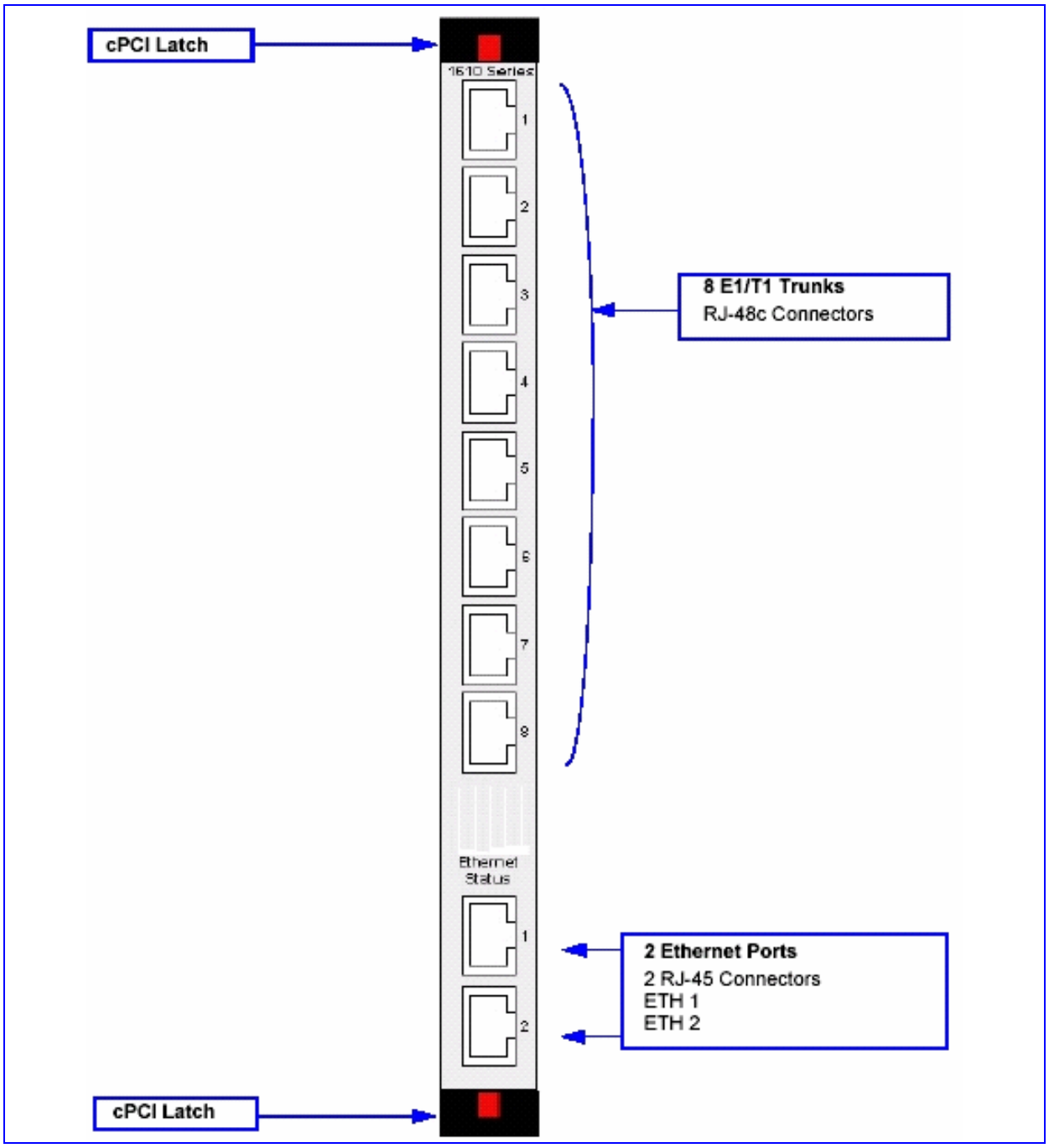


Figure 2-6: RTM Panel with 8 RJ-48c Trunk Connectors



2.3 TP-1610 Board Panel LED Indicators

The tables below provide the LED indicator definitions

.

Table 2-2: Board Status LED Indicators

Label	Color	Function	
FAIL	Red	Normally OFF; Red indicates board failure (fatal error)	
ACT	Green	Board initialization sequence terminated OK	Bi-color indicator
	Yellow	N/A	

The FAIL LED is normally OFF, and illuminates Red to indicate board failure.

The ACT LED illuminates Green as soon as download is completed successfully.

Table 2-3: Trunk Status LED Indicators

Label	Color	Signal Description	
Trunk Status 1 to 8 Trunk Status 9 to 16	Green	Trunk is synchronized (normal operation)	Bi-color indicator
	Red	Loss due to one of the following 4 signals:	
	LOS	Loss of Signal	
	LFA	Loss of Frame Alignment	
	AIS	Alarm Indication Signal (the blue alarm)	
	RAI	Remote Alarm Indication (the yellow alarm)	

During normal operation, the E1/T1 bi-color LED illuminates Green for each trunk. Any other condition, either in the E1/T1 cable, in the MG 3200, or on the remote side, causes the E1/T1 bi-color LED to light up Red, indicating a loss due to any of the 4 signals listed and described in the table below.

Table 2-4: Ethernet LED Indicators

Label	Color	Function
LINK	**Green**	Link all OK
ACT	**Yellow**	Transmit/Receive Activity

Table 2-5: Auxiliary LED Indicators

Label	Color	Function
PWR	Green	Power is supplied to the board
SWAP READY	Blue	The cPCI board can now be removed. Refer to Note 1.
		The cPCI board was inserted successfully. Refer to Note 2.

Note 1: Before removing the board, wait for the blue LED to flash ON and then stay OFF.

Note 2: When inserting the board into the system, if the board has any abnormal physical or electrical condition, the blue LED illuminates ON, indicating a fault. If the board is **NOT** powered up, the blue LED is not lit.

Note 3: When using the board with a host-supported standard cPCI chassis, the blue LED functionality is dependent on the host software.

Note 4: For more information of board replacement, refer to "Board Replacement" on page 41.

3 Hardware Installation

This section describes the installation procedures for the MG 3200 board system, as well as board replacement procedures. The MG 3200 can be installed either as a desktop system or as a chassis in a standard 19-inch rack.

There are no DIP switches to be set.

Warning

The MG 3200 is supplied as a sealed unit and must only be serviced by qualified service personnel.

Electrical Earthing

Prior to installation of any board in a chassis, always correctly connect the chassis to a safety earth according to the laws and regulations of the country in which the installation is performed.

Electrical Component Sensitivity

Electronic components on printed circuit boards are extremely sensitive to static electricity. Normal amounts of static electricity generated by clothing can damage electronic equipment. To reduce the risk of damage due to electrostatic discharge when installing or servicing electronic equipment, it is recommended that anti-static earthing straps and mats be used.

➢ To install the MG 3200 take these 3 steps:

1. Unpack the MG 3200 (refer to 'Unpacking' below).
2. Mount the MG 3200 (refer to 'Mounting the MG 3200').
3. Cable the MG 3200 (refer to 'Cabling the MG 3200').

3.1 Unpacking

➢ To unpack the MG 3200 take these 6 steps:

1. Open the carton and remove the packing materials.
2. Remove the MG 3200 from the carton.
3. Check that there is no equipment damage.
4. Check, retain and process any documents.
5. Notify Nortel of any damage or discrepancies.
6. Retain any diskettes or CDs.

3.1.1 Package Contents

Ensure that the MG 3200 package includes the following items (in addition to the device):

- For the dual AC power supply version of the MG 3200, two AC power cables are supplied.
- For the DC power supply version, one connectorized DC power cable (crimp connection type) and one DC adaptor (screw connection type) connected to the rear panel of the MG 3200, - use only one type.
- CD (software and documentation).
- Small plastic bag containing (refer to the figure below):
  - Two brackets and four bracket-to-device screws for 19-inch rack installation option.
  - Four non-slip pads for desktop / shelf installation option.

Figure 3-1: Plastic Bag Contents

3.2 Mounting the MG 3200

The MG 3200 can be mounted on a desktop, or installed in a standard 19-inch rack. Refer to 'Cabling the MG 3200‘ on page 35 for the cabling procedures.

The figure below shows the front view of the MG 3200 media gateway. For information on the MG 3200 LEDs refer to 'Chassis LED Indicators' on page 24 and 'TP-1610 Board Panel LED Indicators' on page 29.

Figure 3-2: MG 3200 Front Panel

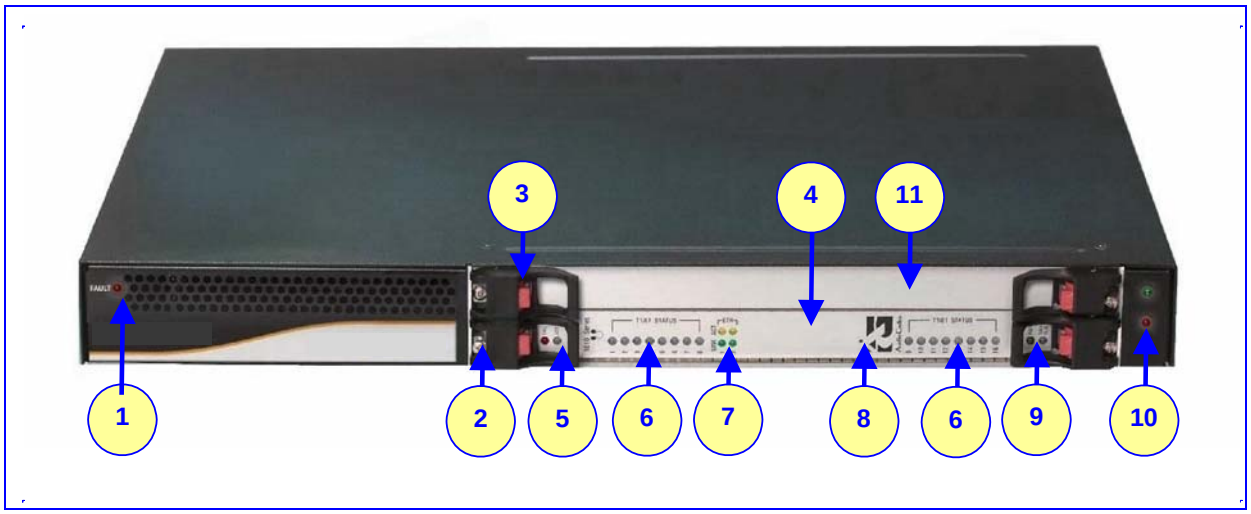


Table 3-1: MG 3200 Front View Component Descriptions

Item #	Label	Component Description
1	FAULT	Dual AC Power LED
2		cPCI board locking screws
3		cPCI latches
4		TP-1610 cPCI board, 16-trunk configuration
5		Status LED Indicators
6	T1/E1 STATUS	E1/T1 Trunk Status LED Indicators
7	ETH	Ethernet LED Indicators
8		Reset button
9		cPCI LED Indicators
10		Power and Fan LEDs
11		An available cPCI slot for an optional third-party CPU board

3.2.1 Mounting a MG 3200 in a 19-inch Rack

Users can mount the device on a standard 19-inch rack shelf preinstalled in the rack (preferred method), or by attaching the device directly to the rack's frame using the 2 brackets and screws supplied.

Rack Mount Safety Instructions (UL)

Note: When mounting the chassis on a rack, be sure to implement the following Safety instructions:

- Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- Maintain Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation on the equipment is not compromised.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips.)

Before rack mounting the chassis, attach the two (supplied) brackets to the front sides of the device. Note that there is an option for two additional brackets to attach the rear sides of the device to the rack.

➢ To attach the two supplied brackets to the front sides of the device, take these 3 steps:

1. Remove the 2 screws nearest the front panel on either side of the device.
2. Align a bracket over 2 holes on one side (so that the bracket's larger holes face front) and with the 2 supplied replacement screws, screw in the bracket.
3. Perform the same procedure on the other side.

➢ To attach the device directly to a 19-inch rack's frame take these 3 steps:

1. Position the device in your 19-inch rack and horizontally align the left-hand and right-hand bracket holes to selected holes in the vertical tracks of the 19-inch rack.
2. Use standard 19-inch rack bolts (not provided) to fasten the device to the rack tracks.
3. Use two additional (not supplied) rear mounting brackets to better support the unit. (Optional but Recommended)

Note 1: Users assembling the rear brackets by themselves should note the following:

Note 2: The distance between the two rear screws is 26.5 mm.

Note 3: To attach the rear brackets use 4-40 UMC screws.

➢ **To place the device on a 19-inch rack's shelf take these 2 steps:**

1. Place the device on the shelf.
2. Follow the steps (optional) for fastening the device to the frame of the rack (as described above) while it is placed on the shelf. This prevents the device from sliding when inserting cables into connectors on the rear panel.

3.2.2 Installing the MG 3200 on a Desktop

No brackets are required. Simply place the device on the desktop in the position you require and attach cables as described below.

3.2.3 Cabling the MG 3200

Refer to "Connecting the E1/T1 Trunk Interfaces" on page 37 for the rear panel cables and cabling procedures.

Note: The MG 3200 is available in all configuration combinations, i.e. AC or DC, as a 16-trunk, 8-trunk, 4-trunk, 2-trunk or 1-trunk configuration. The 16-trunk AC and the 8-trunk DC configuration combinations are illustrated here as representative of the range.

The figure below showing 50-Pin Telco connecters is for 16 Spans. The figure below showing RJ-48c connectors is for up to 8 spans.

3.2.3.1 Power Supply Cabling

3.2.3.2 Connecting the AC Power Supply

➢ **To cable the AC Power Supply , take these 3 Steps:**

1. Permanently connect the unit to a suitable earth with the earthing screw on the rear connector panel, using 14-16 AWG wire.
2. Attach a certified 100/240 VAC power cable to the rear AC socket (or, optionally, two cables to dual AC sockets) and connect to the correct AC power supply.
3. Connect the power connectors, located on the device's rear panel, to the power source using AC power cables.

3.2.3.3 Connecting the DC Power Supply

To connect the MG 3200 to a DC power supply use one of these two options:

- DC Terminal block with a screw connection type.
- DC Terminal block with a crimp connection type.

➢ To cable the DC Power Supply with DC Terminal block with a screw connection type, take these 3 Steps:

1. Create a DC cable by inserting two 14-16 AWG wires into the supplied adaptor (refer to the figure below) and fasten the two screws, each one located directly above each wire.
2. Connect the two insulated wires to the correct DC power supply. Ensure that the connections to the DC power supply maintain the correct polarity.
3. Insert the terminal block to the DC inlet located on the rear of the device.

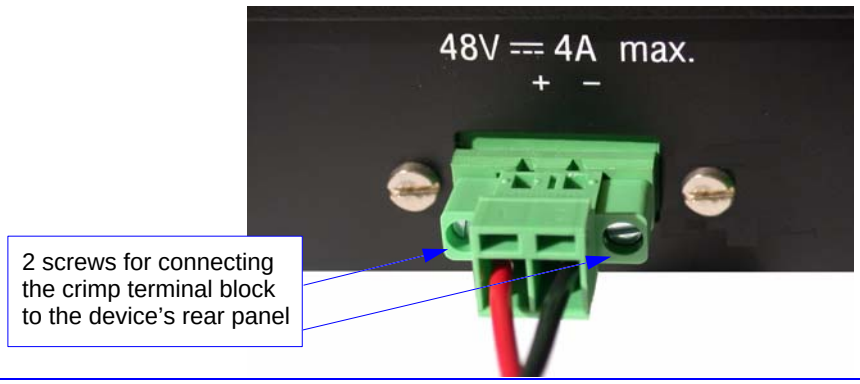
Figure 3-3: DC Power Connector - Screw Type

➢ To cable the DC Power Supply with DC Terminal block with a crimp connection type , take these 3 Steps:

1. Remove the DC adaptor (screw connection type) that is attached to the device's rear panel.
2. Connect the two insolated wires to the correct DC power supply. Ensure that the connections to the DC power supply maintain the correct polarity (refer to the figure below).

3. Insert the terminal block to the DC inlet located on the rear of the device.

Figure 3-4: DC Power Connector - Crimp Type



3.2.4 Connecting the E1/T1 Trunk Interfaces

3.2.4.1 Connecting E1/T1 Trunk Interfaces

1. **If you are using 50-pin Telco connectors:**

   - Connect an E1/T1 trunk cable to the TP-1610 RTM's 50-pin female Telco connector labeled Trunks 1-8 and connect another E1/T1 trunk cable to the RTM's 50-pin female Telco connector labeled Trunks 9-16. **Now continue with Step 4 below.**

Refer to the figure showing the chassis' rear view with connected cables (16 Spans and Dual AC), Rear View with Connected Cables" (on page 40).

Note: The user's 50-pin male connector of Trunks 1 to 8 is connected to the 50-pin female connector (DDK 57AE-40500-21D) labeled **E1/T1 1 to 8.** The User's 50-pin male connector of Trunks 9 to 16 is connected to the 50-pin female connector labeled **E1/T1 9 to 16**. The 2 male connectors **must be** wired identically, according to the table and figure below.

Figure 3-5: 50-Pin Female Telco Board-Mounted Connector

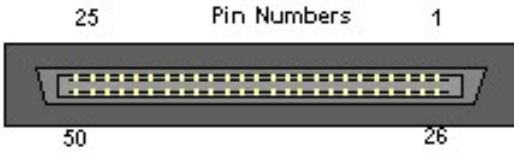


Table 3-2: Connections on Each 50-Pin Telco Connector

E1/T1 Number		Tx Pins (Tip/Ring)	Rx Pins (Tip/Ring)
1 to 8	9 to 16		
1	9	27/2	26/1
2	10	29/4	28/3
3	11	31/6	30/5
4	12	33/8	32/7
5	13	35/10	34/9
6	14	37/12	36/11
7	15	39/14	38/13
8	16	41/16	40/15

2. **If you are using RJ-48c connectors:**

   - Connect the E1/T1 trunk cables to the TP-1610 RTM's E1/T1 interfaces. There are up to eight RJ-48c connectors labeled Trunks 1 to 8 on the RTM.

Refer to the 'figure showing the chassis' rear view with connected cables (8 Spans and DC)' on page 40.

The RJ-48c connectors are wired according to the figure below. **Now continue with Step 4 below.**

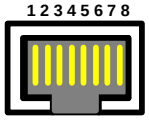
Figure 3-6: RJ-48c Trunk Connectors

3. On the TP-1610 RTM, connect the Category 5, LAN cables to the Ethernet 1 and optionally Ethernet 2 RJ-45 interfaces. Connect the other end of the Category 5 LAN cable to your IP network.

4. For redundant operation, connect **Ethernet 1** to Ethernet Switch #1 and **Ethernet 2** to Ethernet Switch #2.

The RJ-45 connectors labeled **Ethernet 1** and **Ethernet 2** are wired according to the figure below.

Figure 3-7: RJ-45 LAN Connectors and Pinout



1 - Tx+
2 - Tx-
3 - Rx+
6 - Rx-

4, 5, 7, 8 not connected

5. Restart the applications and run the system.
6. Power up the MG 3200. The Ready and LAN LEDs on the front panel turn to green (after a self-testing period of about 60 seconds). Any malfunction causes the Ready LED to turn red (refer to "Chassis LED Indicators" on page 24 for details on the MG 3200 LEDs).
7. When you have completed the hardware setup, proceed to "Getting Started" on page 47 to begin setting up the software.

The MG 3200 hardware installation is now complete.

3.2.4.2 MG 3200 Rear Views with Connected Cables

The figures below display the MG 3200 rear view with connected cables.

Figure 3-8: Rear View with Connected Cables (16 Spans and Dual AC)

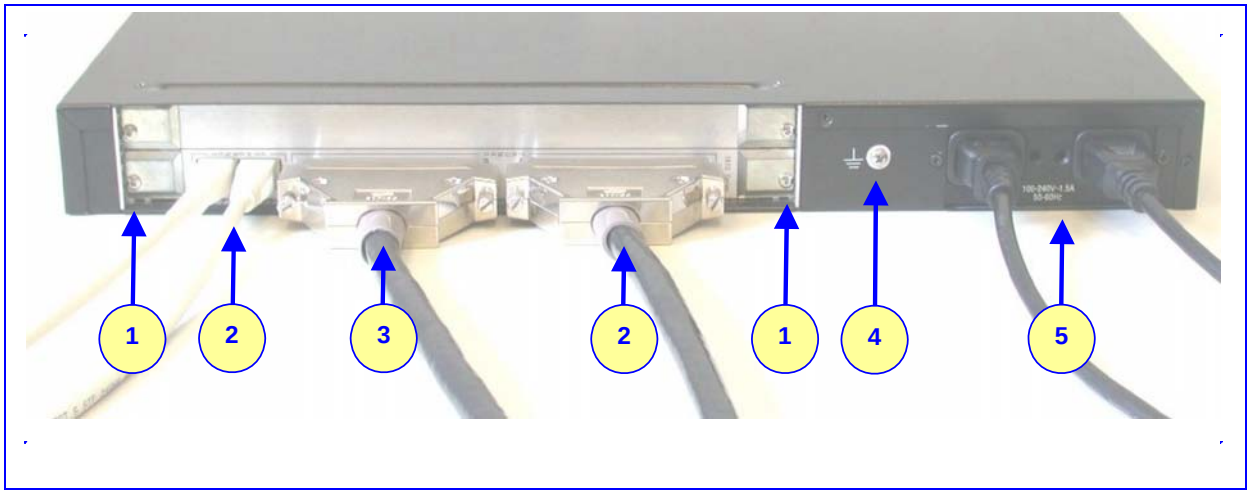


Table 3-3: MG 3200 Rear Panel Cabling (16 Trunks, Dual AC Power) Component Descriptions

Item #	Label	Component Description
1		RTM locking screws
2	ETHERNET	Two Category 5 network cables, connected to the 2 Ethernet RJ-45 ports
3	TRUNKS	Two 50-pin Telco connector cables, each supporting 8 trunks
4	⏚	Protective earthing screw
5	100-240~1.5A	Dual AC power cables

Figure 3-9: Rear View with Connected Cables (8 Spans and DC)

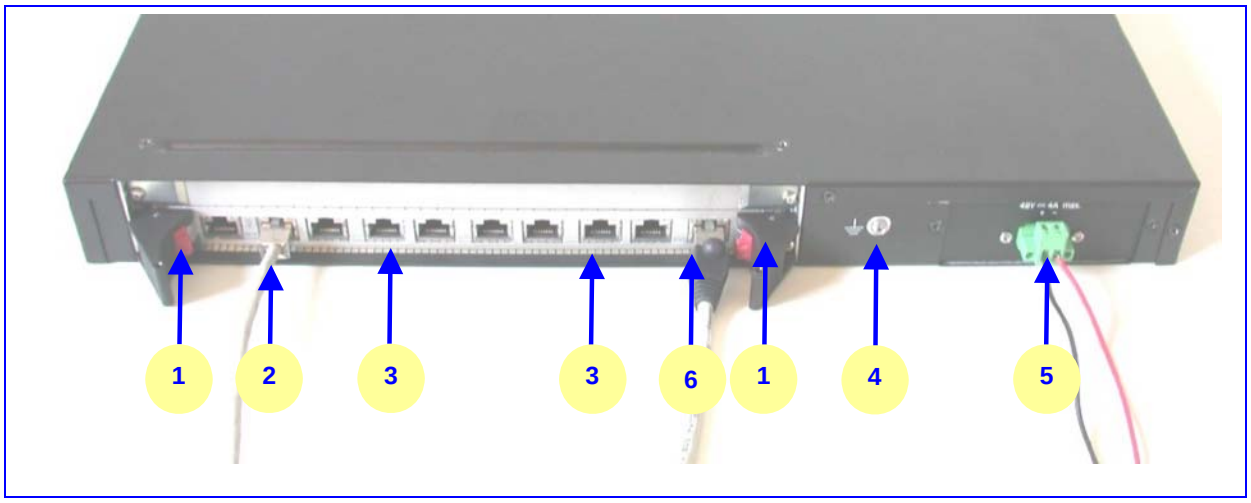


Table 3-4: MG 3200 Rear Panel Cabling (8 Trunks, DC Power) Component Descriptions

Item #	Label	Component Description
1		RTM latches
2	ETH	A Category 5 network cable, connected to the Ethernet 1 RJ-45 port
3	PSTN	8 RJ-48c ports, each supporting a trunk
4	⏚	Protective earthing screw
5	48V 4A max	2-pin connector for DC
6		An RJ-48c trunk cable connected

3.3 Board Replacement

3.3.1 Preliminaries

Observe the general safety precautions against personal injury and equipment damage outlined in the regional Installation Safety Manual at all times.

Note: Electronic components on printed circuit boards are extremely sensitive to static electricity. Normal amounts of static electricity generated by clothing can damage electronic equipment. To reduce the risk of damage due to electrostatic discharge when installing or servicing electronic equipment, it is recommended that anti-static earthing straps and mats be used.

➢ Before removing or replacing boards from the chassis, take these 2 steps:

- Attach a wrist strap for electrostatic discharge (ESD) and connect it to the rack frame using a banana plug or an alligator clip.

Note: Do not set components down without protecting them with a static bag.

The TP-1610 board is hot swappable and can therefore be removed from a slot (and inserted into a slot) while the MG 3200 Media Gateway is under power.

3.3.2 Removing Boards

➢ To remove the front TP-1610 board from the chassis, take these 3 steps:

1. Unfasten the screws on the plate of the board.
2. Press the red ejector buttons on the two black ejector/injector latches on both ends and wait for the hot-swap blue LED to light, indicating that the board can be removed.
3. Pull on the two ejector/injector latches and ease out the board from the slot.

➢ To remove the TP-1610 RTM from the chassis, take these 4 steps:

1. Remove the cables attached to the RTM.
2. Unfasten the screws on the brackets at both ends of the panel that secure the RTM to the device.
3. Press the red ejector buttons on the two black ejector/injector latches on both ends.
4. Grasp the panel and ease the RTM out of the slot.

3.3.2.1 Inserting Boards

Note: Make a note of the MAC address of the replacement board as it is needed for setting the correct parameter configuration for the replacement board in the element management system you are utilizing.

➢ **To insert the TP-1610 board into the chassis, take these 6 steps:**

1. Hold the board horizontally.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board with the grooves on each end.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis. The Blue hot-swap LED is lit.
4. Press the two black ejector/injector latches on both ends inward, toward the middle, until you hear a click.
5. Wait for the hot-swap blue LED to turn off.
6. Fasten the screws on the front panel of the board to secure the board to the chassis and to ensure that the board has a chassis earthing connection.

➢ **To insert the TP-1610 RTM into the chassis, take these 6 steps:**

1. Hold the board horizontally.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board with the grooves on each end.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis.
4. Press the two black ejector/injector latches on both ends inward, toward the middle until you hear a click.
5. Fasten the screws on the front panel of the board to secure the board to the chassis and to ensure that the board has a chassis earthing connection.
6. Reattach the cables. (Refer to 'Cabling the MG 3200'.)

3.3.2.2 Configuring and Unlocking the MG 3200

The MG 3200 should be unlocked using the element management system (EMS) employed in your system. For more information on performing graceful lock, refer to "Performing Graceful Lock" on page 42 or the user documentation accompanying the element management system (EMS) employed in your system.

Reader's Notes

4 Software Package

After installing the device and powering it up, you are ready to install the utilities that are included in the software package. This software package must be installed on the host PC/machine to be used to manage the device. The software package is supplied to customers on a CD accompanying the MG 3200.

➢ To get started, take these basic steps:

1. Check the software package contents (go to "Software Directory Contents & Structure" on page 45)
2. To configure the MG 3200's IP address, go to "Getting Started" on page 47.

4.1 Software Directory Contents & Structure

Refer to the file *Contents.txt* on the software package CD.

Reader's Notes

5 Getting Started

The MG 3200 is supplied with application software already resident in its flash memory (with factory default parameters). The MG 3200 is also supplied with an Embedded (integrally stored) Web Server.

'Assigning the MG 3200 IP Address' below describes how to assign an IP address to the MG 3200.

"Restoring Networking Parameters to their Initial State" on page 49 describes how to restore the network parameters to their initial state.

For detailed information on how to *fully* configure the gateway refer to the "Embedded Web Server" on page 141.

5.1 Assigning the MG 3200 IP Address

To assign an IP address to the MG 3200 use one of the following methods:

- HTTP using a Web browser (refer to "Assigning an IP Address Using HTTP" on page 47).
- BootP (refer to "Assigning an IP Address Using BootP" on page 48).
- DHCP (refer to (refer to "Using BootP/DHCP' on page 53').

The default networking parameters are show in the table below.

Table 5-1: TP-1610 Default Networking Parameters

MG 3200 Version	Default Value
Single module (up to 8 Trunks)	10.1.10.10
Double module (up to 16 Trunks)	10.1.10.10 (Trunks 1-8) and 10.1.10.11 (Trunks 9-16)
Default subnet mask is 255.255.0.0, default gateway IP address is 0.0.0.0	

5.1.1 Assigning an IP Address Using HTTP

➢ To assign an IP address using HTTP, take these 8 steps:

1. Connect your computer to the MG 3200. Either connect the network interface on your computer to a port on a network hub / switch (using an RJ-45 Ethernet cable), or use an Ethernet cross-over cable to directly connect the network interface on your computer to the RJ-45 jack on the MG 3200.
2. Change your PC's IP address and subnet mask to correspond with the MG 3200 factory default IP address and subnet mask, shown in the table above. For details on changing the IP address and subnet mask of your PC, refer to Windows™ Online Help (Start>Help).

3. Access the MG 3200 Embedded Web Server (refer to "Embedded Web Server" on page 141).

4. In the 'Quick Setup' screen (shown in the "Quick Setup Procedure" on page 147, on page 147), set the MG 3200 'IP Address', 'Subnet Mask' and 'Default Gateway IP Address' fields under 'IP Configuration' *to correspond with your network IP settings.* If your network doesn't feature a default gateway, enter a dummy value in the 'Default Gateway IP Address' field.

5. Click the **Reset** button and click **OK** in the prompt. The MG 3200 applies the changes and restarts. This takes approximately 1 minute to complete. When the MG 3200 has finished restarting, the Ready and LAN LEDs on the front panel are lit green.

Tip: Record and retain the IP address and subnet mask you assign the MG 3200. Do the same when defining new username or password. If the Embedded Web Server is unavailable (for example, if you've lost your username and password), use the BootP/TFTP configuration utility to access the device, "reflash" the load and reset the password (refer to the Appendix, "BootP/TFTP Server" on page 223 for detailed information on using a BootP/TFTP configuration utility to access the device).

6. Disconnect your computer from the MG 3200 or from the hub / switch (depending on the connection method you used in step 1 above).

7. Reconnect the MG 3200 and your PC (if necessary) to the LAN.

8. Restore your PC's IP address & subnet mask to what they originally were. If necessary, restart your PC and re-access the MG 3200 via the Embedded Web Server with its new assigned IP address.

5.1.2 Assigning an IP Address Using BootP

Note: BootP procedure can also be performed using any standard compatible BootP server.

Tip: You can also use BootP to load the auxiliary files to the MG 3200 (refer to' 'Using BootP/DHCP' on page 53' and the Appendix, "BootP/TFTP Server" on page 223).

➢ To assign an IP address using BootP, take these 3 steps:

1. Open the BootP application (supplied with the MG 3200 software package).

2. Add the client configuration for the MG 3200, refer to "Client Configuration Screen" on page 229.

3. Reset the gateway *physically* causing it to use BootP. The MG 3200 changes its network parameters to the values provided by the BootP.

5.2 Restoring Networking Parameters to their Initial State

You can use the **Reset** button to restore the TP-1610 networking parameters to their factory default values (described in the "Default Networking Parameters" above) and to reset the username and password.

Note that this process also restores the TP-1610 parameters to their factory settings, therefore you must load your previously backed-up *ini* file, or the default *ini* file (received with the software kit) to set them to their correct values.

➢ To restore networking parameters to their initial state, take these 6 steps:

1. Back up the *ini* file. Refer to "Backup Copies of ini and Aux Files" on page 80.
2. Disconnect the TP-1610 from the power and network cables.
3. Reconnect the power cable; the gateway is powered up. After approximately 45 seconds the Ready LED turns to green and the Control LED blinks for about 3 seconds.
4. While the Control LED is blinking, press shortly on the reset button (located on the left side of the front panel). The gateway resets a second time and is restored with factory default parameters (username: **Admin**, password: **Admin** - both case-sensitive).
5. Reconnect the network cable.
6. Load your previously backed-up *ini* file, or the default *ini* file (received with the software kit). To load the *ini* file via the Embedded Web Server, refer to "Software Upgrade Wizard" on page 190.

Reader's Notes

6 MG 3200 Initialization & Configuration Files

This section describes the configuration options and Initialization procedures for the MG 3200. It includes:

- Boot Firmware & Operational Firmware (refer to "Boot Firmware & Operational Firmware" on page 51)
- Startup Process (refer to "MG 3200 Startup" on page 51)
- BootP/DHCP (refer to "Using BootP/DHCP' on page 53')
- Configuration Parameters and Files (refer to "Configuration Parameters and Files" on page 58)

6.1 Boot Firmware & Operational Firmware

The MG 3200 runs two distinct software programs: Boot firmware and operational firmware.

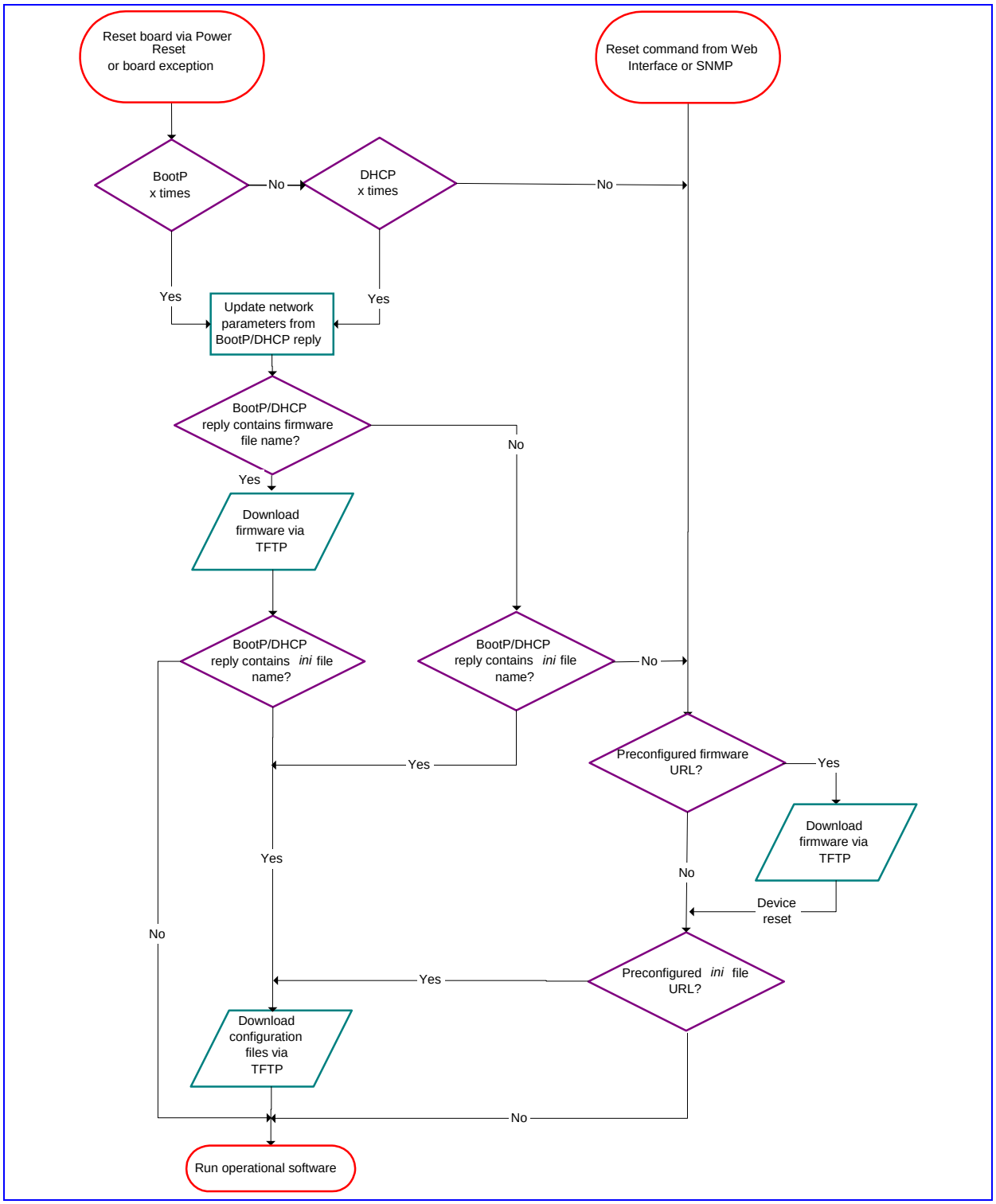
- Boot firmware - Boot firmware (also known as flash software) resides in the MG 3200's non-volatile memory. When the MG 3200 is reset, Boot firmware is initialized and the operational software is loaded into the SDRAM from a TFTP server or integral non-volatile memory. Boot firmware is also responsible for obtaining the MG 3200's IP parameters and *ini* file name (used to obtain the MG 3200's configuration parameters) via integral BootP or DHCP clients. The Boot firmware version can be viewed on the Embedded Web Server's GUI (refer to "Embedded Web Server" on page 141). The last step the Boot firmware performs is to jump to the first line of code in the operational firmware.
- *cmp* Operational firmware files - The operational firmware, in the form of a *cmp* file (the software image file), is supplied in the software package contained on the CD accompanying the MG 3200. These files contain the MG 3200's main software, providing all the services described in this manual. The *cmp* file is usually burned into the MG 3200's non-volatile memory so that it does not need to be externally loaded each time the MG 3200 is reset.

6.2 MG 3200 Startup

The MG 3200's startup process begins when the MG 3200 is reset. The startup process ends when the operational firmware is running. The Startup process includes how the MG 3200 obtains its IP parameters, firmware and configuration files.

The flow chart in the figure below illustrates the Startup process.

Figure 6-1: Startup Process Diagram



Note 1: The BootP/DHCP server should be defined with an *ini* file name when you need to modify configuration parameters or when you're working with a large Voice Prompt file that is not stored in non-volatile memory and must be loaded after every reset.

Note 2: The default time duration between BootP/DHCP requests is set to 1 second. This can be changed by the *ini* file parameter BootPDelay. Also, the default number of requests is 3 and can be changed by the *ini* file parameter BootPRetries. (Both parameters can also be set using the Command Line Switches in the BootP/TFTP Server).

Note 3: The *ini* file configuration parameters are stored in non-volatile memory after the file is loaded. When a parameter is missing from the *ini* file, a default value is assigned to this parameter and stored in non-volatile memory (thereby overriding any previous value set for that parameter). Refer to "Using BootP/DHCP" on page 53 and the Appendix, "BootP/TFTP Server" on page 223.

Note 4: By default, the configuration files are stored in non-volatile memory. Use the *ini* file parameter, 'SaveConfiguration=0', to refrain from storing the configuration files in the non-volatile memory after loading.

6.3 Using BootP/DHCP

The MG 3200 uses BootP (Bootstrap protocol) and DHCP to configure the MG 3200's initial parameters. BootP/DHCP enables network administrators to manage the basic configuration of the MG 3200 from a central server.

RFCs (IETF Requests for Comment) 951, 1542, and 2132 describe BootP in detail. The protocol has been extended to enable BootP/DHCP to configure additional parameters specific to the MG 3200.

As the flow chart in the figure above illustrates, a BootP/DHCP request is issued after a power reset or a device exception.

Note: BootP is normally used to configure the initial parameters of the MG 3200. Thereafter, BootP is no longer required as all parameters can be stored in the MG 3200's non-volatile memory and used when BootP is inaccessible. BootP is required again (for example) to change the IP address of the MG 3200.

6.3.1 BootP/DHCP Server Parameters

BootP/DHCP can be used to provision the following parameters (included in the BootP/DHCP reply. Note that some parameters are optional):

- **IP address, IP subnet mask** - These parameters are mandatory and are supplied by the server to the MG 3200 every time a BootP/DHCP process takes place.
- **Default Gateway IP address** - This configuration parameter is optional. The default Gateway IP address is supplied to the MG 3200 by BootP/DHCP only if the field is defined/configured in the server.

- **TFTP server IP address** - This optional parameter contains the address of the TFTP server from which the firmware file and *ini* file are loaded.
- **DNS Server IP Address (Primary and Secondary)** - These optional parameters contain the IP addresses of the DNS servers. These parameters are available only in DHCP and from Boot version 1.92. A DNS server can only be used by an H.248 configured device.
- **Firmware file name** - When the MG 3200 detects that this optional parameter is defined/configured in BootP/DHCP, it initiates a TFTP process to load the file. If the firmware file name is not specified in the BootP/TFTP server, the MG 3200 uses the last image stored in its non-volatile memory.
- **Command Line Switches**

In the BootP/TFTP Server, you can add command line switches in the Boot File field (in the Client Configuration screen). Command line switches are used for various tasks, such as to determine if the firmware should be burned on the non-volatile memory or not. The table below describes the different command line switches.

➢ To use a command line switch, take these 4 steps:

1. In the **Boot File** field, leave the file name defined in the field as it is (e.g., *ramxxx.cmp*).
2. Place your cursor after *cmp*.
3. Press the space bar.
4. Type in the switch you require (refer to the table below).

Example: **ramxxx.cmp -fb** to burn flash memory

ramxxx.cmp -fb -em 4 to burn flash memory and for Ethernet Mode 4 (auto-negotiate)

The table below lists and describes the available switches.

Table 6-1: Command Line Switch Descriptions

Switch	Description
-fb	Burn ram.cmp in non-volatile memory. Only the *cmp* file (the compressed firmware file) can be burned to the MG 3200's non-volatile memory. The *hex* file (the uncompressed firmware file) can not be burned.
-em#	Use this switch to set Ethernet mode. 0 = 10 Base-T half-duplex 1 = 10 Base-T full-duplex 2 = 100 Base-TX half-duplex 3 = 100 Base-TX full-duplex 4 = auto-negotiate (default) Auto-negotiate falls back to half-duplex mode when the opposite port is not in auto-negotiate but the speed (10 Base-T or 100 Base-TX) in this mode is always configured correctly.

Table 6-1: Command Line Switch Descriptions

Switch	Description
-br	BootP retries: 1 = 1 BootP retry, 1 sec 2 = 2 BootP retries, 3 sec 3 = 3 BootP retries, 6 sec 4 = 10 BootP retries, 30 sec 5 = 20 BootP retries, 60 sec 6 = 40 BootP retries, 120 sec 7 = 100 BootP retries, 300 sec 15 = BootP retries indefinitely Use this switch to set the number of BootP retries that the MG 3200 sends during start-up. The MG 3200 stops issuing BootP requests when either an AA122BootP reply is received or Number Of Retries is reached. This switch takes effect only from the next MG 3200 reset.
-bd	BootP delays. 1 = 1 sec (default), 2 = 10 sec, 3 = 30 sec, 4 = 60 sec, 5 = 120 sec. This sets the delay from the MG 3200's reset until the first BootP request is issued by the MG 3200. The switch only takes effect from the next reset of the MG 3200.
-bs	Selective BootP
-be	Use -be 1 for the MG 3200 to send client information that can be viewed in the main screen of the BootP/TFTP Server, under column 'Client Info' (refer to Figure A-3, on page 165, showing BootP/TFTP Server's main screen with the column 'Client Info' on the extreme right). 'Client Info' can include IP address, number of channels (in the case of MG 3200' media gateways), which cmp file is burned into the MG 3200's non-volatile memory, etc.

Note: After programming a new *cmp* software image file, all configuration parameters and tables are erased. Reprogram them by downloading the *ini* file.

- **Configuration (*ini*) file name** - The *ini* file is a proprietary configuration file with an *ini* extension, containing configuration parameters and tables. For more information on this file, refer to "Configuration Parameters and Files" on page 58. When the MG 3200 detects that this optional parameter field is defined in BootP, it initiates a TFTP process to load the file into the MG 3200. The new configuration contained in the *ini* file can be stored in the MG 3200's integral non-volatile memory. When ever the MG 3200 is reset and no BootP reply is sent to the board or the *ini* file name is missing in the BootP reply, the MG 3200 uses the previously stored *ini* file.

6.3.2 Host Name Support

From Boot software version 1.92, the MG 3200 registers a device-specific Host Name on the DNS server by defining the Host Name field of the DHCP request. The host name is set to **acl_nnnnnnn**, where nnnnnnn is the serial number of the MG 3200 (the serial number is equal to the last 6 digits of the MAC address converted from Hex to decimal). The DHCP server registers this Host Name on the DNS server. This feature allows users to configure the MG 3200 via the Web Browser by providing the following URL: **http://ACL_<serial number>** (instead of using the boards' IP address).

6.3.3 Selective BootP

The Selective BootP mechanism, available from Boot version 1.92, allows the integral BootP client to filter out unsolicited BootP replies. This can be beneficial for environments where more than one BootP server is available and only one BootP server is used to configure devices.

- To activate this feature, add the command line switch **-bs 1** to the Firmware File Name field.
- To deactivate, use **-bs 0**. When activated, the MG 3200 accepts only BootP replies containing the text AUDC in the Vendor Specific Information field.

6.3.4 Vendor Specific Information

The MG 3200 uses the Vendor Specific Information field in the BootP server to provide device-related initial startup parameters (according to RFC 1533). This field is not available in DHCP servers. The field is disabled by default.

To enable / disable this feature user can do one of the following:

a. Set the *ini* file parameter 'ExtBootPReqEnable' = **0** to disable, or **1** to enable.

b. Use the **-be** command line switch in the Boot file field in the BootP server as follows: **ramxxx.cmp -be 0** to disable, or **-be 1** to enable.

The table below details the Vendor Specific Information field according to the MG 3200:

Table 6-2: Vendor Specific Information Field

Tag #	Description	Value	Length
220	Board Type	#02	1
221	Current IP Address	XXX.XXX.XXX.XXX	4
222	Burned Boot Software Version	X.XX	4
223	Burned CMP Software Version	XXXXXXXXXXXX	12
224	Geographical Address	0 - 31	1
225	Chassis Geographical Address	0 - 31	1
226	TPM ID	N/A	1
227	Rear I/O Version	N/A	1

Table 6-2: Vendor Specific Information Field

Tag #	Description	Value	Length
228	In door - Out door (In door is valid for FXS only. FXO is always Out door.)	N/A	1
229	E&M	N/A	1
230	Analog Channels	N/A	1

The structure of the Vendor Specific Information field is demonstrated in the table below.

Table 6-3: Vendor Specific Information Fields

Vendor-Specific Information Code	Length Total	Tag Num	Length	Value	Tab Num	Length	Value	Tag Num	Length	Value (1)	Value (2)	Value (3)	Value (4)	Tag End
42	12	220	1	02	227	1	1	221	4	10	2	70	1	255

6.3.5 Microsoft™ DHCP/BootP Server

The MG 3200 can be configured with a 3rd party BootP server (besides The BootP/TFTP Server), including the Microsoft™ DHCP server, to provide the TP-1610 with an IP address and other initial parameter configurations.

To configure the Microsoft™ Windows™ NT DHCP Server to configure an IP address to BootP clients, add a reservation for each BootP client.

For information on how to add a reservation, view the "Managing Client Reservations Help" topic in the DHCP Manager.

The reservation builds an association between MAC address (12 digits), provided in accompanying product documentation) and the IP address. Windows™ NT Server provides the IP address based on the TP-1610 MAC address in the BootP request frame.

To configure the Microsoft™ Windows™ NT DHCP server to provide Boot File information to BootP clients, edit the BootP Table in the DHCP Manager. The BootP Table is located in the Server Properties dialog, accessed from the Server menu. For information on editing the BootP Table, view the "BootP Table" Help topic in the DHCP Manager.

The following parameters must be specified:

- **Local IP address** - The MG 3200's IP address
- **Subnet mask**
- **Gateway IP address** - Default Gateway IP address

- **BootP File name** - Optional (refer to the following Note)

Note: The BootP File field should normally not be used. The field is only used for software upgrade (refer to "Upgrading MG 3200 Software' on page 80').

6.4 Configuration Parameters and Files

The MG 3200's configuration is stored in two file groups.

- The configuration file - an initialization (*ini*) text file containing configuration parameters of the MG 3200.
- The auxilliary files - *dat* files containing the raw data used for various tasks such as Call Progress Tones, Voice Prompts, logo image, etc.

Table 6-4 presents a brief description of the *ini* file and of each auxiliary file.

Table 6-4: *ini* and Auxiliary Files Descriptions

File Type	Description
Ini	Load the file to provision the MG 3200 parameters. The Embedded Web Server enables practically full device provisioning but customers may occasionally require new feature configuration parameters in which case this file is loaded. Note that loading the *ini* file only provisions parameters that are contained in the *ini* file. If a parameter is not specified in the *ini* file, values associated with that parameter are reset to a default value. These values may not be the same as the values that were configured for the VoIP gateway at the time of manufacture. **Note:** After the file has completed loading, the VoIP gateway automatically restarts (software is loaded from the flash).
Call Progress Tones (CPT)	This is a region-specific, telephone exchange-dependent file that contains the Call Progress Tones levels and frequencies that the VoIP gateway uses. The default CPT file is: U.S.A.
Voice Prompts (VP)	The voice announcement file contains a set of Voice Prompts to be played by the MG 3200 during operation on Call Agent request.
Prerecorded Tones (PRT)	The *dat* PRT file enhances the gateway's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the Call Progress Tones file.
CAS	Up to 8 different CAS files containing specific CAS protocol definitions. These files are provided by Nortel to support various types of CAS signaling. These files are needed for CAS protocols only
VXML	VXML files are auxiliary files that define service logic. These are not applicable for the H.248 MG 3200.
Coder Table (CTBL)	Defines which coders are to be supported on the TP1610 board. It is limited to the supported coders according to the loaded DSP template. This was added to the 4.6 release specifically for Nortel Media Server for legal intercept. It is not applicable for the MG 3200.

These files contain factory-pre-configured parameter defaults when supplied with the MG 3200 and are stored in the MG 3200's non-volatile memory. The MG 3200 is started up initially with this default configuration. Subsequently, these files can be modified and reloaded using any of the following methods:

- via BootP/TFTP during the startup process (refer to "Using BootP/DHCP' on page 53' and the Appendix, "BootP/TFTP Server" on page 223).
- via the Embedded Web Server (refer to "Embedded Web Server" on page 141).

The modified auxiliary files can be burned into the non-volatile memory (refer to the SaveConfiguration parameter in "Downloading Auxiliary Files" on page 67) so that the modified configuration is utilized with subsequent resets. The configuration file is always stored on the non-volatile memory. There in no need to repeatedly reload the modified files after reset.

Note 1: Users who configure the MG 3200 with the Embedded Web Server do not require downloading the *ini* file and have no need to utilize a TFTP server.

Note 2: SNMP users configure the MG 3200 via SNMP. Therefore a very small *ini* file is required which contains the IP address for the SNMP traps.

6.4.1 Initialization (ini) File

The *ini* file can contain a number of parameters. The *ini* file structure supports the following parameter value constructs:

- **Parameter = Value** (refer to 'Parameter = Value Constructs') The lists of parameters are provided inthe Appendix, "Individual '*ini*' File Parameters" on page 233.
- **Tables of Parameter Values** (refer to Table of Parameter Value Constructs). The lists of parameters are provided inthe Appendix, 'Table Parameters' on page 281.

Below is an example of the general structure of the *ini* file for both the Parameter = Value and Tables of Parameter Value Constructs.

```
[Sub Section Name]
Parameter_Name = Parameter_Value
Parameter Name = Parameter Value
.
..

; REMARK

 [Sub Section Name]
...

; Tables Format Rules:
[Table Name]
; Fields declaration
Format Index Name 1 ... Index Name N = Param Name 1 ...
Param Name M
; Table's Lines (repeat for each line)
Table Name Index 1 val ... Index N val = Param Val 1 ...
Param Val M
[\Table_Name]
```

6.4.1.1 Parameter Value Construct

The following are the rules in the *ini* File Structure for individual *ini* file parameters (Parameter = Value):

- Lines beginning with a semi-colon ';' (as the first character) are ignored.
- An Enter must be the final character of each line.
- The number of spaces before and after "=" is not relevant.
- If there is a syntax error in the parameter name, the value is ignored.
- Syntax errors in the parameter value field can cause unexpected errors (because parameters may be set to the incorrect values).
- Sub-section names are optional.
- String parameters, representing file names, for example, CallProgressTonesFileName, must be placed between two inverted commas ('…').
- The parameter name is NOT case sensitive; the parameter value is not case sensitive except for coder names.
- Numeric parameter values should be entered only in decimal format.
- The *ini* file should be ended with one or more Enters.

The example below shows a sample of an *ini* file for H.248.

```
[MEGACO]

; List of Call agents, separated by ','. The default is the loading
computer.
PROVISIONEDCALLAGENTS = 10.2.1.254
; List of ports for the above Call Agents, separated by ','. The
default is 2944.
PROVISIONEDCALLAGENTSPORTS = 2944
; IP of the LOG server
LOGSERVERIP = 10.2.1.254
; The next 3 field are the parts of the termination name. For
example, if you wish the
; name to look like: 'gw3/tr0/ep1', you shall define: ;GATEWAYNAME
= 'gw3/',
; TRUNKNAME = 'tr', and ENDPOINTNAME = 'ep' . The RTP in built from
the GATEWAYNAME,

; the string 'RTP' and a number. In this example it shall be: gw3/
RTP0.;
GATEWAYNAME = 'c4'
TRUNKNAME = 's'

ENDPOINTNAME = 'c'; This parameter activates the MEGACO!!!! If
omitted, MGCP will be active
MGCONTROLPROTOCOLTYPE = 2

; The following disables the keep-alive mechanism if set to 0, else
it is enabled
KEEPALIVEENABLED = 1
;
; This parameter defines the profile used. 1 - is for version 2, 2
- for version 1
MGCPCOMPATIBILITYPROFILE = 2
```

Note: Before loading an *ini* file to the MG 3200, make sure that the extension of the *ini* file saved on your PC is correct: Verify that the checkbox Hide extension for known file types (My Computer>Tools>Folder Options>View) is unchecked. Then, verify that the *ini* file name extension is *xxx.ini* and NOT erroneously *xxx.ini.ini* or *xxx~.ini*.

The lists of individual *ini* file parameters are provided inthe Appendix, "Individual '*ini*' File Parameters" on page 233.

6.4.1.2 Tables of Parameter Value Construct

Tables of Parameter Values group related parameters of a given entity and handle them together. Tables are composed of rows and columns. The columns represent parameters types, while each row represents an entity. The parameters in each row are called the line attributes. Rows in table may represent (for example) a trunk, SS7 Link, list of timers for a given application, etc.

The tables below provide useful examples for reference.

Note: The tables below are provided as examples for the purpose of illustration only and are NOT actually implemented in MG 3200.

Table 6-5: Table of Parameter Values Example - Remote Management Connections

Index Fields: **1. Connection Number**				
Connection Number	**User Name**	**User Password**	**Time Connected (msec)**	**Permissions**
0	Admin	Yellow9	0	All
1	Gillian	Red5	1266656	Read Only
2	David	Orange6	0	Read Write

Table 6-6: Table of Parameter Values Example - Port-to-Port Connections

Index Fields: **1. Source Ports** **2. Destination IP** **3. Destination Port**				
Source Port	**Destination IP**	**Destination Port**	**Connection Name**	**Application Type**
2020	10.4.1.50	2020	ATM_TEST_EQ	LAB_EQ
2314	212.199.201.20	4050	ATM_ITROP_LOOP	LAB_EQ
6010	10.3.3.41	6010	REMOTE_MGMT	MGMT

6.4.1.2.1 Table Indices

Each row in a table must be unique. For this reason, each table defines one or more Index fields. The combination of the Index fields determines the 'line-tag'. Each line-tag may appear only once.

In the example provided in the table above, 'Table of Parameter Values Example - Remote Management Connections', there is only one index field. This is the simplest way to mark rows.

In the example provided in the table above, 'Table of Parameter Values Example - Port-to-Port Connections', there are three Index fields. This more complicated method is a result of the application it represents.

6.4.1.2.2 Table Permissions

Each field in a line has a 'permission' attribute, which determines if and when the user may modify the field.

There are several types of permissions:

- **Read -** The user may read the value of a field (true for all fields).
- **Write -** The user may modify the value of the field at any time.
- **Create -** The user must provide a value for the field at creation time.

The default values set for all fields already determine the initial values.

- **Maintenance write** - The user may modify the value of the field only when the entity represented by the line is in maintenance state.

Each table includes rules to determine when it is in a maintenance state.

In the 'Table of Parameter Values Example - Remote Management Connections' above, the 'User Name' and 'User Password' fields have Read-Create permissions. The 'Time Connected' field has Read-Only permission, and the 'Permissions' field has a Read-Create-Maintenance_write permission.

6.4.1.3 Rules in the *ini* File Structure for the Tables of Parameter Value Construct

The *ini* file allows you to add/modify parameters in tables. When using tables, Read-Only parameters are not uploaded, since the Read-Only parameters cause an error when trying to download the uploaded file. Therefore read-only parameters should not be included in tables in the *ini* file. Consequently, tables are uploaded with all parameters having at least one of the following permissions:

- Write
- Create
- Maintenance write

The 'format-line' rule defines which fields of the table are to be modified by the given *ini* file (this may vary among *ini* files for the same table). The 'format-line' must only include fields, which can be modified (which are all parameters that are not specified as read-only).

One exception is the index-fields, which are ALWAYS mandatory fields. In the 'Table of Parameter Values Example - Remote Management Connections' above, all fields except the 'Time Connected' field are uploaded.

6.4.1.3.1 Tables Structure Rules

Tables are composed of four elements:

- **Table-Title -** The Table's string name in square brackets (e.g., [MY_TABLE_NAME]).
- **Format Line -** This line specifies the table's fields by their string names.
  - The first word MUST be "FORMAT", followed by indices field names, and after '=' sign, all data fields names should be listed.
  - Items must be separated by ',' sign.
  - The Format Line must end with ';' sign.
- **Data Line(s) -** The actual values for parameters are specified in each Data line. The values are interpreted according to the format line. The first word must be the table's string name.
  - Items must be separated by a ',' sign.
  - A Data Line must end with a ';' sign.
- End-of-Table-Mark: Marks the end of a table. Same as Table title, but string name is preceded by '\'.

Below is an example of the table structure in an *ini* file.

```
; Table: Items Table.
; Fields: Item Name, Item Serial Number, Item Color, Item weight.
; NOTE: Item_Color is not specified. It will be given default
value.
[Items Table]
; Fields declaration
Format Item Index =  Item Name, Item Serial Number, Item weight;
Items Table 0 = Computer, 678678, 6;
Items Table 6 = Computer-screen, 127979, 9;
Items Table 2 = Computer-pad, 111111, $$;
[\Items Table]
```

- Indices (in both the Format line and the Data lines) must all appear in order, as determined by the table's specific documentation. The Index field must NOT be omitted.
- Data fields in the Format line may use a sub-set of all of the configurable fields in a table only. In this case, all other fields are assigned with the pre-defined default value for each configured line.
- The order of the Data fields in the Format line is not significant (unlike the Index-fields). Field values in Data lines are interpreted according to the order specified in the Format line.
- The sign '$$' in the Data line means that the user wants the pre-defined default value assigned to the field for the given line.
- The order of Data lines is insignificant.
- Data lines must match the Format line, i.e. it must contain exactly the same number of Indices and Data fields and should be in exactly the same order.
- A line in a table is identified by its table-name and its indices. Each such line may appear only once in the *ini* file.
- Table's dependencies:

  Certain tables may depend on other tables. For example, one table may include a field, which specifies an entry in another table, to specify additional attributes of an entity, or to specify that a given entity is part of a larger entity. The tables must appear in order of dependency (i.e. if Table X is referred to by Table Y, then Table X must appear in the *ini* file before Table Y).

6.4.1.3.2 Dynamic Tables versus Static Tables

Static Table

The Static table type does not support adding new lines or removing (deleting) an existing line. All lines in a Static table are pre-configured with default values. Users may modify values in existing lines. After reset, all lines in a Static table are available.

Dynamic Table

The Dynamic table type supports adding and removing lines. It is always initialized as an empty table, with no lines. Users should add lines to the Dynamic table via the *ini* file or at run-time.

Note: Certain Dynamic tables may initialize one or more lines at start-up time. If so, it is documented in the table's specific section.

6.4.1.3.3 Tables in the Uploaded *ini* File

Tables are grouped according to the applications they configure. For example, several tables are required to configure SS7, and other tables are required to configure ATM.

When uploading the *ini* file, the policy is to include only tables that belong to applications, which have been configured (Dynamic tables of other applications are empty, but static tables are not). The trigger for uploading tables is further documented in the applications' specific sections.

6.4.1.3.4 Secret Tables

A table is defined as a secret table if it contains at least one secret data field or if it depends on such a table. A secret data field is a field that must not be revealed to the user. An example of a secret field can be found in an IPSEC application. The IPsec tables are defined as secret tables because the IKE table contains a pre-shared key field, which must not be revealed to the user. The SPD table depends on the IKE table. Therefore, the SPD table is defined as a secret table.

There are two major differences between tables and secret tables:

- The secret field itself can not be viewed via SNMP, Web Server or any other tool.
- *ini* File behavior: These tables are never uploaded in the ini File (e.g., 'Get INI-File from WEB'). Instead, there is a commented title that states that the secret table is present at the board, and is not to be revealed.

  Secret tables are always kept in the board's non-volatile memory, and may be over-written by new tables that should be provided in a new *ini* File. If a secret table appears in an *ini* File, it replaces the current table regardless of its content. The way to delete a secret table from a board is, for example, to provide an empty table of that type (with no data lines) as part of a new *ini* File. The empty table replaces the previous table in the board.

6.4.1.3.5 Table of Parameter Value Constraints

The *ini* file allows you to add/modify parameters in tables. When using tables, Read-Only parameters are not uploaded, since the Read-Only parameters cause an error when trying to download the uploaded file. Therefore read-only parameters should not be included in tables in the *ini* file. Consequently, tables are uploaded with all parameters having at least one of the following permissions:

- Write
- Create
- Maintenance write

The 'format-line' rule defines which fields of the table are to be modified by the given ini file (this may vary among *ini* files for the same table). The 'format-line' must only include fields, which can be modified (which are all parameters that are not specified as read-only).

One exception is the index-fields, which are ALWAYS mandatory fields. In the "Table of Parameter Values Example - Remote Management Connections" above, all fields except the 'Time Connected' field are uploaded.

The lists of table parameters are provided in the Appendix, 'Table Parameters' on page 281.

6.4.1.4 Secured Configuration File Download

The *ini* file contains sensitive information required for appropriate functioning of the MG 3200. The *ini* file is uploaded to the MG 3200 or downloaded from the gateway using TFTP or HTTP protocols. These protocols are unsecured (and thus vulnerable to a potential hacker). Conversely, if the *ini* file is encoded, the *ini* file would be significantly less vulnerable to outside harm.

6.4.1.4.1 Encoding Mechanism

The *ini* file to be loaded and retrieved is available with or without encoding. When an encoded *ini* file is downloaded to the MG 3200, it is retrieved as encoded from the MG 3200 as well. When a decoded file is downloaded to the MG 3200, it is retrieved as decoded from the MG 3200 as well.

In order to create an encoded *ini* file, the user must first create an *ini* file and then apply the **DConvert** utility to it in order to encode it. (Refer to the Appendix, "Utilities" on page 353 for detailed instruction on *ini* file encoding.)

In order to decode an encoded *ini* file retrieved from the MG 3200, the user must retrieve an encoded *ini* file from the MG 3200 using the Web server (refer to "Downloading Auxiliary Files" below) and then use the **DConvert** utility in order to decode it. (Refer to the ' Appendix, " Utilities' on page 353 for detailed instruction on decoding the *ini* file.)

Downloading the *ini* file with or without encoding may be performed by utilizing either TFTP or HTTP.

6.4.2 Auxiliary Files

The auxiliary files are *dat* files each containing the raw data used for a certain task such as Call Progress Tones, Voice Prompts, logo image, etc. *dat* files are created using the DConvert utility (refer to the Appendix, "Utilities" on page 353), which converts auxiliary source files into *dat* files. Some sample auxiliary source files are available in the software package CD. These *dat* files are downloaded to the MG 3200 using TFTP (see below) or HTTP via the Software Upgrade Wizard (refer to "Upgrading MG 3200 Software" on page 80.) This section describes the various types of auxiliary files.

Note: The auxiliary source files use the same *ini* file extension type as the *ini* configuration file, however, the functionality is different. When ever the term, "*ini* file" is used, it refers to the configuration file and NOT to the auxiliary files.

6.4.2.1 Downloading Auxiliary Files via TFTP During the Board Startup

Each auxiliary file has a corresponding *ini* file parameter in the form of [AuxilaryFileType]FileName. This parameter takes the name of the auxiliary file to be downloaded to the MG 3200. If the *ini* file does not contain a parameter for a specific auxiliary file type, the MG 3200 uses the last auxiliary file that was stored on the non-volatile memory. The SaveConfiguration *ini* file parameter enables storing the auxiliary files on the non-volatile memory.

The following list contains the *ini* file parameters for the different types of auxiliary files that can be downloaded to the MG 3200:

- "VoicePromptsFileName" - The name (and path) of the file containing the voice prompts. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the MG 3200. The Voice Prompt buffer size in the board is 10 Mbyte.

  The Voice Prompt buffer size is also controlled by the feature key. For more information contact an Nortel representative.

- "CallProgressTonesFilename" - The name (and path) of the file containing the Call Progress and User-Defined Tones definition.

- "PrerecordedTonesFileName" - The name (and path) of the file containing the Prerecorded Tones. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the MG 3200

- "CoderTblFilename" - The name (and path) of the file containing the supported coders definition.

- CASFileName_0"…"CASFileName_7" (or "CASFileName") - The names (and path names) of the files containing the CAS protocol configuration. It is possible to use 1 to 8 files. The "CASFileName" name is still supported and can be used instead of the enumerated names when using only one CAS protocol file.

- "CASTablesNum" - Indicates how many CAS protocol configuration files are loaded. Its range is 1-8. It should match the number of "CASFileName_X" fields.

- CASTableIndex_TrunkNum (TrunkNum should be an integer) - This field is a CAS protocol file index. It indicates the CAS protocol file to use in a specific Trunk. The index value corresponds to the number in the field "CASFileName_X".

- SaveConfiguration - (default = 1 = enabled) This parameter replaces the following parameters: BlastCallProgressSetupFile, BlastCASProtocolSetupFile, BlastVoicePromptsFile. When enabled, all configuration and downloadable files are stored in non-volatile memory.

6.4.2.2 Call Progress Tone and User-Defined Tone Auxiliary Files

The auxiliary source file for Call Progress Tones and User-Defined Tones contains the definitions of the Call Progress Tones and User-Defined Tones to be detected/generated by the MG 3200. The Call Progress Tones are mostly used for Telephony In-Band Signaling applications (e.g., Ring Back tone) Each tone can be configured as one of the following types:

- Continuous
- Cadence (up to 4 cadences)
- Burst

A tone can also be configured for Amplitude Modulated (AM) (only 8 of the Call Progress Tones can be AM tones). The Call Progress Tones frequency range is 300 Hz to 1890 Hz.

The User-Defined Tones are general purpose tones to be defined by the user. They can be set only as 'Continuous' and their frequency range is 300 Hz to 3800 Hz. The maximum amount of tones that may be configured for the User Defined and Call Progress Tones together is 32. The maximum frequencies that may be configured in the User Defined and Call Progress Tones together is 64. The MG 3200 sample configuration file supplied by Nortel can be used to construct your own file.

The Call Progress Tones and User-Defined Tones file used by the MG 3200 is a binary file with the extension *tone.dat*. Only this binary *tone.dat* file can be loaded to a MG 3200. Users can generate their own *tone.dat* file by opening the modifiable *tone.ini* file (supplied with the *tone.dat* file as part of the software package on the CD accompanying the MG 3200) in any text editor, modify it, and convert the modified *tone.ini* back into a binary *tones.dat* file using the DConversion Utility supplied with the MG 3200 software package. (Refer to the Appendix, "Utilities" on page 353 for a description of the procedure for generating and downloading the Call Progress Tone file using this utility.)

To load the Call Progress Tones and User-Defined Tones configuration file to the MG 3200, correctly define their parameters in the MG 3200's *ini* file. (Refer to' 'Initialization ('*ini*') Files" on page 59 for the *ini* file structure rules and *ini* file example.)

6.4.2.2.1 Format of the Call Progress Tones Section in the Auxiliary Source File

The format of the Call Progress Tones section in the auxiliary source file starts from the following string:

[NUMBER OF CALL PROGRESS TONES] - containing the following key only:

- **Number of Call Progress Tones** - defines the number of Call Progress Tones to be defined in the file.

[CALL PROGRESS TONE #X] - containing the Xth tone definition (starting from 0 and not exceeding the number of Call Progress Tones -1 defined in the first section) using the following keys:

- **Tone Type** - Call Progress Tone type

  Basic Tone Type Indices

  1. Dial Tone
  2. Ringback Tone
  3. Busy Tone
  4. Congestion Tone
  5. N/A
  6. Warning Tone
  7. Reorder Tone
  8. Confirmation Tone
  9. Call Waiting Tone

- **Tone Modulation Type** – The tone may be either Amplitude Modulated (1) or regular (0).
- **Tone Form** – The format of the tone may be one of the following indices:
  - Continuous
  - Cadence
  - Burst
- **Low Freq [Hz]** - Frequency in Hertz of the lower tone component for a dual frequency tone, or the frequency of the tone for a single tone. This parameter is relevant only in case the tone is not Amplitude Modulated.
- **High Freq [Hz]** - Frequency in Hertz of the higher tone component for of a dual frequency tone, or zero (0) for a single tone. This parameter is relevant only in case the tone is not modulated.
- **Low Freq Level [-dBm]** - Generation level 0 dBm to -31 dBm. This parameter is relevant only in case the tone is not Amplitude Modulated.
- **High Freq Level [-dBm]** - Generation level. 0 to -31 dBm. The value should be zero (0) for a single tone. This parameter is relevant only in case the tone is not Amplitude Modulated.
- **First Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the first cadence ON-OFF cycle, for cadence tone. When a tone is configured to be continuous, this parameter defines the tone On event detection time. When a tone is configured to be burst tone, it defines the tone's duration.
- **First Signal Off Time [10 msec]** - "Signal Off" period (in 10 msec units) for the first cadence ON-OFF cycle, for cadence tone. In case of burst tone, this parameter defines the off time required after burst tone ended until the tone detection is reported. For a continuous tone, this parameter is ignored.
- **Second Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the second cadence ON-OFF cycle. This may be omitted if there is no second cadence.
- **Second Signal Off Time [10 msec]** - "Signal Off" period (in 10 msec units) for the second cadence ON-OFF cycle. This may be omitted if there is no second cadence.

- **Third Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the third cadence ON-OFF cycle. This may be omitted if there is no third cadence.
- **Third Signal Off Time [10 msec]** - "Signal Off" period (in 10 msec units) for the third cadence ON-OFF cycle. This may be omitted if there is no third cadence.
- **Forth Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the forth cadence ON-OFF cycle. This may be omitted if there is no forth cadence.
- **Forth Signal Off Time [10 msec]** - "Signal Off" period (in 10 msec units) for the forth cadence ON-OFF cycle. This may be omitted if there is no forth cadence.
- **Carrier Freq [Hz]** – the Carrier signal frequency in case the tone is Amplitude Modulated.
- **Modulation Freq [Hz]** – The Modulated signal frequency in case the tone is Amplitude Modulated (valid range from 1 Hz to 128 Hz).
- **Signal Level [-dBm]** – the tone level in case the tone is Amplitude Modulated.
- **AM Factor [steps of 0.02]** – Amplitude modulation factor. Valid values: 1 to 50. Recommended values: 10 to 25.
- **Default Duration [msec]** - The default duration (in 1 msec units) of the generated tone.

Note 1: When defining the same frequencies for both a continuous tone and a cadence tone, the Signal On Time parameter of the continuous tone should have a value that is greater than the Signal On Time parameter of the cadence tone. Otherwise the continuous tone is detected instead of the cadence tone.

Note 2: The tone frequency should differ by at least 40 Hz from one tone to other defined tones**.**

Note 3: For more information on generating the Call Progress Tones Configuration file, refer to 'Converting a CPT *ini* File to a Binary *dat* File' in the Appendix, 'Utilities'.

Note 4: When constructing a CPT *dat* file, the **Use dBm units for Tone levels** checkbox must be marked. This checkbox enables defining the levels in [-dBm] units.

6.4.2.2.2 Format of the User Defined Tones Section

The format of the User Defined Tones section of the Call Progress Tone source auxiliary file starts from the following string:

[NUMBER OF USER DEFINED TONES] - containing the following key only:

- *Number of User Defined Tones* - defines the number of User Defined Tones to be defined in the file.

[USER DEFINED TONE #X] - containing the Xth tone definition (starting from 0 and not exceeding the number of User Defined Tones -1 defined in the first section) using the following keys:

- **Tone Type** – User Defined Tone type

  Basic Tone Type Indices

1. Dial Tone
2. Ringback Tone
3. Busy Tone
4. Congestion Tone
5. N/A
6. Warning Tone
7. Reorder Tone
8. Confirmation Tone
9. Call Waiting Tone

- **Low Freq [Hz]** - Frequency in Hertz of the lower tone component for a dual frequency tone, or the frequency of the tone for a single tone.
- **High Freq [Hz]** - Frequency in Hertz of the higher tone component for of a dual frequency tone, or zero (0) for a single tone.
- **Low Freq Level [-dBm]** - Generation level 0 dBm to -31 dBm.
- **High Freq Level [-dBm]** - Generation level. 0 to -31 dBm. The value should be zero (0) for a single tone.
- **Default Duration [msec]** - The default duration (in 1 msec units) of the generated tone.

6.4.2.2.3 Default Template for Call Progress Tones

The MG 3200 is initialized with the default Call Progress Tones configuration. To change one of the tones, edit the default call *progress txt* file. The table below lists the default call progress tones.

Table 6-7: Default Call Progress Tones

[NUMBER OF CALL PROGRESS TONES] **Number of Call Progress Tones=9**	
#Dial tone [CALL PROGRESS TONE #0]	Tone Type=1 Tone Form = 1 (Continuous) Low Freq [Hz]=350 High Freq [Hz]=440 Low Freq Level [-dBm]=13 (-13dBm) High Freq Level [-dBm]=13 First Signal On Time [10msec]=300

Table 6-7: Default Call Progress Tones

[NUMBER OF CALL PROGRESS TONES] **Number of Call Progress Tones=9**	
#Dial tone [CALL PROGRESS TONE #1]	Tone Type=1 Tone Form = 1 (Continuous) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=10 (-10dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=300
#Ringback [CALL PROGRESS TONE #2]	Tone Type=2 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=480 Low Freq Level [-dBm]=19 (-19dBm) High Freq Level [-dBm]=19 First Signal On Time [10msec]=200 First Signal Off Time [10msec]=400
#Ringback [CALL PROGRESS TONE #3]	Tone Type=2 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=16 (-16dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=100 First Signal Off Time [10msec]=300
#Busy [CALL PROGRESS TONE #4]	Tone Type=3 Tone Form = 2 (Cadence) Low Freq [Hz]=480 High Freq [Hz]=620 Low Freq Level [-dBm]=24 (-24dBm) High Freq Level [-dBm]=24 First Signal On Time [10msec]=50 First Signal Off Time [10msec]=50

Table 6-7: Default Call Progress Tones

[NUMBER OF CALL PROGRESS TONES] **Number of Call Progress Tones=9**	
#Busy [CALL PROGRESS TONE #5]	Tone Type=3 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=50 First Signal Off Time [10msec]=50
#Reorder tone [CALL PROGRESS TONE #6]	Tone Type=7 Tone Form = 2 (Cadence) Low Freq [Hz]=480 High Freq [Hz]=620 Low Freq Level [-dBm]=24 (-24dBm) High Freq Level [-dBm]=24 First Signal On Time [10msec]=25 First Signal Off Time [10msec]=25
#Confirmation tone [CALL PROGRESS TONE #7]	Tone Type=8 Tone Form = 2 (Cadence) Low Freq [Hz]=350 High Freq [Hz]=440 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=20 First Signal On Time [10msec]=10 First Signal Off Time [10msec]=10
#Call Waiting Tone [CALL PROGRESS TONE #8]	Tone Type=9 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=30 First Signal Off Time [10msec]=900

6.4.2.2.4 Modifying the Call Progress Tones File

Customers are supplied with modifiable Call Progress Tone auxiliary source files (with *ini* file extension) and non-modifiable Call Progress Tone *dat* binary files in the software package under **Tones**.

Only the binary *dat* file can be sent to the MG 3200.

In the auxiliary source file, customers can modify Call Progress Tone levels, Call Progress Tone frequencies to be detected/generated by the MG 3200, to suit customer-specific requirements. An example of a Call Progress Tone *ini* file name is *call_progress_defaults.dat*. Note that the word 'tones' is defined in the Call Progress Tone *ini* file name, to differentiate it from the MG 3200's *ini* file.

The default call progress tones configuration is found on call_progress_defaults.ini file. To change one of the tones, edit the default call progress txt file.

For example: to change the dial tone to 440 Hz only, replace the #Dial tone section in the table below with the following text:

#Dial tone

[CALL PROGRESS TONE #1]

Tone Type=1

Tone Form = 1

Low Freq [Hz]=440

High Freq [Hz]=0

Low Freq Level [-dBm]=10 (-10dBm)

High Freq Level [-dBm]=0

First Signal On Time [10msec]=300; the dial tone is detected after 3 sec

Users can specify several tones of the same type using Tone Type definition. These additional tones are used only for tone detection. Generation of specific tone is according to the first definition of the specific tone. For example, the user can define an additional dial tone by appending the second dial tone definition lines to the tone *ini* file. The MG 3200 reports dial tone detection if either one of the two tones is detected.

➢ To modify these *ini* files and send the *dat* file to the MG 3200, take these 4 steps:

1. Open the CPT *ini* file (it opens in **Notepad** or in a customer-defined text file editor.)
2. Modify the file in the text file editor according to your specific requirements.
3. Save your modifications and close the file.
4. Convert the file with the DConversion Utility into a binary dat file (refer to "Converting a Modified CPT *ini* File to a *dat* File with the Download Conversion Utility" below).

6.4.2.2.5 Converting a Modified CPT ini File to a dat File with the Download Conversion Utility

After modifying the original CPT *ini* file (supplied with the MG 3200's software package), you can use the Download Conversion Utility to convert the modified file into a *dat* binary file. You can only send the *dat* file to the MG 3200. The *ini* file cannot be sent.

To convert a modified CPT *ini* file to a binary *dat* file, Run the executable Download Conversion Utility file, *DConvert240.exe.* For more information, refer to the Appendix,' 'Utilities'' on page 353.

After making the *dat* file, send it to the MG 3200 using one of the folliwing:

- The Embedded Web Server GUI's Auxiliary Files. (Refer to ''Auxiliary Files Download'' on page 199.)

  or

- The BootP/TFTP Server to send to the MG 3200 the MG 3200's *ini* file (which simultaneously downloads the Call Progress Tone *dat* file, provided that the MG 3200's *ini* file parameter CallProgressTonesFilename is defined and provided that both files are located in the same directory.) (Refer to the Appendix, ''BootP/TFTP Server'' on page 223).

6.4.2.3 Playing Prerecorded Tones (PRT)

The Call Progress Tones and the User-Defined Tones mechanisms have several limitations such as limited number of predefined tones, or limited number of frequency integrations in one tone. To solve these problems and provide a more flexible tone generation capability, prerecorded tones and play can be downloaded to the MG 3200 and be played using regular tones generation commands.

6.4.2.3.1 PRT File Configuration

The PRT file that should be downloaded to the MG 3200 is a binary dat file, which was created using The DConvert utility. The tones should be recorded (or created using a Signaling Editor) if the user intends to download them in separate PCM files. The PCM files should include the following characteristics:

- Coder: G.711 A-law, G.711 µ -law or Linear PCM.
- Rate: 8 kHz
- Resolution: 8-bit
- Channels: mono

The PRT module plays the recorded tone repeatedly. This provides the ability to record only part of the tone, while still playing it for a full duration. For example, if a tone has a cadence of 2 seconds on and 4 seconds off, the recorded file should contain only the 6 seconds of the cadence. The PRT module repeatedly plays this cadence for the configured duration. In the same manner, a continuous tone can be played by repeating only part of it.

After the PCM files are properly prepared, these files should be converted into one *dat* file using the DConvert utility For more information regarding the DConvert utility, and how to make a *dat* PRT file, refer to the Appendix, ''BootP/TFTP Server'' on page 223.

Note: The maximum number of prerecorded tones that can be stored in one *dat* file is 40.

6.4.2.3.2 Downloading the PRT *dat* File

Downloading the PRT *dat* file into the MG 3200 can be done using one of the following:

- HTTP
- TFTP

For HTTP and TFTP download, refer to "Software Upgrade Wizard" on page 190.

Note 1: The maximum PRT buffer size is 1 MB.

Note 2: If the same tone type was defined as PRT and as Call Progress Tone or User-Defined Tone, the MG 3200 plays it using the PRT module.

6.4.2.4 Coder Table File

The Coders' Table file defines which coders are to be supported by the MG 3200. It is limited to the supported coders according to the loaded DSP template. Other coders can not be added.

The following is an example of an ini file that includes these Coder Table definitions.

This ini file is converted (using the **DConvert** utility) to a binary file, and loaded to the MG 3200. If no such file is loaded, the default settings are used.

```
[Internal name]     [Coder name] [Txpayload] [RxPayload] [Ptime]
            PCMA             PCMA           8           8       20
            PCMU             PCMU           0           0       20
        G726-16          G726-16          35          35       20
        G726-24          G726-24          36          36       20
        G726-32          G726-32           2           2       20
        G726-40          G726-40          38          38       20
     X-G727-16        X-G727-16          39          39       20
  X-G727-24-16     X-G727-24-16          40          40       20
     X-G727-24        X-G727-24          41          41       20
  X-G727-32-16     X-G727-32-16          42          42       20
  X-G727-32-24     X-G727-32-24          43          43       20
     X-G727-32        X-G727-32          44          44       20
  X-G727-40-16     X-G727-40-16          45          45       20
  X-G727-40-24     X-G727-40-24          46          46       20
  X-G727-40-32     X-G727-40-32          47          47       20
      G723HIGH             G723           4           4       30
       G723LOW             G723          80          80       30
          G729             G729          18          18       20
          G728             G728          15          15       20
         X-CCD            X-CCD          56          56       20
        iLBC13             iLBC         100         100       30
        iLBC15             iLBC         101         101       20
          BV16             BV16         102         102       20
        EVRC C             EVRC         103         103       20
telephone-event  telephone-event          96          96       20
           RED              RED         104         104       20
```

```
CN              CN          13          13      20
```

The first field is a text representation of the internal coder name. The second field is free text, and contains the name that is to be used in the SDP. The two payload fields define the default payload for this coder. The PTIME field defines the default to be used for this coder. The maximal value is the basic packet size (i.e., 20) multiplied by 6.

6.4.2.4.1 New Coders Introduced with the Table

- EVRC0 – This is actually not a new coder, it was called until now EVRC in our SDP. The correct name (according to RFC 3558) is EVRC0, as this is what our board supports.
- BV16 and iLBC – Both are supported for BCT only.

6.4.2.4.2 Coders Support Level

The application defines the following support levels for coders:

- None - A coder with support level "None" is not supported. An error is generated if an attempt is made to use the coder.
- Full - A coder with support level "Full" is valid for all type of calls.
- BCT - A coder with support level "BCT" (a new feature) is valid ONLY for BCT calls. The coders iLBC and BV16 belong to this feature. Other coders, that appears in the file, but are not supported in the current DSP template, also receive this support level.

The support level is defined internally by the board.

6.4.2.4.3 Converting a Modified CoderTable ini File to a dat File Using DConvert Utility

After modifying the original CoderTable (Tbl) *ini* file (originally supplied with the MG 3200's software package), you can use the **DConvert** Utility (*DConvert240.exe*) to convert the modified file into a *dat* binary file. (The *ini* file cannot be sent.) For more information, refer to the Appendix,' Utilities' on page 353. You can only send the *dat* file to the MG 3200.

After creating the *dat* file, send it to the MG 3200 using one of the following:

- The Embedded Web Server GUI's Auxiliary Files (Refer to 'Auxiliary Files Download' on page 199.)

or

- The BootP/TFTP Server - used to send the *ini* file (which simultaneously downloads the CoderTbl *dat* file, to the MG 3200, The *ini* file parameter CoderTblFilename must be enabled and both the ini file and CoderTbl *dat* file must be located in the same directory.) (Refer to the Appendix, 'BootP/TFTP Server' on page 223).

6.4.2.4.4 Default Coder Table (Tbl) ini file

The following is the default file for building the Coder Table (Tbl) *dat* file:

```
[Internal name]     [Coder name] [Txpayload] [RxPayload] [Ptime]
           PCMA             PCMA           8           8      20
           PCMU             PCMU           0           0      20
        G726-16          G726-16          35          35      20
        G726-24          G726-24          36          36      20
        G726-32          G726-32           2           2      20
        G726-40          G726-40          38          38      20
     X-G727-16        X-G727-16          39          39      20
  X-G727-24-16     X-G727-24-16          40          40      20
     X-G727-24        X-G727-24          41          41      20
  X-G727-32-16     X-G727-32-16          42          42      20
  X-G727-32-24     X-G727-32-24          43          43      20
     X-G727-32        X-G727-32          44          44      20
  X-G727-40-16     X-G727-40-16          45          45      20
  X-G727-40-24     X-G727-40-24          46          46      20
  X-G727-40-32     X-G727-40-32          47          47      20
      G723HIGH             G723           4           4      30
       G723LOW             G723          80          80      30
          G729             G729          18          18      20
          G728             G728          15          15      20
         X-CCD            X-CCD          56          56      20
  NETCODER_4_8       X-NETCODER          49          49      20
  NETCODER 5 6       X-NETCODER          50          50      20
  NETCODER 6 4       X-NETCODER          51          51      20
  NETCODER_7_2       X-NETCODER          52          52      20
    NETCODER 8       X-NETCODER          53          53      20
  NETCODER 8 8       X-NETCODER          54          54      20
  NETCODER_9_6       X-NETCODER          55          55      20
          EVRC             EVRC0          60          60      20
    X-EVRC-TFO       X-EVRC-TFO          81          81      20
    X-EVRC-TTY       X-EVRC-TTY          85          85      20
     X-QCELP-8        X-QCELP-8          61          61      20
 X-QCELP-8-TFO    X-QCELP-8-TFO          82          82      20
         QCELP            QCELP          62          62      20
   X-QCELP-TFO      X-QCELP-TFO          83          83      20
         G729E            G729E          63          63      20
      AMR_4_75              AMR          64          64      20
      AMR 5 15              AMR          65          65      20
       AMR 5 9              AMR          66          66      20
       AMR_6_7              AMR          67          67      20
       AMR 7 4              AMR          68          68      20
      AMR 7 95              AMR          69          69      20
      AMR_10_2              AMR          70          70      20
      AMR 12 2              AMR          71          71      20
         iLBC13             iLBC         100         100      30
         iLBC15             iLBC         101         101      20
           BV16             BV16         102         102      20
         EVRC C             EVRC         103         103      20
telephone-event telephone-event          96          96      20
            RED              RED         104         104      20
 X-MODEM-RELAY    X-MODEM-RELAY         254         254      20
            CN               CN          13          13      20
      Image/T38        Image/T38         254         254      20
```

6.4.3 Automatic Update Facility

The MG 3200 is capable of automatically downloading updates to the *ini* file, auxiliary files and firmware image. Any standard Web server may be used to host these files.

The Automatic Update processing is performed:

- Upon MG 3200 start-up (after the MG 3200 is operational)
- At a configurable time of day, e.g., 18:00 (disabled by default)
- At fixed intervals, e.g., every 60 minutes (disabled by default)

The Automatic Update process is entirely controlled by configuration parameters in the ini file. During the Automatic Update process, the MG 3200 contacts the external Web server and requests the latest version of a given set of URLs. Configuration ini files are downloaded only if they were modified since the last update.

The following is an example of an ini file activating the Automatic Update facility.

```
# DNS is required for specifying domain names in URLs
DnsPriServerIP = 10.1.1.11

# Load extra configuration ini file using HTTP
INIFILEURL = 'http://webserver.corp.com/Nortel/inifile.ini'
# Load call progress tones using HTTPS
# Note: HTTPS is not available on MP-104, MP-108, MP-124 platforms
CPTFILEURL = 'https://10.31.2.17/usa_tones.dat'
# Load voice prompts, using user "root" and password "wheel"
VPFILEURL = 'https://root:wheel@webserver.corp.com/vp.dat'

# Update every day at 03:00 AM
AutoUpdatePredefinedTime = '03:00'
```

Notes on Configuration URLs:

- Additional URLs may be specified, as described in the "System Parameters' table' on page 233.
- Updates to non-ini files are performed only once. To update a previously-loaded binary file, you must update the ini file containing the URL for the file.
- To provide differential configuration for each of the devices in a network, add the string "<MAC>" to the URL. This mnemonic is replaced with the hardware (MAC) address of the MG 3200.
- To update the firmware image using the Automatic Update facility, use the CMPFILEURL parameter to point to the image file. As a precaution (in order to protect the MG 3200 from an accidental update), you must also set AUTOUPDATECMPFILE to 1.

The following example illustrates how to utilize Automatic Updates for deploying devices with minimum manual configuration, for an "out of the box" experience.

➢ To utilize Automatic Updates for deploying the MG 3200 with minimum manual configuration, take these 4 steps:

1. Set up a Web server (in this example it is **http://www.corp.com/**) where all the configuration files are to be stored.
2. On each device, pre-configure the following setting: (DHCP/DNS are assumed)

```
INIFILEURL = 'http://www.corp.com/master configuration.ini'
```

3. Create a file named **master_configuration.ini**, with the following text:

```
# Common configuration for all devices
# ------------------------------------
CptFileURL = 'http://www.corp.com/call progress.dat'
# Check for updates every 60 minutes
AutoUpdateFrequency = 60

# Additional configuration per device
# -----------------------------------
# Each device will load a file named after its MAC address,
# e.g. config 00908F033512.ini
IniFileTemplateURL = 'http://www.corp.com/config <MAC>.ini'

# Reset the device after configuration has been updated.
# The device will reset after all files were processed.
RESETNOW = 1
```

4. You may modify the master_configuration.ini file (or any of the *config_<MAC>.ini* files) at any time. The MG 3200 queries for the latest version every 60 minutes, and applies the new settings immediately.

6.5 Backup Copies of ini and Auxiliary Files

Be sure to separately store a copy of the *ini* file and all auxiliary files, as well as a note of the software version for use should a board require replacement.

6.6 Upgrading MG 3200 Software

To upgrade the MG 3200's firmware, load the upgraded firmware cmp file into the MG 3200 (and optionally burn it into integral non-volatile memory) using:

1. Embedded Web Server - For a complete description of this option refer to "Software Upgrade Wizard" on page 190.
2. BootP/TFTP Server - By using the -fb BootP command line switch, the user can direct the board to burn the firmware on the non-volatile memory. The board thereby downloads the specified firmware name via TFTP and also “burns” the firmware on the non-volatile memory. Refer to the Appendix, "BootP/TFTP Server" on page 223.

Note: Upgrading the MG 3200's firmware requires reloading the *ini* file and reburning the configuration files. A Software Upgrade Key may be required if the new firmware's version is greater than that listed in the Software Upgrade Key menu (refer to' 'Software Upgrade Key Screen").

6.7 Software Upgrade Key

6.7.1 About the Software Upgrade Key

MG 3200s are loaded with a Software Upgrade Key already pre-configured for each of its TrunkPack Modules (TPM).

Users can later upgrade their MG 3200 features, capabilities and quantity of available resources by specifying what upgrades they require and the corresponding TPM's serial number (or MAC address), and ordering a new key to match their specification.

The Software Upgrade Key is sent as a string in a text file, to be loaded into the MG 3200. Stored in the MG 3200's non-volatile flash memory, the string defines the features and capabilities allowed by the specific key purchased by the user. The MG 3200 allows users to utilize *only these* features and capabilities. A new key overwrites a previously installed key.

Note: The Software Upgrade Key is an encrypted key. Each TPM utilizes a unique key. The Software Upgrade Key is provided by Nortel only.

6.7.2 Backing up the Current Software Upgrade Key

Back up your current Software Upgrade Key before loading a new key to the MG 3200. You can always reload this backed-up key to restore your MG 3200 capabilities to what they originally were if the 'new' key does not comply with your requirements.

➢ To backup the current Software Upgrade Key, take these 5 steps:

1. Access the MG 3200's Embedded Web Server (refer to the "Embedded Web Server" on page 141).
2. Click the **Software Update** button.
3. Click the **Software Upgrade Key** tab. The Software Upgrade Key screen is displayed (shown in the figure, 'Software Upgrade Key Screen' below).
4. Copy the string from the **Current Key** field and paste it in a new file.
5. Save the text file with a name of your choosing.

6.7.3 Loading the Software Upgrade Key

After receiving the Software Upgrade Key file (do not modify its contents in any way), ensure that its first line is [LicenseKeys] and that it contains one or more lines in the following format:

S/N<Serial Number of TPM> = <long Software Upgrade Key>

For example: S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj...

One S/N must match the S/N of your MG 3200 module (TPM). The MG 3200's S/N can be viewed in the Device Information screen (refer to "Device Information" on page 188).

You can load a Software Upgrade Key using:

- The Embedded Web Server (refer to "Loading the Software Upgrade Key Using the Embedded" below).
- The BootP/TFTP configuration utility (refer to "Loading the Software Upgrade Key Using BootP/TFTP" on page 83).
- The EMS (refer to the EMS User's Manual or EMS Product Description).

6.7.3.1 Loading the Software Upgrade Key Using the Embedded Web Server

➢ To load a Software Upgrade Key using the Web Server, take these 7 steps:

1. Access the MG 3200's Embedded Web Server (refer to "Accessing the Embedded Web Server" on page 144).
2. Click the **Software Update** button.
3. Click the **Software Upgrade Key** tab; the Software Upgrade Key screen is displayed (shown in the figure, 'Software Upgrade Key Screen' below).
4. **When loading a single key S/N line to a MG 3200:**

   Open the Software Upgrade Key file (it should open in Notepad), select and copy the key string of the MG 3200's S/N and paste it into the Web field **New Key**. If the string is sent in the body of an Email, copy and paste it from there. Press the **Add Key** button.
5. **When loading a Software Upgrade Key text file containing multiple S/N lines to a MG 3200:**

   (Refer to the figure, "Example of a Software Upgrade Key File Containing Multiple S/N Lines" on page 83)

   Click the **Browse** button in the **Send "Upgrade Key" file from your computer to the device** field, and navigate to the Software Upgrade Key text file.
   Click the **Send File** button.

   The new key is loaded to the MG 3200, validated and if valid is burned to memory. The new key is displayed in the **Current Key** field.
6. **Validate the new key by scrolling through the 'Key features:' panel and verifying the presence / absence of the appropriate features.**
7. **After verifying that the Software Upgrade Key was successfully loaded, reset the MG 3200; the new capabilities and resources are active.**

Figure 6-2: Software Upgrade Key Screen

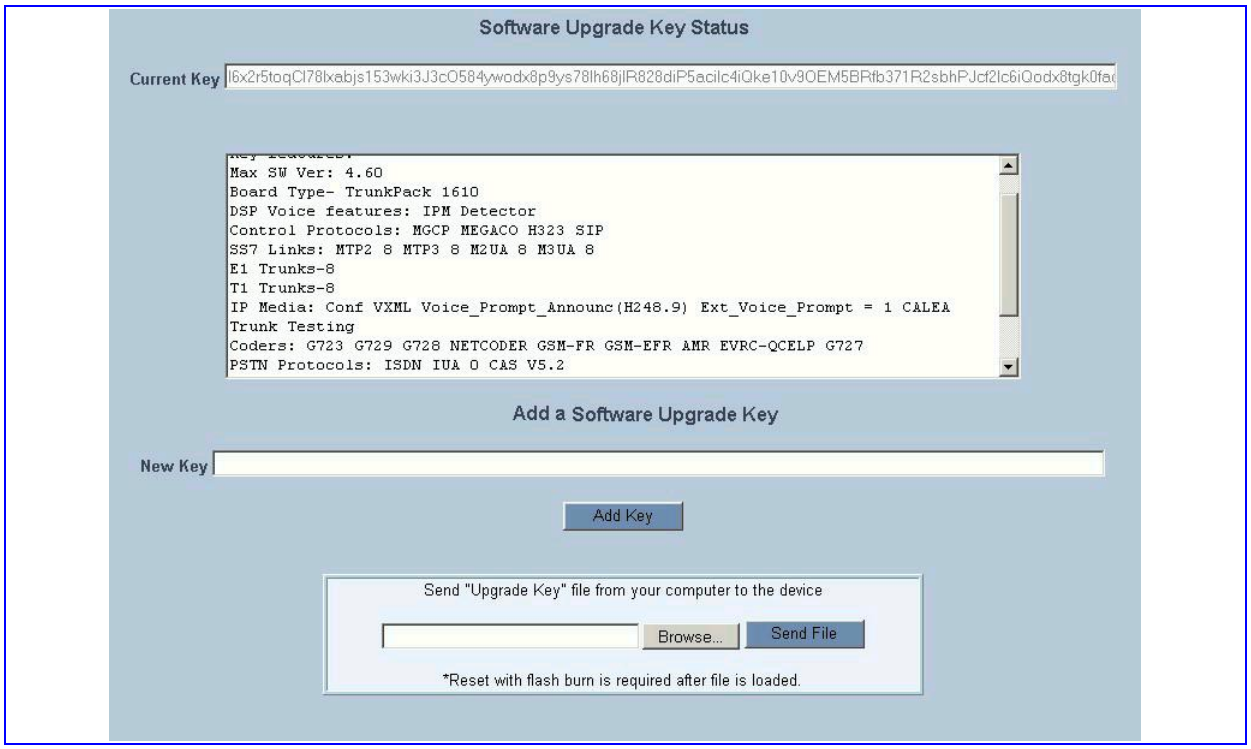
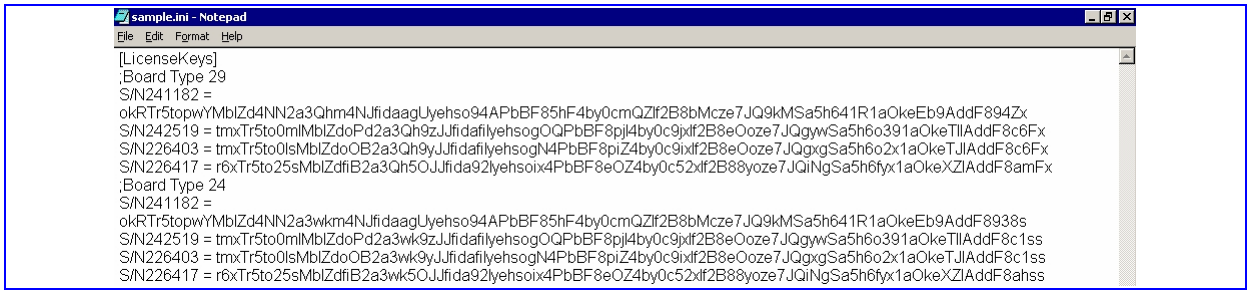


Figure 6-3: Example of a Software Upgrade Key File Containing Multiple S/N Lines



6.7.3.2 Loading the Software Upgrade Key Using BootP/TFTP

➢ **To load the Software Upgrade Key file using BootP/TFTP, take these 5 steps:**

1. Place the file in the same location you've saved the *MG 3200's cmp* file.
2. Start the BootP/TFTP configuration utility and from the **Services** menu in the main screen, choose option **Clients**; the Client Configuration screen is displayed (refer to the' 'Client Configuration Screen" on page 229).
3. From the drop-down list in the **INI File** field, select the Software Upgrade Key file instead of the MG 3200's *ini* file. Note that the MG 3200's *cmp* file must be specified in the **Boot File** field.

4. Configure the initial BootP/TFTP parameters required, and click **OK** (refer to the Appendix, "BootP/TFTP Server" on page 223).

5. Reset the MG 3200; the MG 3200's *cmp* and Software Upgrade Key files are loaded to the MG 3200.

6.7.4 Verifying that the Key was Successfully Loaded

After installing the key, you can determine in the Embedded Web Server's read-only 'Key features:' panel (**Software Update** menu > **Software Upgrade Key**) (refer to Figure H-1) that the features and capabilities activated by the installed string match those that were ordered.

You can also verify that the key was successfully loaded to the MG 3200 by accessing the Syslog server. For detailed information on the Syslog server, refer to "Syslog" on page 209. When a key is successfully loaded, the following message is issued in the Syslog server:

"S/N___ Key Was Updated. The Board Needs to be Reloaded with *ini* file\n"

6.7.5 Troubleshooting an Unsuccessful Loading of a Key

If the Syslog server indicates that a Software Upgrade Key file was unsuccessfully loaded (the SN_ line is blank), take the following preliminary actions to troubleshoot the issue:

- Open the Software Upgrade Key file and check that the S/N line of the specific MG 3200 whose key you want to update is listed in it. If it isn't, contact Nortel.
- Verify that you've loaded the correct file and that you haven't loaded the MG 3200's *ini* file or the CPT *ini* file by mistake. Open the file and ensure that the first line is [LicenseKeys].
- Verify that you did not alter in any way the contents of the file.

6.7.6 Abort Procedure

Reload the key you backed-up in "Backing up the Current Software Upgrade Key" on page 81 to restore your device capabilities to what they originally. To load the backed-up key use the procedure described in "Loading the Software Upgrade Key".

Reader's Notes

7 Standard Control Protocols

7.1 General

MG 3200 can be controlled from a Media Gateway Controller (MGC) / Call Agent using standard H.238 (MEGACO Media Gateway Control).

7.2 H.248 (Media Gateway Control) Protocol

7.2.1 H.238 Overview

H.238 (MEGACO Media Gateway Control) Protocol is a standards-based network control protocol (based on IETF RFC 3015 and ITU-T H.248 V1). H.248 assumes a call control architecture where the call control intelligence is outside the MG 3200 and handled by an external Media Gateway Controller (MGC). H.248 is a master/slave protocol, where the MG 3200 is expected to execute commands sent by the Call Agent (another name for MGC).

The connection is handled using two elements: **Terminations** and **Contexts**. Termination is the basic element of the call. There is a physical Termination representing a physical entity (e.g., B-channel), and an ephemeral Termination representing the generated stream. To create a connection, a Context is used. A Context contains one or more Terminations, and describes the topology between the Terminations. A typical connection creation command creates a new Context and adds into it one physical Termination and one new (ephemeral) Termination. The ephemeral Termination parameters describe the media type and the stream direction (SendReceive, SendOnly or ReceiveOnly).

Since this is a standards-based control protocol, no special software library to enable users to construct their own Call Agent is provided. (Users can choose any of many such stacks are available in the market.)

7.2.2 Operation

7.2.2.1 Executing H.248 Commands

H.248 commands, received from an external Call Agent through the IP network, are decoded and executed in the MG 3200. Both text encoding and binary encoding are supported. Commands can create new connections, delete connections, or modify the connection parameters.

Several commands that support the basic operations required to control a MG 3200:

- Status change command - The command ServiceChange allows changing the status of one or more Terminations. When used with a special Termination, called the ROOT Termination, it affects the entire MG 3200.
- Connection commands - The commands Add, Move, Modify and Subtract allow the creation and deletion of a call connection inside the MG 3200. These commands allow the application to create new connections, delete existing connections, and modify the connection parameters.

- Notify command - The Notify command is used by the MG 3200 to inform the Call Agent of events occurring on one of the Terminations.
- Audit commands - The AuditCapabilities and AuditValue commands are used to query the MG 3200 about Termination configuration and state. This information helps in managing and controlling the MG 3200.

A H.248-configured MG 3200 starts by sending a ServiceChange command to its primary MGC. If no response is received from it, the gateway goes on to the next MGC in its list. When an MGC accepts the MG 3200 registration, the session can start. Subsequently, the MG 3200 responds to MGC commands. Event notifications are sent only if the MGC requests them specifically.

7.2.2.2 KeepAlive Notifications From the Gateway

The Keep Alive notifications from the gateway to the MGC are implemented either using the proprietary mechanism via a NOP ServiceChange command (controlled by ini file parameters), or using the standard inactivity timer package (H.248.14).

For the proprietary mechanism via a NOP ServiceChange command there are two parameters:

- KeepAliveEnabled - activates or de-activate the Keep Alive function
- KeepAliveInterval - defines the inactivity period in seconds

If the KeepAlive mechanism is enabled, the MG 3200 sends a NOP ServiceChange command when it detects a defined period without commands from the MGC (the default period is 12 sec.) If no response is received from the MGC, the retransmission mechanism is initiated and eventually causes a new ServiceChange command to be sent to the next available MGC.

For the standard inactivity timer package (H.248.14) Inactivity detection is fully supported. The activation is by requesting the 'it/ito' event on the root termination. The 'mit' parameter of this event defines the inactivity period in 10 millisecond units. Note that this function is not set by configuration. The Call Manager must send a request for this event.

7.2.2.3 Setting H.248 Call Agent IP Address and Port

Users can provide the MG 3200 with up to 5 IP addresses of the H.248 Call Agents using the parameters, ProvisionedCallAgents and ProvisionedCallAgentsPorts.

The first Call Agent in the list is the primary one. In the case of a loss of connection, the MG 3200 tries to connect with the next on the list, and it continues trying until one of the Call Agents accepts the registration request. If the current connection is with a secondary MGC, the MG 3200 starts again from the primary MGC. The current Call Agent can override this setting by sending a ServiceChange command with a new IP address (not necessarily in the original list) and a HandOff method. If no CallAgent IP address exists, H.248 does not become operational.

Instead of defining an IP address, users can use a domain name for the Call Agent using the CallAgentDomainName parameter. When using it, define also the DNSPRIServerIP and DNSSECServerIP parameters. When using a domain name, the MG 3200 resolves the name on each disconnection, allowing the user to switch to another Call Agent.

7.2.2.4 Authorization Check of Call Manager IP Addresses

While the H.248 specification specifies that only one Call Manager can send commands to the gateway at a time, MG 3200 gateways handle the Authorization

Check in either of these modes:

1. No authorization check is performed. This mode specifies that every command is accepted and executed.
2. The IP address of the Call Manager sending the incoming command is checked against the list of provisioned Call Managers. If it matches one on the list, the command is executed. If The Call Manager' IP Address is not found on the list, an error message is sent. This mode is set as the default.

These two modes are controlled by the ini file parameter 'MEGACOCheckLegalityOfMGC', for which the default value is 1.

7.2.2.5 Support of DiffServ Capabilities

The DiffServ value of the IP header can be set for both the control path and the media path. The range of the DiffServ parameter is between 0 and 63. It enables routers to differentiate between different streams. The values are set via SNMP, Web or *ini* file parameter. Note, that changing the value of the control path requires the Gateway to be reset.

The value of the control path is set via the *ini* file parameter 'ControlDIFFSERV', and the value for the media path is set via the *ini* file parameter 'IPDIFFSERV'.

7.2.2.6 Handling Events

Events are declared in an EventsDescriptor that has an ID and a list of events on which the Call Agent requires notification. Up to 16 events can be defined in the descriptor. Wildcards are permitted in the events names. For example, if the list includes **dd/***, and the user presses the number **1**, the Call Agent receives notification when the digit starts (dd/std{tl=d1}) and when it ends (dd/etd{tl=d1}). The event **dd/d1** is not sent, as it is included in the other two. An event can have parameters, for example, the KeepActive flag. When the event having the KeepActive flag is received, it does not stop the currently played signals.

An event can have an embedded descriptor in it. It can be a SignalsDescriptor (refer to "Playing Signals" below), a new EventDescriptor, or both. The embedded descriptor replaces the current descriptor.

7.2.2.7 Playing Signals

Signals in H.248 reside in a SignalsDescriptor. Only one signal is allowed in the descriptor as the MG 3200s cannot play more than one signal at a time. However, this one signal can be of the SignalList type. In which case, there can be up to 30 signals in the list, and they are played sequentially until the list ends or the execution is interrupted.

Interrupting the execution can be one of the following:

- Event - Only events required by the Call Agent stop the execution, and only if they do not have the KeepActive flag.
- New Signals Descriptor - Stops the execution, unless the same signal is received, and it has a KeepActive flag. If the old signal and the new signal are both signal lists and have the same ID, the new signal is ignored.
- Subtracting the termination from the call

When a signal is ended, a signal completion notification is sent only if:

- The signal has the NotifyCompletion parameter and the completion reason (TimeOut, Interrupted by Signal, Interrupted by Event) matches one of the NotifyCompletion parameters.
- The events descriptor contains the signal completion event (g/sc).

The notification includes the ID of the signal that was ended and the signal list ID if it was a signal list.

Signal duration can be defined as a parameter in the signal. If omitted, a default value is used (refer to the package's description in the beginning of this section).

Call Progress Tones must be defined by the user in a Call Progress Tones (CPT ID) file. An off-line utility is supplied to convert this file to a binary file. Each tone has a **toneId** in the file, used by H.248 when playing the signal. For the correlation between signal names and CPT file IDs, refer to the column, **Map to CPT File** of the table, 'Generic Media Package - G'.

When a CPT file is missing, the MG 3200 defines default values only for the following signals:

- Dial tone
- Ringing tone
- Busy tone

Announcements should also be prepared offline by users.

The following example shows a command that plays a list of announcements. When the list is finished, a notify command is sent:

```
MEGACO/1 [172.16.8.88]
T=207{
C = 1 {
Modify = gws0c1 {
  SG{SL=1234{an/apf{an=2},an/apf{an=3},an/apf{an=1,NC={TO,IBS}}}},
  E=1001 {g/sc}}}}
And the Notify request:
MEGACO/1 [10.2.229.18]:2944
T=2015{
C = 1 {
O-N=gws0c1{
OE=1001{19700101T00003542: g/sc{
Meth=TO,SigId=an/apf,SLID=1234}}}}}
```

7.2.2.8 Mediation

Mediation in H.248 connects two ephemeral terminations. This operation can be used by a Call Agent to connect users with different coders or to connect two types of users, such as ATM and RTP. The mediation operation requires up to two DSPs according to the following rules:

- When both users use the same coder, no DSP is allocated.
- When one user uses a G.711, one DSP is allocated for the other user.
- When both users use non-G.711 and different coders, two DSPs are allocated.

The mediation is created with a simple H.248 ADD command, with two ephemeral terminations, as shown in the following example:

```
MEGACO/1 [10.10.0.70]; Connect the streams,
Transaction = 2 {
   Context = $ {
                        Add =  $ {
                             Media {
                                    LocalControl {
                                      Mode = SendReceive,
                rtp/jit=70 },
                                Local {
v=0
m=audio $ RTP/AVP 0
c=IN IP4 $
                            },
                 Remote {
v=0
m=audio 4000 RTP/AVP 0
c=IN IP4 10.2.229.19
                                 }
                                  }
                               },
                        Add = $ {
                             Media {
                                    LocalControl {
                                      Mode = SendReceive,
              rtp/jit=70 },
          Local {
v=0
m=audio $ RTP/AVP 4
c=IN IP4 $
                            },
                 Remote {
v=0
m=audio 4010 RTP/AVP 4
c=IN IP4 10.2.229.19
 }}}}}
```

This example connects two RTP streams, one uses the G.711 coder and the other uses the G.723 coder.

7.2.2.9 CAS/R2 Support in H.248

The CAS/R2 trunk protocols are supported in H.248 by using the 'bcas' package defined in H.248.25, the 'icas' and 'casblk' packages defined in H.248.28 and 'icasc' package defined in H.248.29

Using these packages, the MG 3200 converts from the MFC-R2 protocol, which is a PSTN protocol, to the H.248 protocol, thereby bridging the PSTN world with the IP world.

Note: Currently only E1-MFCR2 protocol is supported, there is no R1 support or T1 support.

When H.248 and MFC-R2 protocols share control of a channel, their timings are synchronized so that H.248 commands do not cause damage to the MFC-R2 protocol's negotiation. For example, MFC-R2 protocol must work with the Echo Canceler in OFF state or else Multiple Frequency (MF) is not received correctly. Thus, if H.248 protocol receives a command to open a channel with the Echo Canceler ON and MFC-R2 protocol's negotiation is not yet finished, the entire negotiation could be damaged. To avoid this problem, the H.248 will not change the echo canceler state until the call was accepted by the answering side.

The actual call should start only after the accept signal is finished. (See the call flow of call start).

The application supports a special option called re-answer. In this option, the answering side can put down the phone, and pick it up again. The phone close will result with the 'icas/cb' event, but if the phone is taken up again, the 'bcas/ans' event will be sent. The timing of this action is defined by the MGC. It is the MGC responsibility to decide when the call should be disconnected by sending the 'icas/cf' signal. (refer to the figures below for the call flow of the call disconnect for the use of these signals and events).

Blocking the Bchannel is done by using the 'casblk' package. The 'blk' and 'ublk' events are reported only if the action was done by the remote side. The reason for this is that the local side already knows its status. Unfortunately, sometimes the MGC loses the state and needs to synchronize with the current status. The recommended command for this is to send the 'bcas/idle' signal, and ask for the 'bcas/idle' and 'casblk/blk' events. This results in idling the line in case of a partial call, and getting the current state of the line: Idle (After idling completed) or Blocked (If blocked by the other side).

Figure 7-1: H.248-R2 Call Start Flow Diagram

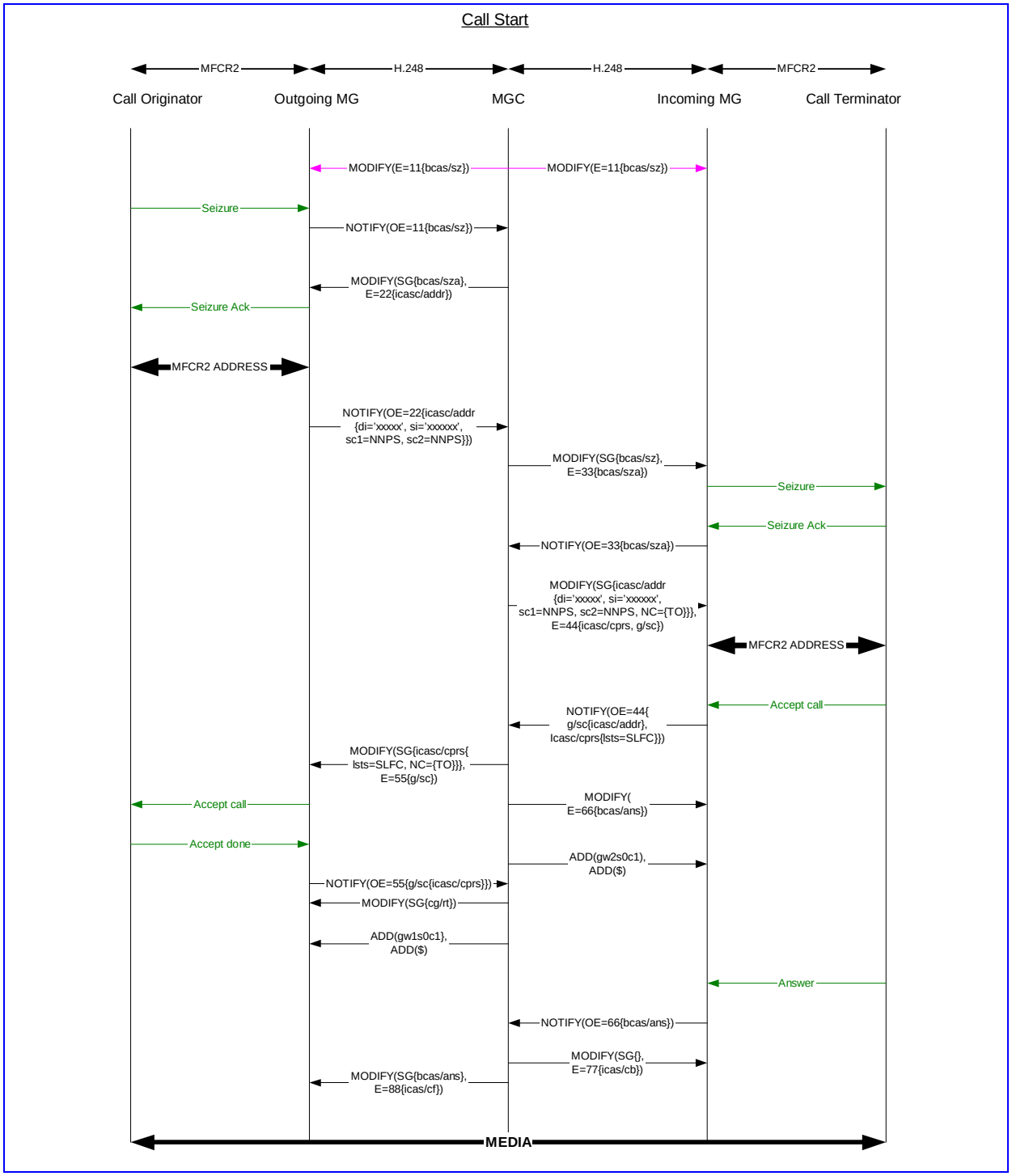
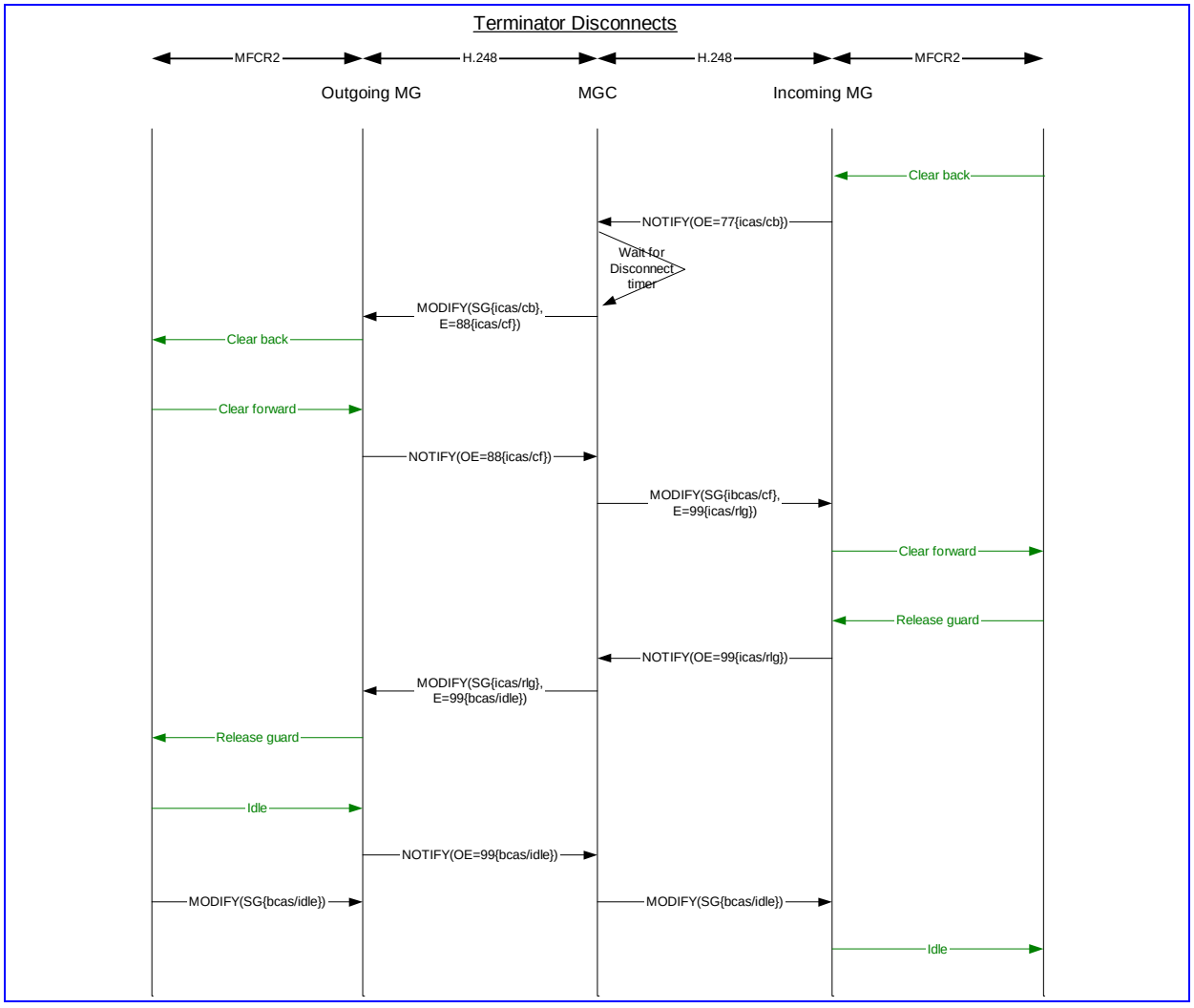


Figure 7-2: H.248-R2 Call Disconnect Flow Diagram



Note: The disconnection from the originator side looks the same. It only starts from the 'Clear forward' line signal. Also, even though the 'idle' notification is sent regardless of the 'bcas/idle' signal, this signal is still required for the internal state machine.

7.2.2.10 RFC 2833 Support

DTMF Transport Type can be set to use RFC 2833 through configuration or dynamically through H.248 commands.

Note: RFC 2833 support is only applicable when running Voice Over IP traffic. It is not relevant on Voice over ATM.

Configuration is performed through the *ini* file (the DTMFTransportType=3 parameter), or through the Web. This value is used by H.248 as the default value, but commands can override it.

To enable RFC 2833 via a command, add a payload type in the media line of the SDP and define this payload type to be RF 2833 according to the following example:

```
v=0
c= IN IP4 $
m=audio $ RTP/AVP 0 97
a=rtpmap:97 telephone-event 0-15
```

'telephone-event' is the name defined in RFC 2833, and 97 is used as the payload number (any number from the dynamic range can be used).

Negotiation is performed according to the following rules:

- If the remote side does not specify the 'telephone-event' in the SDP, the MG 3200 uses the default value as the transport type.
- If the local and remote payload types are different, the remote payload number is used.

Therefore, if a user needs to activate the RFC 2833 only when both sides agree on it, users should configure the default value to be different to RFC 2833 (e.g., Transparent).

7.2.2.11 Silence Suppression Support

1. Silence suppression can be enabled in two ways:
2. Configure it to ON through one of the configuration tools. This is a static way, and applies to all calls.
3. Use the SDP attribute a=silencesupp:on both for the local and remote side. This is done on a per call basis.
4. Silence suppression can be disabled by:
5. Setting it to OFF in the *ini* file. This is a static way, and applies to all calls.
6. For G.729 or G.723 - If the remote descriptor contains the a=fmtp line with annexb=no (G.729) or annexa=no (G.723). Note that the default for the **annex** fields in the SDP is **Yes**. Therefore, if this line is omitted, the assumption is that this side supports the silence suppression according to the annex.
7. Using the SDP attribute a=silencesupp:off in the local or remote side. This is performed on a per call basis. Note that the silencesupp attribute is specified only in RFC 3108 (SDP for ATM). However, as parsers ignore fields they do not recognize, it is legal to use it for IP also, assuming that the call manager is capable of doing it.
8. In all other cases, the MG 3200 default value is used.

The table below summarizes the operation of silence suppression:

Table 7-1: Silence Suppression Operation

CONFIG Setting	G.711	G.723	G.729
ON	ON only if: - a=silencesupp:on AND - payload 13 was offered on both sides	ON only if: - a=silencesupp:on AND - remote SDP does not contain the line a=fmtp:4 annexa=no	ON only if: a=silencesupp:on AND - remote SDP does not contain the line a=fmtp:18 annexb=no
OFF	OFF only if: - a=silencesupp:off	OFF only if: - a=silencesupp:off OR - remote SDP contains the line a=fmtp:4 annexa=no	OFF only if: - a=silencesupp:off OR - remote SDP contains the line a=fmtp:18 annexb=no

7.2.2.12 Fax T.38 and Voice Band Data Support (Bypass Mode)

Previous loads supported T.38 without H.248 interference, if the MG 3200 was configured to support T.38:

- FaxTransportType should be configured to T.38 Relay.
- Fax redundancy can be controlled using the configuration parameter FaxRelayRedundancyDepth. This parameter controls only non-V21 packets. For V21 packets that carry important data, the redundancy depth is hard-coded to be 4.
- The fax port is assumed to be the RTP port + 2, both for the local and remote side.

Following these rules, transition to T.38 is performed automatically upon detection.

Bypass (VBD) mode is also supported by using *ini* file parameters:

- FaxTransportType should be configured to be Bypass.
- The packetization period is configured by the parameter FaxModemBypassBasicRTPPacketInterval.
- The payload to be used is configured by the parameter FaxBypassPayLoadType and ModemBypassPayloadType.

Support of the Fax type (T.38, Bypass or Transparent) was added to the SDP according to the following rules:

- If the Call Manager wants this call to support T.38, it should send an additional line in the local SDP to the MG 3200, as in the following example:

```
v=0
c= IN IP4 $
m=audio $ RTP/AVP 0
m=image $ udptl t38
```

The first three lines describe the voice stream, and can differ according to the user's requirements. Attributes to the voice ('a' lines) should be added after the first 'm' line. The 'm=image' line, however, is mandatory, and should appear in the identical format to the above.

The MG 3200 returns a fully specified line with the local port used for the T.38.

- Fax redundancy can be requested by including the following attribute line after the 'm=image' line:

```
a=T38FaxUdpEC:T38UdpRedundancy
```

This parameter is only applicable for non-V21 packets. For V21 packets, the redundancy is hard coded 4.

Two modes of fax support are available. The modes are chosen by the value of bit 2 (value 4) of the H.248 profiling parameter MGCPCompatibilityProfile. If this bit is not set, the MG 3200 uses a positive negotiation:

- If the 'm=image' line is not received both in local AND in remote descriptors, the MG 3200 works with the defaults defined in the MG 3200. For example, if the MG 3200 is configured to work with T.38 (default setting) and the 'm=image' line is received in the local description only, the MG 3200 still works with T.38.
- If the fax redundancy attribute line does not appear both in local and remote descriptors, the MG 3200 uses the default value.

However, if bit 2 is set, the negotiation rules are as follows:

- If the 'm=image' line is not received both in local AND remote descriptors, T.38 is NOT used. In this case, if the local SDP "m=audio" line contains the G.711 coder, the fax and modem mode is Bypass (VBD), and the G.711 payload type is used for the fax. The modem payload type is still according to the ini file. If the G.711 coder is not offered in the local SDP, the Fax and modem Transport Type is Transparent.
- If the fax redundancy attribute line does not appear both in local and remote descriptors, redundancy for non-V21 packets is NOT used.

7.2.2.13 Digits Collection Support

The following methods for digit collection are supported:

- One by one collection using the single events in the 'dd' package (e.g., dd/d3).
- Collection according to digit map. This includes the basic collection 'dd/ce' event defined in the basic package and the 'xdd/xce' and 'edd/mce', both defined it H.248.16. The maximal pattern length is 150 bytes, and the maximal collected number is 30 digits. For the extended digit collection, the buffering of type ahead digits continues up to the limit of 30 digits. New digits after that are lost.

7.2.2.14 Reporting Fax Events

Some of the Fax events can be reported using the packages from H.248.2: "CTYP" and "IPFAX". The only Fax events reported by the "CTYP" package are the "V21flag" and "cng", using the "ctyp/dtone" event.

The reported Fax states are "CONNECTED" and "EOF". "CONNECTED" is reported when the H.248 application gets "EVENT_DETECT_FAX" from the board. "EOF" is reported when the H.248 application gets "EVENT_END_FAX" from the board.

The number of Fax pages is reported in the statistics descriptor when this descriptor is requested. The number of Fax pages can also be audited during the Fax.

7.2.3 SDP Support in H.248

H.248 supports basic SDP, as defined in RFC 2327. It also supports SDP-ATM, as defined in RFC 3108. The SDP parser can receive all lines defined in the RFC, but it ignores all but the following lines: 'v', 'c', 'm', 'a'.

In addition to the above four lines, the outgoing SDP can contain the 't' 's' 'o' lines, which are mandatory in some non-H.248 applications. This option is controlled by the *ini* file parameter MGCPCompatibilityProfile, by adding the number 8 to the current value (2). For the SDP to have these lines, set the *ini* file parameter to 10.

In the 'a' line, the only supported attributes in SDP are:

- SILENCESUPP:VAL
  (VAL=on or off) - To turn silence suppression on or off (defined in RFC 3108)

- RTPMAP
  Used for dynamic payload mapping, to map the number to the coder. The format is:

  a=rtpmap: 97 G723/8000/1

  Where: 97 is the payload number to be used
  G723 is the encoding name
  8000 is the clock rate (optional)
  1 is the number of channels (optional)

- FMTP
  Defines the dynamic payload mapping for the session. For example for where 97 is the payload number to be used and the bitrate is a G.723 coder parameter, the following line should be used:

  a=fmtp: 97 bitrate=5.3

  Other supported parameters are:

  mode-set - Defines for the AMR and the X-NETCODER coder,
  which mode is: used (0-7)

  annexa - Defines for G.723 if silence suppression is on (yes or no)

  annexb - Defines for G.729 if silence suppression is on (yes or no)

- PTIME
  Defines the packetization time for the session. For example for setting packetization time to 20 msec, the following line should be used:

  a=ptime: 20

7.2.3.1 Selecting a Coder or Ptime Using an Under-specified Local Descriptor

Before the current version, the supported under-specified fields in the SDP had been:

- IP address
- Port
- Payload

Added from the current version, the Profile and Ptime are also supported, as in the following example:

- c=IN IP4 $
- m=audio $ $ $
- a=ptime:$

The reply is a list of all supported coders.

7.2.3.2 Support of RFC 3407 – Simple Capabilities

RCF 3407 defines a minimal and backward-compatible capability declaration feature in SDP by defining a set of new SDP attributes. Together, these attributes define a capability set, which consists of a capability set sequence number followed by one or more capability descriptions. Each capability description in the set contains information about supported media formats, but the endpoint is not required to use any of these. In order to actually use a declared capability, session negotiation must be carried out by the call manager.

Example 1

The following call flows example illustrates the usage of this capability:

```
MEGACO/1 [10.2.1.228]:2944
Transaction = 10264 {
       Context = $ {
          Add  = $ {Media {
                       LocalControl {
                          Mode = Receiveonly
                       },
         Local {
   v=0
   c=IN IP4 $
   m=audio $ RTP/AVP 0
  m=image $ UDPTL t38
},
         Remote {
   v=0
   c=IN IP4 10.4.4.46
   m=audio 4020 RTP/AVP 0
}}}}}
```

The reply to this is:

```
MEGACO/1 [10.4.4.46]:2944
P=10264{
C=2{
A = gwRTP/1{
M{
L{

v=0
c=IN IP4 10.4.4.46
a=sqn: 0
a=cdsc: 1 image udptl t38
a=cpar: a=T38FaxMaxBuffer:1024
a=cpar: a=T38FaxMaxDatagram:238
m=audio 4010 RTP/AVP 0
a=ptime:20
a=silencesupp:off - - - -
}}}}}
```

In this case, the local was requested to use both audio and image, but the remote supports only the audio. The reply will return the image as a capability, in the session level.

Example 2

In this example the capabilities are displayed both in the session and in the media level:

```
MEGACO/1 [10.2.1.228]:2944
Transaction = 10265 {
       Context = $ {
          Add  = $ {Media {
                    LocalControl {
                       Mode = Receiveonly
                    },
         Local {
   v=0
   c=IN IP4 $
   m=audio $ RTP/AVP 0 18 4
  m=image $ UDPTL t38
},
         Remote {
   v=0
   c=IN IP4 10.4.4.46
   m=audio 4020 RTP/AVP 0
}}}}}
```

The reply to this is:

```
MEGACO/1 [10.4.4.46]:2944
P=10265{
C=3{
A = gwRTP/2{
M{
L{

v=0
c=IN IP4 10.4.4.46
a=sqn: 0
a=cdsc: 1 image udptl t38
a=cpar: a=T38FaxMaxBuffer:1024
a=cpar: a=T38FaxMaxDatagram:238
```

```
m=audio 4020 RTP/AVP 0
a=ptime:20
a=silencesupp:off - - - -
a=cdsc: 2 audio RTP/AVP 0 18 4
a=cpar: a=fmtp:18 annexb=yes
a=cpar: a=rtpmap:4 G723/8000/1
a=cpar: a=fmtp:4 bitrate=6.3;annexa=yes
a=cpar: a=ptime:20
a=cpar: a=silencesupp:off - - - -
}}}}}
```

In Example 2, the local was requested to use both audio and image, but the remote supports only the audio and parts of the coders. The reply returns the image as a capability in the session level and the fully supported coders in the media level.

7.2.3.3 Mapping Payload Numbers to Coders

The table below shows the default mapping between payload numbers and coders when the dynamic payload assignment **is not used.** Note that this is a general table and only the DSP template that is loaded to a MG 3200 defines which coder is supported on this MG 3200.

These values can be overridden by the external CoderTbl.

Table 32: MEGACO Mapping Payload Numbers to Coders

Default Payload Number	Encoding Name	Coder
0	"PCMU"	G711Mulaw
2	"G726-32"	G726_32
4	"G723"	G723 (High)
80	"G723"	G723 (Low)
8	"PCMA"	G711Alaw_64
15	"G728"	G728
18	"G729"	G729
35	"G726-16"	G726_16
36	"G726-24"	G726_24
38	"G726-40"	G726_40
39	"X-G727-16"	G727_16
40	"X-G727-24-16"	G727_24_16
41	"X-G727-24"	G727_24
42	"X-G727-32-16"	G727_32_16
43	"X-G727-32-24"	G727_32_24
44	"X-G727-32"	G727_32

Table 32: MEGACO Mapping Payload Numbers to Coders

Default Payload Number	Encoding Name	Coder
45	"X-G727-40-16"	G727_40_16
46	"X-G727-40-24"	G727_40_24
47	"X-G727-40-32"	G727_40_32
49	"X-NETCODER"	NetCoder_4_8
50	"X-NETCODER"	NetCoder_5_6
51	"X-NETCODER"	NetCoder_6_4
52	"X-NETCODER"	NetCoder_7_2
53	"X-NETCODER"	NetCoder_8
54	"X-NETCODER"	NetCoder_8_8
55	"X-NETCODER"	NetCoder_9_6
56	"X-CCD"	Transparent
60	"EVRC0"	EVRC0
81	"X-EVRC-TFO"	EVRC (TFO)
61	"X-QCELP-8"	QCELP_8
82	"X-QCELP-8-TFO"	QCELP_8_TFO
62	"QCELP"	QCELP_13
83	"X-QCELP-TFO"	QCELP_13_TFO
63	"G729E"	G.729E
64	"AMR"	AMR (4.75)
65	"AMR"	AMR (5.15)
66	"AMR"	AMR (5.9)
67	"AMR"	AMR (6.7)
68	"AMR"	AMR (7.4)
69	"AMR"	AMR (7.95)
70	"AMR"	AMR (10.2)
71	"AMR"	AMR (12.2)
100	“iLBC”	iLBC (13)
101	“iLBC”	iLBC (15)
102	“BV16”	BV16
96	“telephone-event”	RFC 2833

Table 32: MEGACO Mapping Payload Numbers to Coders

Default Payload Number	Encoding Name	Coder
104	"RED"	Redundancy per RFC 2198
13	"CN"	Comfort Noise

Note: When using dynamic payloads, do not use the MG 3200 default payloads for RFC 2833 (96) and RFC 2198 (104). If these values must be used, the default values for the two RFCs should be changed in the *ini* file.

7.2.4 Supported H.248 Packages

Events, signals, properties and statistics are grouped in packages. A package can be extended by a new package. In this case, the basic package becomes a part of the new package.

The TrunkPack series H.248 protocol supports the basic set of packages as defined in Annex E of RFC 3015 (Refer to the document at www.letf.org/rfc/, 'RFC Index'.), according to the device type. For example, the Analog Line package is supported only for analog devices.

Note: For H.248, the MGC must define ALL events for which it requires notification. There are NO persistent events in H.248.

7.2.4.1 Generic Media Package - G

Table 7-2: Generic Media Package - G

Symbol	Definition	Type
cause	General failure report	Event
sc	Signal completion	Event

Notes are for all H.248 Package tables:

S: The signal type; the following symbols identify the type of signal:

OO signal: The ON/OFF signal is turned ON until commanded by the Call Agent to turn it OFF, and vice versa.

TO signal: The Timeout signal lasts for a given duration unless it is superseded by a new signal.

BR signal: The Brief signal event has a short, known duration.

Duration: Specifies the duration of TO signals.

7.2.4.2 Base Root Package - ROOT

Table 7-3: Base Root Package - ROOT

Symbol	Definition	Type
maxNumberOfContexts	Maximum number of Contexts in the device	Property
maxTerminationsPerContext	Maximum Terminations in a Context	Property
normalMGExecutionTime	Timer for Retransmission	Property
normalMGCExecutionTime	Timer for Retransmission	Property
MGProvisionalResponseTimerValue	Timer for Retransmission	Property
MGCProvisionalResponseTimerValue	Timer for Retransmission	Property

7.2.4.3 Tone Generator Package - ToneGen

Table 7-4: Tone Generator Package - ToneGen

Symbol	Definition	Type	S	Duration
pt	Plays audio tone	Signal	TO	

7.2.4.4 Tone Detection Package - ToneDet

Table 7-5: Tone Detection Package - ToneDet

Symbol	Definition	Type
std	Detects the start of a tone	Event
etd	Detects the end of a tone	Event
ltd	Detects a long tone	Event

7.2.4.5 DTMF Generator Package - DG (Extends ToneGen)

Table 7-6: DTMF Generator Package - DG

Symbol	Definition	Type	S	Duration
d0	DTMF 0	Signal	BR	
d1	DTMF 1	Signal	BR	
d2	DTMF 2	Signal	BR	
d3	DTMF 3	Signal	BR	
d4	DTMF 4	Signal	BR	
d5	DTMF 5	Signal	BR	
d6	DTMF 6	Signal	BR	
d7	DTMF 7	Signal	BR	
d8	DTMF 8	Signal	BR	
d9	DTMF 9	Signal	BR	
ds	DTMF *	Signal	BR	
do	DTMF #	Signal	BR	
da	DTMF A	Signal	BR	
db	DTMF B	Signal	BR	
dc	DTMF C	Signal	BR	
dd	DTMF D	Signal	BR	

7.2.4.6 DTMF Detection Package - DD (Extends ToneDet)

Table 7-7: DTMF Detection Package - DD

Symbol	Definition	Type
ce	DigitMap Completion Event	Event
d0	DTMF 0	Event
d1	DTMF 1	Event
d2	DTMF 2	Event
d3	DTMF 3	Event
d4	DTMF 4	Event
d5	DTMF 5	Event
d6	DTMF 6	Event
d7	DTMF 7	Event
d8	DTMF 8	Event
d9	DTMF 9	Event
ds	DTMF *	Event
do	DTMF #	Event
da	DTMF A	Event
db	DTMF B	Event
dc	DTMF C	Event
dd	DTMF D	Event

7.2.4.7 Call Progress Tones Generator Package - CG (Extends ToneGen)

Table 7-8: Call Progress Tones Generator Package - CG

Symbol	Definition	Type	S	Duration	Map to CPT File
dt	Dial tone	Signal	TO	180 sec	1
rt	Ringing tone	Signal	TO	180 sec	2
bt	Busy tone	Signal	TO	180 sec	3
ct	Congestion tone	Signal	TO	180 sec	4
sit	Special Information tone	Signal	BR	2 sec	5
wt	Warning tone	Signal	BR	1sec	6
pt	Payphone Recognition tone	Signal	TO	180 sec	38
cw	Call Waiting tone	Signal	BR	1 sec	9
cr	Caller Waiting tone	Signal	TO	180 sec	15

7.2.4.8 Call Progress Tones Detection Package - CD (Extends ToneDet)

Table 7-9: Call Progress Tones Detection Package - CD

Symbol	Definition	Type
dt	Dial tone	Event
rt	Ringing tone	Event
bt	Busy tone	Event
ct	Congestion tone	Event
sit	Special Information tone	Event
wt	Warning tone	Event
pt	Payphone Recognition tone	Event
cw	Call Waiting tone	Event
cr	Caller Waiting tone	Event

7.2.4.9 Basic Continuity Package - CT

Table 7-10: Basic Continuity Package - CT

Symbol	Definition	Type	S	Duration	Map to CPT file
cmp	Detects test completion	Event			
ct	Initiates sending the tone	Signal	TO	2 sec	User Defined CO1
rsp	Responds to continuity test	Signal	TO	2 sec	

7.2.4.10 Network Package - NT

Table 7-11: Network Package - NT

Symbol	Definition	Type
jit	Maximal jitter buffer size	Property
netfail	Network failure	Event
qualert	Quality alert - Not supported	Event
dur	Termination's InContext duration	Statistics
os	Octets sent	Statistics
or	Octets received	Statistics

7.2.4.11 RTP Package - RTP (Extends - NT)

Table 7-12: RTP Package - RTP

Symbol	Definition	Type
pltrans	PayLoad Transition - Not supported	Event
ps	Packets sent	Statistics
pr	Packets received	Statistics
pl	Packet loss	Statistics
jit	Current inter-arrival jitter value	Statistics
delay	Current packets propagation delay	Statistics

7.2.4.12 TDM Circuit Package - TDMC (Extends - NT)

Table 7-13: TDM Circuit Package - TDMC

Symbol	Definition	Type
ec	Maximum Jitter Buffer size	Property
gain	Gain control	Property

7.2.4.13 Generic Announcement Package - AN

Table 7-14: Generic Announcement Package

Symbol	Definition	Type	Supported Parameters
apf	Initiates the play of a fixed announcement	Signal	An - Announcement number Di - The direction of the announcement Noc - Number of cycles
apv	Initiates the play of a variable announcement	Signal	Handled in the same manner as apf

7.2.4.14 Expanded Call Progress Tones Generator Package - XCG (Extends - ToneGen)

Table 7-15: Expanded Call Progress Tones Generator Package - XCG

Symbol	Definition	Type	S	Duration	Map to CPT File
cmft	Comfort tone	Signal	TO	180 sec	18
roh	Off-hook warning tone	Signal	TO	180 sec	16
nack	Negative Acknowledgement	Signal	TO	180 sec	19
vac	Vacant Number tone	Signal	TO	180 sec	20
spec	Special Conditions dial tone	Signal	TO	180 sec	21

7.2.4.15 Basic Service Tones Generation Package - SRVTN (Extends - ToneGen)

Table 7-16: Basic Service Tones Generation Package - SRVTN

Symbol	Definition	Type	S	Duration	Map to CPT File
rdt	Recall dial tone	Signal	TO	180 sec	22
conf	Confirmation tone	Signal	BR	1 sec	8
ht	Held tone	Signal	TO	180 sec	23
mwt	Message Waiting tone	Signal	TO	180 sec	17

7.2.4.16 Expanded Services Tones Generation Package - XSRVTN (Extends - ToneGen)

Table 7-17: Expanded Services Tones Generation Package - XSRVTN

Symbol	Definition	Type	S	Duration	Map to CPT File
xferdt	Call Transfer Dial Tone	Signal	TO	180 sec	24
cft	Call Forward Tone	Signal	BR	1 sec	25
ccst	Credit Card Service Tone	Signal	BR	1 sec	26
srdt	Special Recall Dial Tone	Signal	TO	180 sec	27

7.2.4.17 Basic CAS Package - BCAS

Table 7-18: Basic CAS Signal/Events

Symbol	Definition	Type	S	Duration	Map to CPT File	Symbol
sz	Seizure	Signal/ Event	BR		None	
sza	Seizure ack	Signal/ Event	BR		None	
ans	Answer	Signal/ Event	BR		None	
idle	idle	Signal/ Event	BR		None	
casf	CAS failure	Event	-		None	

7.2.4.18 International CAS Package – ICAS (Extends – BCAS)

Table 7-19: International CAS Signal/Events

Symbol	Definition	Type	S	Duration	Map to CPT File	Symbol
sls	Subscriber line status	Signal/ Event	BR		None	
cf	Clear forward	Signal/ Event	BR		None	
cb	Clear back	Signal/ Event	BR		None	
casf	CAS failure	Event	-		None	
rlg	Release Guard	Siganl/ Event			None	
Cng	Congestion	Signal/ Event	BR		None	

7.2.4.19 CAS Blocking Package - CASBLK

Table 7-20: CAS Blocking Signal/Events

Symbol	Definition	Type	S	Duration	Map to CPT File	Symbol
blk	Seizure	Signal/ Event	BR		None	
ublk	Answer	Event			None	

7.2.4.20 International CAS compelled Package - ICASC

Table 7-21: ICASC Signal/Events Table

Symbol	Definition	Type	S	Duration	Map to CPT File	Note
addr	Address	Signal/ Event	TO		None	
casf	CAS failure	Event	BR		None	
cprs	Called party reachability status	Signal/ Event	TO		None	
cng	Congestion	Signal/ Event	TO			

7.2.4.21 MF Generator Package - MFG (Extends - ToneGen)

Table 7-22: MF Generator Package - MFG

Symbol	Definition	Type	S	Duration
mf0	MF 0	Signal	BR	
mf1	MF 1	Signal	BR	
mf2	MF 2	Signal	BR	
mf3	MF 3	Signal	BR	
mf4	MF 4	Signal	BR	
mf5	MF 5	Signal	BR	
mf6	MF 6	Signal	BR	
mf7	MF 7	Signal	BR	
mf8	MF 8	Signal	BR	
mf9	MF 9	Signal	BR	
mfa	MF A	Signal	BR	
mfb	MF B	Signal	BR	
mfc	MF C	Signal	BR	
mfd	MF D	Signal	BR	
mfe	MF E	Signal	BR	
mff	MF F	Signal	BR	
mfg	MF G	Signal	BR	
mfh	MF H	Signal	BR	

7.2.4.22 MF Detection Package - MFD (Extends - ToneDet)

Table 7-23: MF Generator Package - MFG

Symbol	Definition	Type
mf0	MF 0	Event
mf 1	MF 1	Event
mf 2	MF 2	Event
mf 3	MF 3	Event
mf 4	MF 4	Event
mf 5	MF 5	Event
mf 6	MF 6	Event
mf 7	MF 7	Event
mf 8	MF 8	Event
mf 9	MF 9	Event
mfa	MF A	Event
mfb	MF B	Event
mfc	MF C	Event
mfd	MF D	Event
mfe	MF E	Event
mff	MF F	Event
mfg	MF G	Event
mfh	MF H	Event

7.2.4.23 Inactivity Timer Package - IT

Table 7-24: Inactivity Timer Package - IT

Symbol	Definition	Type
ito	Detects that inactivity timer has expired	Event

7.2.4.24 Basic Call Progress Tones Generator with Directionality Package - BCG (Extends ToneGen)

Table 7-25: Basic Call Progress Tones Generator with Directionality Package - BCG

Symbol	Definition	Type	S	Duration	Map to CPT File
bdt	Dial tone	Signal	TO	180 sec	1
brt	Ringing tone	Signal	TO	180 sec	2
bbt	Busy tone	Signal	TO	180 sec	3
bct	Congestion tone	Signal	TO	180 sec	4
bsit	Special Information tone	Signal	BR	2 sec	5
bwt	Warning tone	Signal	BR	1 sec	6
bpt	Payphone Recognition tone	Signal	TO	180 sec	38
bcw	Call Waiting tone	Signal	BR	1 sec	9
bcr	Caller Waiting tone	Signal	TO	180 sec	15
bpy	Pay tone	Signal	TO	180 sec	Not supported

7.2.4.25 Call Type Discrimination Package - CTYP

Table 7-26: Call Type Discrimination Package - CTYP

Symbol	Definition	Type
dtone	Discriminating tone detected	Event

7.2.4.26 IP Fax Package - IPFAX

Table 7-27: IP Fax Package - IPFAX

Symbol	Definition	Type
faxconnchange	Fax connection state changed (Only 'Connected' and 'EOF' are supported)	Event
pagestrans	Number of pages transferred	Statistics

7.2.4.27 Extended Digit Collection Package - XDD (Extends – DD)

Table 7-28: Extended digit collection Package - XDD

Symbol	Definition	Type
xce	Extended Digitmap Completion Event	Event

7.2.4.28 Enhanced Digits Collection Package - EDD

Table 7-29: Enhanced Digits Collection Package - EDD

Symbol	Definition	Type
mce	Matched Digitmap Completion Event	Event

7.2.5 H.248 Profiling

Profiling of various H.248 features is controlled via the *ini* file parameter MGCPCompatibilityProfile. Initially, only value **2** has been supported. (Values **0** is obsolete). Value **1** and **2** are the same and are for supporting H.248 version 1. Value **2** is the default value. Additional features are:

- Bit 2 (Value 4) -Controls the type of support for the Fax T.38 negotiation. (Refer to' 'Fax T.38 & Voice Band Data Support'' on page 96)
- Bit 3 (Value 8) - Enables the extra lines in the outgoing SDP ('t' 's' 'o' lines).' (Refer to 'SDP Support i'n H.248' on page 98.)
- Bit 4 (Value 16) - Enables the following features:
  - In the serviceChange request, the Timestamp parameter is omitted.
  - The audit command on ROOT termination with packages descriptor returns the total supported packages for the MG 3200.
  - The default packetization period (ptime) for the transparent coder is 10 milliseconds. Using the SDP attribute ptime can change this.
  - The packetization period for Bypass Fax mode is the same as the packetization period used for voice. If this bit is not set, the packetization period for the Fax Bypass is taken from the *ini* file.
  - When sending a notification transaction request, the MG 3200 does not mark it as optional.

7.2.6 H.248 Termination Naming

The basic entities controlled by H.248 protocol are called Terminations. Physical Terminations represent a physical entity and ephemeral Terminations represent the stream. Ephemeral Terminations exist only during a connection. From version 4.4, the terminations names are defined by a new set of pattern parameters, as described in the next section. Backward Compatibility is kept for the previous Terminations. (Refer to ''Backward Compatibility' on page 119'.)

7.2.6.1 Termination Name Patterns

Each termination type name is defined by an *ini* file or SNMP parameter. The pattern may contain acceptable characters as defined in H.248. The '*' character is used to represent the place where a digit should be. Therefore, it can not be part of the name itself. All other characters, including slash, are considered text.

For example: The pattern "gws*c*" matches the termination name "gws0c1" and also "gws10c20". The trunk numbers, in this case, are 0 and 10 and the channels are 1 and 20.

- PHYSTERMNAMEPATTERN - Pattern of the physical terminations.
- LOGICALRTPTERMPATTERN - Pattern for ephemeral terminations based on RTP stream.

The starting number of each level can be controlled by a set of parameters:

- EP_NUM - Controls the numbering of the physical terminations name pattern
- EP_NUM_0 - Defines the starting trunk number
- EP_NUM_1 - Defines the starting channel number
- RTP_NUM - Defines the starting number for the RTP terminations. (The default is 0)

7.2.6.2 Old Termination Naming Method

Physical Termination names have up to three components: Gateway (in this case the MG 3200) name, Trunk name and Endpoint name (for non-trunking gateways, the trunk field does not exist).

Ephemeral Termination names have two components: The gateway name and a constant string - 'RTP/' for RTP terminations and 'ATM/' for ATM terminations. So assuming that the MG 3200 name is 'gw', if the first ephemeral Termination is of RTP type, it is called 'gwRTP/1', and if it is of ATM type, it is called 'gwATM/1'.

Set the name parts using the following *ini* file parameters (the last two are used only for physical Terminations):

'GatewayName', 'TrunkName', 'EndpointName'.

Note that the '/' (the forward slash) should be part of the name used. It is not added automatically.

Note also that for trunking gateways, the 'TrunkName' can NOT be null. The default values for the Termination name parts for **Trunking boards** is the default gateway name, 'tgw/'; the default trunk name is 's' and the default Endpoint name is '/c'. So the Termination that represents B-channel 1 of trunk 0 is 'tgw/s0/c1'.

PSTN Interface - mapping Trunk/B-channel pairs to Endpoints is hardware-specific (refer to the table, "H.248 EndPoint Names" on page 119.) Note that the number of supported terminations per MG 3200 is equal to the channel density of the MG 3200.

LOGICALRTPTERMPATTERN = "gwrtp/*"

7.2.6.3 Backward Compatibility

The connection between the old naming parameters and the new ones is done by creating the name pattern from the old name parameters. Let's assume for example that the old name parameters are:

GATEWAYNAME = "gw"

TRUNKNAME = "s"

ENDPOINTNAME = "chan"

This is equivalent to the following new name parameters:

PHYSTERMNAMEPATTERN = "gws*chan*"

LOGICALRTPTERMPATTERN = "gwrtp/*"

7.2.6.4 Termination Mapping to a PSTN Interface

The table below describes the mapping between Endpoints and channels for a PSTN interface, according to the interface type used. The table below assumes the following initial values:

Channel density - 60

Gateway name = 'Acgw/'

Trunk name = 'T'

Endpoint name = '/C',

The table below lists only the names for a two trunks unit.

Table 7-30: H.248 Endpoint Names

Endpoint Name	E1 - PRI/CAS E1 - Transparent	E1 - Transparent 62	T1/J1 - PRI	T1/J1 - CAS T1/J1 - Transparent
Acgw/T0/C1	Trunk#0/TS1	Trunk#0/TS1	Trunk#0/TS1	Trunk#0/TS1
Acgw/T0/C2	Trunk#0/TS2	Trunk#0/TS2	Trunk#0/TS2	Trunk#0/TS2
Acgw/T0/C3	Trunk#0/TS3	Trunk#0/TS3	Trunk#0/TS3	Trunk#0/TS3
Acgw/T0/C4	Trunk#0/TS4	Trunk#0/TS4	Trunk#0/TS4	Trunk#0/TS4
Acgw/T0/C5	Trunk#0/TS5	Trunk#0/TS5	Trunk#0/TS5	Trunk#0/TS5
Acgw/T0/C6	Trunk#0/TS6	Trunk#0/TS6	Trunk#0/TS6	Trunk#0/TS6
Acgw/T0/C7	Trunk#0/TS7	Trunk#0/TS7	Trunk#0/TS7	Trunk#0/TS7
Acgw/T0/C8	Trunk#0/TS8	Trunk#0/TS8	Trunk#0/TS8	Trunk#0/TS8
Acgw/T0/C9	Trunk#0/TS9	Trunk#0/TS9	Trunk#0/TS9	Trunk#0/TS9
Acgw/T0/C10	Trunk#0/TS10	Trunk#0/TS10	Trunk#0/TS10	Trunk#0/TS10
Acgw/T0/C11	Trunk#0/TS11	Trunk#0/TS11	Trunk#0/TS11	Trunk#0/TS11
Acgw/T0/C12	Trunk#0/TS12	Trunk#0/TS12	Trunk#0/TS12	Trunk#0/TS12

Table 7-30: H.248 Endpoint Names

Endpoint Name	E1 - PRI/CAS E1 - Transparent	E1 - Transparent 62	T1/J1 - PRI	T1/J1 - CAS T1/J1 - Transparent
Acgw/T0/C13	Trunk#0/TS13	Trunk#0/TS13	Trunk#0/TS13	Trunk#0/TS13
Acgw/T0/C14	Trunk#0/TS14	Trunk#0/TS14	Trunk#0/TS14	Trunk#0/TS14
Acgw/T0/C15	Trunk#0/TS15	Trunk#0/TS15	Trunk#0/TS15	Trunk#0/TS15
Acgw/T0/C16	N/A	Trunk#0/TS16	Trunk#0/TS16	Trunk#0/TS16
Acgw/T0/C17	Trunk#0/TS17	Trunk#0/TS17	Trunk#0/TS17	Trunk#0/TS17
Acgw/T0/C18	Trunk#0/TS18	Trunk#0/TS18	Trunk#0/TS18	Trunk#0/TS18
Acgw/T0/C19	Trunk#0/TS19	Trunk#0/TS19	Trunk#0/TS19	Trunk#0/TS19
Acgw/T0/C20	Trunk#0/TS20	Trunk#0/TS20	Trunk#0/TS20	Trunk#0/TS20
Acgw/T0/C21	Trunk#0/TS21	Trunk#0/TS21	Trunk#0/TS21	Trunk#0/TS21
Acgw/T0/C22	Trunk#0/TS22	Trunk#0/TS22	Trunk#0/TS22	Trunk#0/TS22
Acgw/T0/C23	Trunk#0/TS23	Trunk#0/TS23	Trunk#0/TS23	Trunk#0/TS23
Acgw/T0/C24	Trunk#0/TS24	Trunk#0/TS24	N/A (D-channel)	Trunk#0/TS24
Acgw/T0/C25	Trunk#0/TS25	Trunk#0/TS25		
Acgw/T0/C26	Trunk#0/TS26	Trunk#0/TS26		
Acgw/T0/C27	Trunk#0/TS27	Trunk#0/TS27		
Acgw/T0/C28	Trunk#0/TS28	Trunk#0/TS28		
Acgw/T0/C29	Trunk#0/TS29	Trunk#0/TS29		
Acgw/T0/C30	Trunk#0/TS30	Trunk#0/TS30		
Acgw/T0/C31	Trunk#0/TS31	Trunk#0/TS31		
Acgw/T1/C1	Trunk#1/TS1	Trunk#1/TS1	Trunk#1/TS1	Trunk#1/TS1
Acgw/T1/C2	Trunk#1/TS2	Trunk#1/TS2	Trunk#1//TS2	Trunk#1/ /TS2
Acgw/T1/C3	Trunk#1/TS3	Trunk#1/TS3	Trunk#1/TS3	Trunk#1/TS3
Acgw/T1/C4	Trunk#1/TS4	Trunk#1/TS4	Trunk#1/TS4	Trunk#1/TS4
Acgw/T1/C5	Trunk#1/TS5	Trunk#1/TS5	Trunk#1/TS5	Trunk#1/TS5
Acgw/T1/C6	Trunk#1/TS6	Trunk#1/TS6	Trunk#1/TS6	Trunk#1/TS6
Acgw/T1/C7	Trunk#1/TS7	Trunk#1/TS7	Trunk#1/TS7	Trunk#1/TS7
Acgw/T1/C8	Trunk#1/TS8	Trunk#1/TS8	Trunk#1/TS8	Trunk#1/TS8
Acgw/T1/C9	Trunk#1/TS9	Trunk#1/TS9	Trunk#1/TS9	Trunk#1/TS9
Acgw/T1/C10	Trunk#1/TS10	Trunk#1/TS10	Trunk#1/TS10	Trunk#1/TS10

Table 7-30: H.248 Endpoint Names

Endpoint Name	E1 - PRI/CAS E1 - Transparent	E1 - Transparent 62	T1/J1 - PRI	T1/J1 - CAS T1/J1 - Transparent
Acgw/T1/C11	Trunk#1/TS11	Trunk#1/TS11	Trunk#1/TS11	Trunk#1/TS11
Acgw/T1/C12	Trunk#1/TS12	Trunk#1/TS12	Trunk#1/TS12	Trunk#1/TS12
Acgw/T1/C13	Trunk#1/TS13	Trunk#1/TS13	Trunk#1/TS13	Trunk#1/TS13
Acgw/T1/C14	Trunk#1/TS14	Trunk#1/TS14	Trunk#1/TS14	Trunk#1/TS14
Acgw/T1/C15	Trunk#1/TS15	Trunk#1/TS15	Trunk#1/TS15	Trunk#1/TS15
Acgw/T1/C16	N/A	Trunk#1/TS16	Trunk#1/TS16	Trunk#1/TS16
Acgw/T1/C17	Trunk#1/TS17	Trunk#1/TS17	Trunk#1/TS17	Trunk#1/TS17
Acgw/T1/C18	Trunk#1/TS18	Trunk#1/TS18	Trunk#1/TS18	Trunk#1/TS18
Acgw/T1/C19	Trunk#1/TS19	Trunk#1/TS19	Trunk#1/TS19	Trunk#1/TS19
Acgw/T1/C20	Trunk#1/TS20	Trunk#1/TS20	Trunk#1/TS20	Trunk#1/TS20
Acgw/T1/C21	Trunk#1/TS21	Trunk#1/TS21	Trunk#1/TS21	Trunk#1/TS21
Acgw/T1/C22	Trunk#1/TS22	Trunk#1/TS22	Trunk#1/TS22	Trunk#1/TS22
Acgw/T1/C23	Trunk#1/TS23	Trunk#1/TS23	Trunk#1/TS23	Trunk#1/TS23
Acgw/T1/C24	Trunk#1/TS24	Trunk#1/TS24	N/A (D-channel)	Trunk#1/TS24
Acgw/T1/C25	Trunk#1/TS25	Trunk#1//TS25		
Acgw/T1/C26	Trunk#1/TS26	Trunk#1/TS26		
Acgw/T1/C27	Trunk#1/TS27	Trunk#1/TS27		
Acgw/T1/C28	Trunk#1/TS28	Trunk#1/TS28		
Acgw/T1/C29	Trunk#1/TS29	Trunk#1/TS29		
Acgw/T1/C30	Trunk#1/TS30			
Acgw/T1/C31	Trunk#1/TS31			

Reader's Notes

8 MG 3200 Management

Two types of MG 3200 management are detailed in this section:

- SNMP-Based Client Program - Refer to "Using SNMP" below
- Web interface - Refer to "Embedded Web Server" on page 141

8.1 Using SNMP

Simple Network Management Protocol (SNMP) is a standards-based network control protocol for managing elements in a network. The SNMP Manager (usually implemented by a network Management System (NMS) or an Element Management System (EMS)) connects to an SNMP Agent (embedded on a remote Network Element (NE)) to perform network element Operation, Administration and Maintenance (OAM).

Both the SNMP Manager and the NE refer to the same database to retrieve information or configure parameters. This database is referred to as the Management Information Base (MIB), and is a set of statistical and control values. Apart from the standard MIBs documented in IETF RFCs, SNMP additionally enables the use of proprietary MIBs, containing a non-standard information set (specific functionality provided by the Network Element).

Directives, issued by the SNMP Manager to an SNMP Agent, consist of the identifiers of SNMP variables (referred to as MIB object identifiers or MIB variables) along with instructions to either get the value for that identifier, or set the identifier to a new value (configuration). The SNMP Agent can also send unsolicited events towards the EMS, called SNMP traps.

The definitions of MIB variables supported by a particular agent are incorporated in descriptor files, written in Abstract Syntax Notation (ASN.1) format, made available to EMS client programs so that they can become aware of MIB variables and their usage.

The MG 3200 contains an embedded SNMP Agent supporting both general network MIBs (such as the IP MIB), VoP-specific MIBs (such as RTP) and the proprietary MIBs (AcBoard, acGateway, AcAlarm and other MIBs) enabling a deeper probe into the inter-working of the Gateway. All supported MIB files are supplied to Customers as part of the release.

8.1.1 About SNMP

8.1.1.1 SNMP Message Standard

Four types of SNMP messages are defined:

- Get - A request that returns the value of a named object.
- Get-Next - A request that returns the next name (and value) of the "next" object supported by a network device given a valid SNMP name.
- Set - A request that sets a named object to a specific value.
- Trap - A message generated asynchronously by network devices. It notifies the network manager of a problem apart from the polling of the device.

Each of these message types fulfills a particular requirement of network managers:

- Get Request - Specific values can be fetched via the "get" request to determine the performance and state of the device. Typically, many different values and parameters can be determined via SNMP without the overhead associated with logging into the device, or establishing a TCP connection with the device.
- Get Next Request - Enables the SNMP standard network managers to "walk" through all SNMP values of a device (via the "get-next" request) to determine all names and values that a device supports. This is accomplished by beginning with the first SNMP object to be fetched, fetching the next name with a "get-next", and repeating this operation.
- Set Request - The SNMP standard provides a action method for a device (via the "set" request) to accomplish activities such as disabling interfaces, disconnecting users, clearing registers, etc. This provides a way of configuring and controlling network devices via SNMP.
- Trap Message - The SNMP standard furnishes a mechanism for a device to "reach out" to a network manager on their own (via the “trap" message) to notify or alert the manager of a problem with the device. This typically requires each device on the network to be configured to issue SNMP traps to one or more network devices that are awaiting these traps.

The above message types are all encoded into messages referred to as "Protocol Data Units" (PDUs) that are interchanged between SNMP devices.

8.1.1.2 SNMP MIB Objects

The SNMP MIB is arranged in a tree-structure, similar to a disk directory structure of files. The top level SNMP branch begins with the ISO "internet" directory, which contains four main branches:

- The "mgmt" SNMP branch - Contains the standard SNMP objects usually supported (at least in part) by all network devices.
- The “private" SNMP branch - Contains those "extended" SNMP objects defined by network equipment vendors.
- The "experimental" and "directory" SNMP branches - Also defined within the "internet" root directory, are usually devoid of any meaningful data or objects.

The "tree" structure described above is an integral part of the SNMP standard, though the most pertinent parts of the tree are the "leaf" objects of the tree that provide actual management data regarding the device. Generally, SNMP leaf objects can be partitioned into two similar but slightly different types that reflect the organization of the tree structure:

- Discrete MIB Objects - Contain one precise piece of management data. These objects are often distinguished from "Table" items (below) by adding a “.0" (dot-zero) extension to their names. The operator must merely know the name of the object and no other information.
- Table MIB Objects - Contain multiple pieces of management data. These objects are distinguished from "Discrete" items (above) by requiring a "." (dot) extension to their names that uniquely distinguishes the particular value being referenced. The "." (dot) extension is the "instance" number of an SNMP object. For "Discrete" objects, this instance number is zero. For "Table" objects, this instance number is the index into the SNMP table. SNMP tables are special types of SNMP objects, which allow parallel arrays of information to be supported. Tables are distinguished from scalar objects, such that tables can grow without bounds. For example, SNMP defines the "ifDescr" object (as a standard SNMP object) that indicates the text description of each interface supported by a particular device. Since network devices can be configured with more than one interface, this object can only be represented as an array.

By convention, SNMP objects are always grouped in an "Entry" directory, within an object with a "Table" suffix. (The "ifDescr" object described above resides in the "ifEntry" directory contained in the "ifTable" directory).

8.1.1.3 SNMP Extensibility Feature

One of the principal components of an SNMP manager is a "MIB Compiler", which allows new MIB objects to be added to the management system. When a MIB is compiled into an SNMP manager, the manager is made "aware" of new objects that are supported by agents on the network. The concept is similar to adding a new schema to a database.

Typically, when a MIB is compiled into the system, the manager creates new folders or directories that correspond to the objects. These folders or directories can typically be viewed with a "MIB Browser", which is a traditional SNMP management tool incorporated into virtually all network management systems.

The act of compiling the MIB allows the manager to know about the special objects supported by the agent and access these objects as part of the standard object set.

8.1.2 Carrier-Grade Alarm System

The basic alarm system has been extended to a carrier-grade alarm system. A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account element management system outages, network outages, and transport mechanism such as SNMP over UDP.

A carrier-grade alarm system is characterized by the following:

- The device allows an EMS to determine which alarms are currently active in the device. That is, the device maintains an active alarm table.
- The device allows an EMS to detect lost alarms and clear notifications. [sequence number in trap, current sequence number MIB object]
- The device allows an EMS to recover lost alarm raise and clear notifications [maintains a log history]
- The device sends a cold start trap to indicate that it is starting. This allows the EMS to synchronize its view of the device's active alarms.

When the SNMP alarm traps are sent, the carrier-grade alarm system does not add or delete alarm traps as part of the feature. This system provides the mechanism for viewing of history and current active alarm information.

8.1.2.1 Active Alarm Table

The board maintains an active alarm table to allow an EMS to determine which alarms are currently active in the device. Two views of the active alarm table are supported by the agent:

- acActiveAlarmTable in the enterprise AcAlarm
- alarmActiveTable and alarmActiveVariableTable in the IETF standard AcAlarm MIB (rooted in the MIB tree)

The acActiveAlarmTable is a simple, one-row per alarm table that is easy to view with a MIB browser.

The Alarm MIB is currently a draft standard and therefore, has no OID assigned to it. In the current software release, the MIB is rooted in the <ProcuctName> MIB subtree. In a future release, after the MIB has been ratified and an OID assigned to it, it is to be moved to the official OID.

8.1.2.2 Alarm History

The board maintains a history of alarms that have been raised and traps that have been cleared to allow an EMS to recover any lost raise or clear traps. Two views of the alarm history table are supported by the agent:

- acAlarmHistoryTable in the enterprise AcAlarm
- nlmLogTable and nlmLogVariableTable in the standard NOTIFICATION-LOG-MIB

As with the acActiveAlarmTable, the acAlarmHistoryTable is a simple, one-row per alarm table, that is easy to view with a MIB browser.

8.1.3 Cold Start Trap

MG 3200 technology supports a cold start trap to indicate that the unit is starting. This allows the EMS to synchronize its view of the unit's active alarms. In fact, two different traps are sent at start-up:

- The standard coldStart trap - iso(1).org(3).dod(6).internet(1). snmpV2(6). snmpModules(3). snmpMIB(1). snmpMIBObjects(1). snmpTraps(5). coldStart(1) sent at system initialization.
- The enterprise acBoardEvBoardStarted, which is generated at the end of system initialization. This is more of an "application-level" cold start sent after all the initializing process is over and all the modules are ready.

8.1.4 Performance Measurements for a Third-Party System

Performance Measurements are available for a Third-Party Performance Monitoring System through an SNMP interface and can be polled at scheduled intervals by an external poller or utility in the management server or other off board system.

The MG 3200 provides performance measurements in the form of two types:

1. **Gauges** - Gauges represent the current state of activities on the media server. Gauges unlike counters can decrease in value and like counters, can increase. The value of a gauge is the current value or a snapshot of the current activity on the media server at that moment.
2. **Counters** - Counters always increase in value and are cumulative. Counters, unlike gauges, never decrease in value unless the server is reset and then the counters are zeroed.

The MG 3200 performance measurements are provided by several proprietary MIBs (located under the "acPerformance" sub tree:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).AudioCodes(5003).acPerformance(10).

There are two formats of Performance Monitoring MIBs:

1. Older Format

Each MIB is made up of a list of single MIB objects, each relating to a separate attribute within a gauge or counter. All counters and gauges give the current time value only.

- **acPerfMediaGateway** - a generic-type of PM MIB that covers:
  - Control protocol
  - RTP stream
  - System packets statistics
- **acPerfMediaServices** - Media services devices specific performance MIB.

2. New Format - includes new MIBs.

   They all have an identical structure, which includes two major subtrees:

   - **Configuration sub tree** - allows configuration of general attributes of the MIB and specific attributes of the monitored objects.
   - **Data sub tree**

   The monitoring results are presented in tables. There are one or two indices in each table. If there are two - the first is a sub-set in the table (Example: trunk number) and the second (or the single where there is only one) index represents the interval number (present - 0, previous - 1 and the one before - 2).

   The MIBs are:

   - **acPMMedia** - for media (voice) related monitoring such as RTP and DSP.
   - **acPMControl** - for Control Protocol related monitoring such as connections, commands.
   - **acPMPSTN** - for PSTN related monitoring such as channel use, trunk utilization.
   - **acPMSystem** - for general (system related) monitoring.

The log trap, acPerformanceMonitoringThresholdCrossing (non-alarm) is sent out every time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it goes back under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.

8.1.4.1 TrunkPack-VoP Series Supported MIBs

The TrunkPack-VoP Series contains an embedded SNMP Agent supporting the following MIBs:

- **The Standard MIB (MIB-2)** - The various SNMP values in the standard MIB are defined in RFC 1213. The standard MIB includes various objects to measure and monitor IP activity, TCP activity, UDP activity, IP routes, TCP connections, interfaces, and general system description.
- **RTP MIB** - The RTP MIB is supported according to RFC 2959. It contains objects relevant to the RTP streams generated and terminated by the board and to the RTCP information related to these streams.

Note: The inverse tables are NOT supported.

- **Notification Log MIB** - This standard MIB (RFC 3014 - iso.org.dod.internet.mgmt.mib-2) is supported as part of The implementation of Carrier Grade Alarms.
- **Alarm MIB** - This is an IETF proposed MIB also supported as part of The implementation of Carrier Grade Alarms. This MIB is still not standard and therefore is under the audioCodes.acExperimental branch.
- **SNMP Target MIB** - This MIB is partially supported, (RFC 2273). It allows for configuration of trap destinations and trusted managers only.
- **SNMP Research International enterprise MIBs** - The MG 3200 supports two SNMP Research International MIBs: SR-COMMUNITY-MIB and TGT-ADDRESS-MASK-MIB. These MIBs are used in configuration of SNMPv2c community strings and trusted managers.

Note: Support for the SR-COMMUNITY-MIB is to be discontinued and it is to be replaced by the standard snmpCommunity MIB in the next applicable release.

In addition to the standard MIBs, the complete product series contains several proprietary MIBs:

- **AcBoard MIB** - This proprietary MIB contains objects related to configuration of the board and channels as well as to run-time information. Through this MIB, users can set up the board configuration parameters, reset the board, monitor the board's operational robustness and quality of service during run-time and receive traps.

Note: The AcBoard MIB is being phased out. It is still supported, but it is being replaced by an updated proprietary MIBs.

The AcBoard MIB has the following Groups:

- boardConfiguration
- boardInformation
- channelConfiguration
- channelStatus
- reset
- acTrap

As noted above, new proprietary MIBs cover the general parameters in the board.

They each contain a Configuration subtree, for configuring the related parameters. In some there also are Status and Action subtrees.

The new proprietary MIBs are:

- **acControl MIB**
- **acMedia MIB**
- **acPSTN MIB**
- **acSystem MIB**
- **acSS7 MIB**

Other proprietary MIBs are:

- **AcAlarm** - This is a proprietary carrier-grade alarm MIB. It is a simpler implementation of the notificationLogMIB and the IETF suggested alarmMIB (both also supported in all TP-1610 boards).

  The acAlarm MIB has the following groups:

  - **ActiveAlarm** - straight forward (single indexed) table listing all currently active Alarms together with their bindings (the Alarm bindings are defined in acAlarm. acAlarmVarbinds and also in acBoard.acTrap. acBoardTrapDefinitions. oid_1_3_6_1_4_1_5003_9_10_1_21_2_0).
  - **acAlarmHistory** - straight forward (single indexed) table listing all recently raised Alarms together with their bindings (the Alarm bindings are defined in acAlarm. acAlarmVarbinds and also in acBoard.acTrap. acBoardTrapDefinitions. oid_1_3_6_1_4_1_5003_9_10_1_21_2_0).

The table size can be altered via notificationLogMIB.notificationLogMIBObjects.nlmConfig.nlmConfigGlobalEntryLimit or notificationLogMIB.notificationLogMIBObjects.nlmConfig.nlmConfigLogTable.nlmConfigLogEntry.nlmConfigLogEntryLimit.

The table size can be any value between 50 and 1000 and the default is 500.

Note 1: The following are special notes pertaining to MIBs:

- A detailed explanation of each parameter can be viewed in an SNMP browser in the MIB Description field.
- Not all groups in the MIB are implemented. Refer to version release notes.
- Certain parameters are not implemented. Their MIB status is marked 'obsolete'.
- When a parameter is SET to a new value via SNMP, the change may affect board functionality immediately or may require that the board be soft reset for the change to take effect. This depends on the parameter type.

Note 2: The current (updated) board configuration parameters are programmed into the board provided that the user does not load an *ini* file to the board after reset. Loading an *ini* file after reset overrides the updated parameters.

Additional MIBs are to be supported in future releases.

- **Traps**

Note: As of this version all traps are sent out from the SNMP port (default 161). This is part of the NAT traversal solution.

Full proprietary trap definitions and trap Varbinds are found in AcBoard MIB and AcAlarm MIB. For a detailed inventory of traps, refer to the Appendix, "SNMP Alarm Traps" on page 381.

The following proprietary traps are supported in MG 3200:

- **acBoardFatalError -** Sent whenever a fatal board error occurs.

- **acBoardConfigurationError -** Sent when a board's settings are illegal - the trap contains a message stating/detailing/explaining the illegality of the setting.
- **acBoardTemperatureAlarm -** Sent when a board exceeds its temperature limits.
- **acBoardEvResettingBoard -** Sent after a board is reset.
- **acBoardEvBoardstarted -** Sent after a board is successfully restored and initialized following reset.
- **acFeatureKeyError -** Development pending. Intended to relay Feature Key errors etc. (To be supported in the next applicable release)
- **acgwAdminStateChange -** Sent when Graceful Shutdown commences and ends. (Currently supported in H.248 only)
- **acBoardEthernetLinkAlarm -** Ethernet Link or links are down.
- **acActiveAlarmTableOverflow -** An active alarm could not be placed in the active alarm table because the table is full.
- **acAudioProvisioningAlarm** - Raised if the MG 3200 is unable to provision its audio.
- **acOperationalStateChange** - Raised if the operational state of the node goes to disabled. Cleared when the operational state of the node goes to enabled.
- **acKeepAlive** – part of the NAT traversal mechanism. If the STUN application in the MG 3200 detects a NAT then this trap is sent out on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the MAC address of the MG 3200.
- **acNATTraversalAlarm** - When the NAT is placed in front a MG 3200, it is identified as a symmetric NAT - this alarm is raised. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one.
- **acEnhancedBITStatus** - This trap is used to for the status of the BIT (Built In Test). The information in the trap contains board hardware elements being tested and their status. The information is presented in the additional info fields.
- **acPerformanceMonitoringThresholdCrossing** - This log trap is sent out for every time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it goes back under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.
- **acSS7LinkStateChangeAlarm** - This alarm is raised if the operational state of the SS7 link becomes BUSY. The alarm is cleared when the operational state of the link becomes -SERVICE or OFFLINE.
- **acSS7LinkInhibitStateChangeAlarm** - This alarm is raised if the SS7 link becomes inhibited (local or remote). The alarm is cleared when the link becomes uninhibited - local AND remote. Note that this alarm is raised for any change in the remote or local inhibition status.
- **acSS7LinkBlockStateChangeAlarm** - This alarm is raised if the SS7 link becomes blocked (local or remote). The alarm is cleared when the link becomes unblocked - local AND remote. Note that this alarm is raised for any change in the remote or local blocking status.
- **acSS7LinkCongestionStateChangeAlarm** - This alarm is raised if the SS7 link becomes congested (local or remote). The alarm is cleared when the link becomes uncongested - local AND remote. Note that this alarm is raised for any change in the remote or local congestion status.

- **acSS7LinkSetStateChangeAlarm** - This alarm is raised if the operational state of the SS7 linkset becomes BUSY. The alarm is cleared when the operational state of the linkset becomes -SERVICE or OFFLINE.
- **acSS7RouteSetStateChangeAlarm** - This alarm is raised if the operational state of the SS7 routeset becomes BUSY. The alarm is cleared when the operational state of the routeset becomes -SERVICE or OFFLINE.
- **acSS7SNSetStateChangeAlarm** - This alarm is raised if the operational state of the SS7 node becomes BUSY. The alarm is cleared when the operational state of the node becomes IN-SERVICE or OFFLINE..
- **acSS7RedundancyAlarm** - Raised when the SS7 redundancy degregated.

In addition to the listed traps the Board also supports the following standard traps:

- **authenticationFailure**
- **coldStart**
- **dsx1LineStatusChange**

8.1.5 SNMP Interface Details

This section describes details of the SNMP interface needed when developing an Element Management System (EMS) for any of the TrunkPack-VoP Series products, or to manage a device with a MIB browser.

SNMP can be encoded over IPSec. For more details, refer to the Appendix,' 'Security" on page 319.

For *ini* file encoding, refer to the Appendix "Utilities" on page 353.

8.1.5.1 SNMP Community Names

By default, the board uses a single, read-only community string of "public" and a single read-write community string of "private".

One can configure up to 5 read-only community strings and up to 5 read-write community strings, and a single trap community string is supported:

8.1.5.1.1 Configuration of Community Strings via the *ini* File

SNMPREADONLYCOMMUNITYSTRING_<x> = '#######'

SNMPREADWRITECOMMUNITYSTRING_<x> = '#######'

Where <x> is a number between 0 and 4, inclusive. Note that the '#' character represents any alphanumeric character. The maximum length of the string is 20 characters.

8.1.5.1.2 Configuration of Community Strings via SNMP

To configure read-only and read-write community strings, the EM must use the srCommunityMIB. To configure the trap community string, the EM must also use the snmpVacmMIB and the snmpTargetMIB.

Note: Support for the SR-COMMUNITY-MIB is to be discontinued and it is to be replaced by the standard snmpCommunity MIB in the next applicable release.

➢ **To add a read-only community string, v2user, take this step:**

- Add a new row to the srCommunityTable with CommunityName v2user and GroupName ReadGroup.

➢ **To delete the read-only community string, v2user, take these 2 steps:**

1. If v2user is being used as the trap community string, follow the procedure for changing the trap community string. (See below.)
2. Delete the srCommunityTable row with CommunityName v2user.

➢ **To add a read-write community string, v2admin, take this step:**

- Add a new row to the srCommunityTable with CommunityName of v2admin and GroupName ReadWriteGroup.

➢ **To delete the read-write community string, v2admin, take these 2 steps:**

1. If v2admin is being used as the trap community string, follow the procedure for changing the trap community string. (See below.)
2. Delete the srCommunityTable row with a CommunityName of v2admin and GroupName of ReadWriteGroup.

➢ **To change the only read-write community string from v2admin to v2mgr, take these 4 steps:**

1. Follow the procedure above to add a read-write community string to a row for v2mgr.
2. Set up the EM such that subsequent set requests use the new community string, v2mgr.
3. If v2admin is being used as the trap community string, follow the procedure to change the trap community string. (See below.)
4. Follow the procedure above to delete a read-write community name in the row for v2admin.

➢ To change the trap community string, take these 2 steps:

The following procedure assumes that a row already exists in the srCommunityTable for the new trap community string. The trap community string can be part of the TrapGroup, ReadGroup or ReadWriteGroup. If the trap community string is used solely for sending traps (recommended), then it should be made part of the TrapGroup.

1. Add a row to the vacmSecurityToGroupTable with these values: SecurityModel=2, SecurityName=the new trap community string, GroupName=TrapGroup, ReadGroup or ReadWriteGroup. The SecurityModel and SecurityName objects are row indices.

Note: You must add GroupName and RowStatus on the same set.

2. Modify the **SecurityName** field in the appropriate row of the snmpTargetParamsTable.

8.1.5.2 Trusted Managers

By default, the agent accepts get and set requests from any IP address, as long as the correct community string is used in the request. Security can be enhanced via the use of Trusted Managers. A Trusted Manager is an IP address from which the SNMP agent accepts and process get and set requests. An EM can be used to configure up to 5 Trusted Managers.

Note: If Trusted Managers are defined, then all community strings works from all Trusted Managers. That is, there is no way to associate a community string with particular trusted managers.

8.1.5.2.1 Configuration of Trusted Managers via *ini* File

To set the Trusted Mangers table from start up, write the following in the *ini* file:

SNMPTRUSTEDMGR_X = D.D.D.D

Where X is any integer between 0 and 4 (0 sets the first table entry, 1 sets the second and so on), and D is an integer between 0 and 255.

8.1.5.2.2 Configuration of Trusted Managers via SNMP

To configure Trusted Managers, the EM must use the srCommunityMIB, the snmpTargetMIB and the TGT-ADDRESS-MASK-MIB.

➢ To add the first Trusted Manager, take these 3 steps:

The following procedure assumes that there is at least one configured read-write community. There are currently no Trusted Managers. The taglist for columns for all srCommunityTable rows are currently empty.

1. Add a row to the snmpTargetAddrTable with these values: Name=mgr0, TagList=MGR, Params=v2cparams.
2. Add a row to the tgtAddressMaskTable table with these values: Name=mgr0, tgtAddressMask=255.255.255.255:0. The agent does not allow creation of a row in this table unless a corresponding row exists in the snmpTargetAddrTable.
3. Set the value of the TransportLabel field on each non-TrapGroup row in the srCommunityTable to MGR.

➢ To add a subsequent Trusted Manager, take these 2 steps:

The following procedure assumes that there is at least one configured read-write community. There are currently one or more Trusted Managers. The taglist for columns for all rows in the srCommunityTable are currently set to MGR. This procedure must be done from one of the existing Trusted Managers.

1. Add a row to the snmpTargetAddrTable with these values: Name=mgrN, TagList=MGR, Params=v2cparams, where N is an unused number between 0 and 4.
2. Add a row to the tgtAddressMaskTable table with these values: Name=mgrN, tgtAddressMask=255.255.255.255:0.

An alternative to the above procedure is to set the tgtAddressMask column while you are creating other rows in the table.

➢ To delete a Trusted Manager (not the final one), take this step:

The following procedure assumes that there is at least one configured read-write community. There are currently two or more Trusted Managers. The taglist for columns for all rows in the srCommunityTable are currently set to MGR. This procedure must be done from one of the existing trusted managers, but not the one that is being deleted.

- Remove the appropriate row from the snmpTargetAddrTable.

The change takes affect immediately. The deleted trusted manager cannot access the board. The agent automatically removes the row in the tgtAddressMaskTable.

➢ To delete the final Trusted Manager, take these 2 steps:

The following procedure assumes that there is at least one configured read-write community. There is currently only one Trusted Manager. The taglist for columns for all rows in the srCommunityTable are currently set to MGR. This procedure must be done from thefinal Trusted Manager.

1. Set the value of the TransportLabel field on each row in the srCommunityTable to the empty string.
2. Remove the appropriate row from the snmpTargetAddrTable

The change takes affect immediately. All managers can now access the board.

8.1.5.3 SNMP Ports

The SNMP Request Port is 161 and Trap Port is 162

These ports can be changed by setting parameters in the board *ini* file. The parameter name is:

SNMPPort = <port_number>
Valid UDP port number; default = 161

This parameter specifies the port number for SNMP requests and responses.

Usually it should not be specified. Use the default.

8.1.5.4 Multiple SNMP Trap Destinations

An agent can send traps to up to five managers. For each manager the user needs to set the manager IP and trap receiving port along with enabling the sending to that manager.

8.1.5.4.1 Trap Manager Configuration via Host Name

A trap manager can be set using the manager's host name. This is currently supported via *ini* file only, using the parameter name, SNMPTrapManagerHostName.
When this parameter value is set for this trap, the board at start up tries to resolve the host name. Once the name is resolved (IP is found) the bottom entry in the trap manager's table (and also in the snmpTargetAddrTable in the snmpTargetMIB) is updated with the IP.
The port is 162 unless specified otherwise. The row is marked as 'used' and sending is 'enabled').
When using 'host name' resolution, any changes made by the user to this row in either MIBs are overwritten by the board when a resolving is redone (once an hour).

Note: Some traps may be lost until the name resolving is complete.

8.1.5.4.2 Configuration via the *ini* File

In the TP-1610 board *ini* file, parameters below can be set to enable or disable the sending of SNMP traps. Multiple trap destinations can be supported on the media server by setting multiple trap destinations in the *ini* file.

SNMPMANAGERTRAPSENDINGENABLE_<x> = 0 or 1 indicates if traps are to be sent to the specified SNMP trap manager. A value of '1' means that it is enabled, while a value of '0' means disabled.

Where <x> = a number 0, 1, 2 and is the array element index. Currently up to 5 SNMP trap managers can be supported.

Below is an example of entries in the board *ini* file regarding SNMP. The media server can be configured to send to multiple trap destinations. The lines in the file below are commented out with the ";" sign at the beginning of the line. All of the lines below are commented out since the first line character is a semi-colon.

```
; SNMP trap destinations
; The board maintains a table of trap destinations containing 5
;rows. The rows are numbered 0..4. Each block of 4 items below
;apply to a row in the table.
; To configure one of the rows, uncomment all 4 lines in that
;block. Supply an IP address and if necessary, change the port
;number.
; To delete a trap destination, set ISUSED to 0.
; -change these entries as needed
;SNMPMANAGERTABLEIP_0=
;SNMPMANAGERTRAPPORT 0=162
;SNMPMANAGERISUSED 0=1
;SNMPMANAGERTRAPSENDINGENABLE_0=1
;
;SNMPMANAGERTABLEIP 1=
;SNMPMANAGERTRAPPORT_1=162
;SNMPMANAGERISUSED 1=1
;SNMPMANAGERTRAPSENDINGENABLE 1=1
;
;SNMPMANAGERTABLEIP 2=
;SNMPMANAGERTRAPPORT 2=162
;SNMPMANAGERISUSED_2=1
;SNMPMANAGERTRAPSENDINGENABLE 2=1
;
;SNMPMANAGERTABLEIP_3=
;SNMPMANAGERTRAPPORT 3=162
;SNMPMANAGERISUSED 3=1
;SNMPMANAGERTRAPSENDINGENABLE_3=1
;
;SNMPMANAGERTABLEIP 4=
;SNMPMANAGERTRAPPORT_4=162
;SNMPMANAGERISUSED 4=1
;SNMPMANAGERTRAPSENDINGENABLE 4=1
```

The 'trap manager host name' is configured via SNMPTrapManagerHostName. For example:

```
;SNMPTrapManagerHostName = 'myMananger.corp.MyCompany.com'
```

Note: The same information that is configurable in the *ini* file can also be configured via the acBoardMIB.

8.1.5.4.3 Configuration via SNMP

There are two MIB interfaces for the trap managers. The first is via the acBoard MIB that has become obsolete and is to be removed from the code in the next applicable release. The second is via the standard snmpTargetMIB.

1. Using the acBoard MIB:

   The following parameters, which are defined in the snmpManagersTable:

   a. snmpTrapManagerSending
   b. snmpManagerIsUsed
   c. snmpManagerTrapPort
   d. snmpManagerIP

When snmpManagerIsUsed is set to zero (not used) the other three parameters are set to zero. (The intent is to have them set to the default value, which means TrapPort is to be set to 162. This is to be revised in a later release.)

- snmpManagerIsUsed Default = Disable(0)

  The allowed values are 0 (disable or no) and 1 (enable or yes).

- snmpManagerIp Default = 0.0.0.0

  This is known as SNMPMANAGERTABLEIP in the *ini* file and is the IP address of the manager.

- snmpManagerTrapPort Default = 162

  The valid port range for this is 100-4000.

- snmpManagerTrapSendingEnable Default = Enable(1)

  The allowed values are 0 (disable) and 1 (enable).

Note 1: Each of these MIB objects is independent and can be set regardless of the state of snmpManagerIsUsed.

Note 2: If the IsUsed parameter is set to 1, then the IP address for that row should be supplied in the same SNMP PDU.

2. Using the SNMPTargetMIB:

➢ To add a trap destination, take this step:

- Add a row to the snmpTargetAddrTable with these values: Name=trapN, TagList=AC_TRAP, Params=v2cparams, where N is an unused number between 0 and 4

All changes to the trap destination configuration take effect immediately.

➢ To delete a trap destination, take this step:

- Remove the appropriate row from the snmpTargetAddrTable.

➢ To modify a trap destination, take this step:

You can change the IP address and or port number for an existing trap destination. The same effect can be achieved by removing a row and adding a new row.

- Modify the IP address and/or port number for the appropriate row in the snmpTargetAddrTable.

➢ To disable a trap destination, take this step:

- Change TagList on the appropriate row in the snmpTargetAddrTable to the empty string.

➢ To enable a trap destination, take this step:

- Change TagList on the appropriate row in the snmpTargetAddrTable to "AC_TRAP".

8.1.5.4.4 SNMP Manager Backward Compatibility

With support of the Multi Manager Trapping feature, there is also a need to support the older acSNMPManagerIP MIB object, which is synchronized with the first index in the snmpManagers MIB table. This is translated in two new features:

- SET/GET to either of the two; is for now identical.
  i.e. OID 1.3.6.1.4.1.5003.9.10.1.1.2.7 is identical
  to OID 1.3.6.1.4.1.5003.9.10.1.1.2.21.1.1.3 as far as the SET/GET are concerned.
- When setting ANY IP to the acSNMPManagerIP (this is the older parameter, not the table parameter), two more parameters are SET to ENABLE. snmpManagerIsUsed.0 and snmpManagerTrapSendingEnable.0 are both set to 1.

8.1.6 Dual Module Interface

Dual module boards have a first and second module (the first is on the right side of the TP-1610 when looking at it from the front). Differentiation is based on the modules' serial numbers.

MIB object acSysIdSerialNumber always returns the serial number of the module on which the GET is performed.

MIB object acSysIdFirstSerialNumber always returns the serial number of the first module.

If the module on which the GET is performed is the second module, the values in these two are different. If, on the other hand, the module is the first module, the value in the two objects are the same.

8.1.7 SNMP NAT Traversal

A NAT placed between a <product Name> and the element manager calls for traversal solutions:

- **Trap source port** – all traps are sent out from the SNMP port (default – 161). A manager receiving these traps can use the binding information (in the UDP layer) to traverse the NAT back to the device.
  The trap destination address (port and IP) are as configured in the snmpTargetMIB.
- **acKeepAliveTrap** – this trap is designed to be a constant life signal from the device to the manager allowing the manager NAT traversal at all times. The acBoardTrapGlobalsAdditionalInfo1 varbind has the device's serial number.

  The Trap is instigated in three ways:

  - Via an ini file parameter - 'SendKeepAliveTrap = 1'. This ensures that the trap is continuously sent. The frequency is set via the 9/10 of the NATBINDINGDEFAULTTIMEOUT (or MIB object - acSysSTUNBindingLifeTime) parameter.
  - After the STUN client has discovered a NAT (any NAT).
  - If the STUN client can not contact a STUN server.

Note: The two latter options require the STUN client be enabled (*ini* file parameter – EnableSTUN).

Also, once the acKeepAlive trap is instigated it does not stop.

- The manager can see the NAT type in the MIB:
  audioCodes(5003).acProducts(9).acBoardMibs(10).acSystem(10).acSystemStatus(2).acSysNetwork(6).acSysNAT(2).acSysNATType(1)
- The manger also has access to the STUN client configuration:
  audioCodes(5003).acProducts(9).acBoardMibs(10).acSystem(10).acSystemConfiguration(1).acSysNetworkConfig(3).acSysNATTraversal(6).acSysSTUN(21)
- **acNATTraversalAlarm** - When the NAT is placed in front a device is identified as a symmetric NAT - this alarm is raised. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one.

8.2 Administrative State Control

8.2.1 Node Maintenance

Node maintenance for the MG 3200 is provided via an SNMP interface. The acBoardMIB provides two parameters for graceful and forced shutdowns of the MG 3200. (Refer to the note in "Graceful Shutdown" below.) These parameters are in the acBoardMIB as acgwAdminState and acgwAdminStateLockControl.

The acgwAdminState is used either to request (set) a shutdown (0), undo shutdown (2), or to view (get) the gateway condition (0 = locked, 1 = shutting down, 2 = unlocked).

The acgwAdminStateLockControl is used to set a time limit for the shutdown (in seconds) where 0 means shutdown immediately (forced), -1 means no time limit (graceful) and x where x>0 indicates a time limit in seconds (timed limit is considered a graceful shutdown).

The acgwAdminStateLockControl should be set first followed by the acgwAdminState.

8.2.2 Graceful Shutdown

acgwAdminState is a read-write MIB object. When a get request is sent for this object, the agent returns the current board administrative state.

Note: Graceful shutdown is currently supported in H.248 only.

The possible values received on a get request are:

- locked(0) - The board is locked
- shuttingDown(1) - The board is in the process of performing a graceful lock
- unlocked(2) - The board is unlocked

On a set request, the manager supplies the desired administrative state, either locked(0) or unlocked(2).

When the board changes to either shuttingDown or locked state, an adminStateChange alarm is raised. When the board changes to an unlocked state, the adminStateChange alarm is cleared.

Before setting acgwAdminState to perform a lock, acgwAdminStateLockControl should be set first to control the type of lock that is performed. The possible values are:

- 1 = Perform a graceful lock. Calls are allowed to complete. No new calls are allowed to be originated on this device.
- 0 = Perform a force lock. Calls are immediately terminated.
- Any number greater than 0 - Time in seconds before the graceful lock turns into a force lock.

8.3 Embedded Web Server

The MG 3200 boards and modules contain an Embedded Web Server to be used for device configuration and for run-time monitoring. The Embedded Web Server enables users equipped with any standard Web-browsing application such as Microsoft™ Internet Explorer™ (Ver. 5.0 and higher) or Netscape™ Navigator™ (Ver. 7.2 and higher) to:

- Provision devices (refer to "Advanced Configuration Screen" on page 204)
- Verify configuration changes in the Status screens (refer to "Status and Diagnostic Menu" on page 182)
- Load the *ini* file (refer to "Software Upgrade Wizard" on page 190)
- Load the CMP, Voice Prompt, Prerecorded Tones, CPT and CAS Files (refer to' 'Auxiliary Files Download" on page 199.)

8.3.1 Embedded Web Server Protection & Security Mechanisms

Access to the Embedded Web Server is controlled by the following protection and security mechanisms:

- **Dual Access Level Username and Password** - Refer to "Username and Password" below
- **Limiting the Web Server GUI to Read-Only Mode** - Refer to "Limiting the Web Server GUI to Read-Only Mode" below
- **Disabling the Web Server GUI** - Refer to "Disabling the Web Server GUI" on page 143
- **Encrypted HTTP transport (HTTPS - SSL)** - Refer to "Encrypted HTTP transport (HTTPS - SSL)" on page 143
- **Limiting Web Access to a Predefined List of Client IP Addresses** - Refer to' 'Limiting Web Access to a Predefined List of Client IP Addresses" on page 143
- **Managing Web Access Using a RADIUS Server** - Refer to "Managing Web Server Access Using a RADIUS Server" on page 143

8.3.1.1 Username and Password

Username and Password protected duel level Access is provided in the default settings.

Two levels of access are defined:

- **Administrator Level** - 'Read and Write' privileges
- **Monitoring Level** - 'Read Only' privileges

Each of the two access levels has A unique Username and Password combination.

The default Administrator access level Username and Password for all devices is:

- Username: Admin
- Password: Admin

The default Monitoring access level Username and Password for all devices is:

- Username: User
- Password: User

The Enter Network Password dialog is case-sensitive.

If the Embedded Web Server is left idle for more than 5 minutes, the session is expires. Subsequently, when a screen is accessed, you are prompted again for the Username and Password.

For more information about changing the Password and Username for each access level or resetting them to the defaults, refer to "Changing the Password" on page 180.

8.3.2 Limiting the Embedded Web Server to Read-Only Mode

Initially, the Embedded Web Server displays the default parameters that are pre-installed in the board. These parameters can be modified using the Embedded Web Server, either by modifying parameters on the various pages or by loading a text configuration file - an *ini* file to the MG 3200.

Users can limit the Web Server to read-only mode by changing the default of *ini* file parameter DisableWebConfig. The read-only mode feature can be used as a security measure. This security level provides protection against unauthorized access (such as Internet hacker attacks), particularly important to users without a firewall.

8.3.2.1 Limiting the Embedded Web Server to Read-Only Mode

Users can limit the Web Server to read-only mode by changing the default of *ini* file parameter DisableWebConfig. Use the read-only mode feature as a security measure. This security level provides protection against unauthorized access (such as Internet hacker attacks), particularly important to users without a firewall.

When the device is loaded through a PCI/cPCI bus, the Embedded Web Server is always set to read-only mode regardless of the web access level of the current user.

➢ To limit the Web Server to read-only mode:

- Set the *ini* file parameter DisableWebConfig to 1 (Default = 0, i.e. read-write mode) and send the modified *ini* file to the device. All Web pages are presented in read-only mode. The ability to modify configuration data is disabled. In addition, users do NOT have access to any file loading page, to the "Change Password" page, to the "SaveConfiguration", or to the "Reset" page.

Note 1: 'Read Only' policy also dan be employed by setting DisableWebConfig to **0** and distributing the Monitoring level and Administrator level user name password pairs according to the organization's security policy.

Note 2: When DisableWebConfig is set to **1** the Dual Access level scheme is overridden, so that a user who is accessing the web server as an Administrator level user to view the web GUI in 'Read Only' mode.

8.3.2.2 Disabling the Embedded Web Server

You can deny access to the device's Web Server by changing the default of *ini* file parameter DisableWebTask. The ability to disable access to the device's Web Server via HTTP provides a high level of security in which protection against unauthorized access (such as Internet hacker attacks) is included. This is particularly important to users without a firewall.

When the device is controlled through a PCI/cPCI bus, the Embedded Web Server is always activated. The user cannot disable it in PCI mode.

➢ **To disable the Embedded Web Server:**

- Set the *ini* file parameter DisableWebTask to 1 (Default = 0, i.e. web task enabled). Access to the device's Web Server is denied.

8.3.2.3 Encrypted HTTP transport (HTTPS - SSL)

Data transportation between Web server and Web client may be conducted over a secured SSL link that encrypts the HTTP layer. The Web server may be configured to accept communications only on a secured link (HTTPS) or both on a secured link (HTTPS) and a non secured link (HTTP). For further details refer to the Appendix, "Security" on page 319.

8.3.2.4 Limiting Web Access to a Predefined List of Client IP Addresses

When client IP addresses are known in advance. Users can define a list of up to 10 client IP addresses that are to be accepted by the Web server. Any client that does not bear an IP address in the predefined list is unable to connect to the Web server. For further details refer to the Appendix, "Security" on page 319.

8.3.2.5 Managing Web Server Access Using a RADIUS Server

Users are given the option to manage the web server's password-username pairs via a RADIUS server. When this option is used the Dual level access scheme is disabled and all users that access the web server are deemed to be Administrators with Read/Write privileges. For further details refer to the Appendix, "Security" on page 319.

8.3.3 Correlating PC / MG 3200 IP Address & Subnet Mask

Before using the Web browser to access the MG 3200's Embedded Web Server, change the PC's IP address and Subnet Mask to correspond with the MG 3200's factory default IP address and Subnet Mask shown in the table below. For details on changing the IP address and Subnet Mask, refer to the Help information provided by the Operating System used.

Table 8-1: Default IP Address and Subnet Mask

E1/T1 Trunks	IP Address	Subnet Mask
Trunks 1-8	10.1.10.10	255.255.0.0
Trunks 9-16	10.1.10.11	255.255.0.0

Note 1: The two IP addresses refer to two different modules residing on the same (TP-1610) board (one IP address for the module containing Trunks 1-8 and another for the module containing Trunks 9-16).

Note 2: Note and retain the IP Address and Subnet Mask that you assign to the device. Do the same when defining Username and Password (refer to "Username and Password" on page 141). If the Embedded Web Server is unavailable (for example, if you have lost your Username and Password), use the BootP/TFTP Server to access the device, “reflash” the files and reset the password. For more information on the BootP/TFTP Server, refer to the Appendix, "BootP/TFTP Server" on page 223.

8.3.4 Accessing the Embedded Web Server

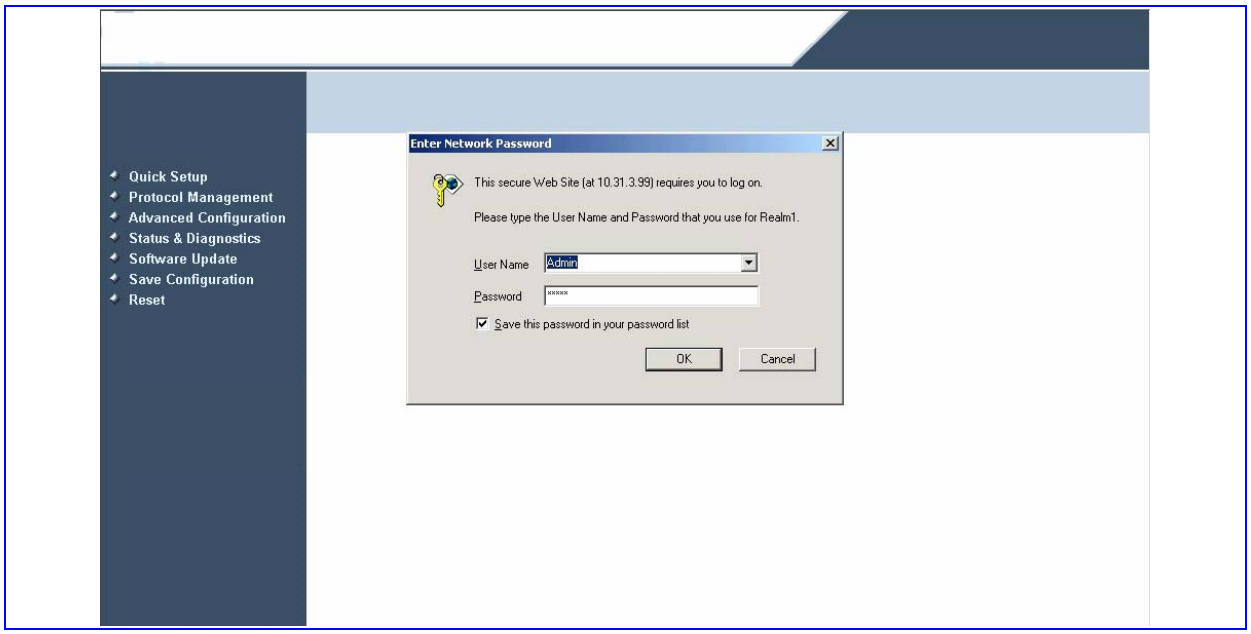
➢ **To access the Embedded Web Server, take these 2 steps:**

1. Open any standard Web-browser application, such as Microsoft™ Internet Explorer™™ (Ver. 5.0 and higher) or Netscape™™ Navigator™ (Ver. 7.2 and higher).

Note: The browser must be Java-script enabled. If java-script is disabled, a message box with notification of this is displayed.

2. Specify the IP address of the device in the browser's URL field (e.g., http://10.1.229.17 or https://10.1.229.17 for an SSL secure link). The Embedded Web Server Enter Network Password screen appears.

Figure 8-1: Enter Network Password Screen



8.3.5 Using Internet Explorer to Access the Embedded Web Server

Internet Explorer's security settings may block access to the Gateway's Web browser if they're configured incorrectly. If this happens, the following message appears:

> **Unauthorized**
>
> **Correct authorization is required for this area. Either your browser does not perform authorization or your authorization has failed. RomPager server.**

➢ To troubleshoot blocked access to Internet Explorer, take these 7 steps:

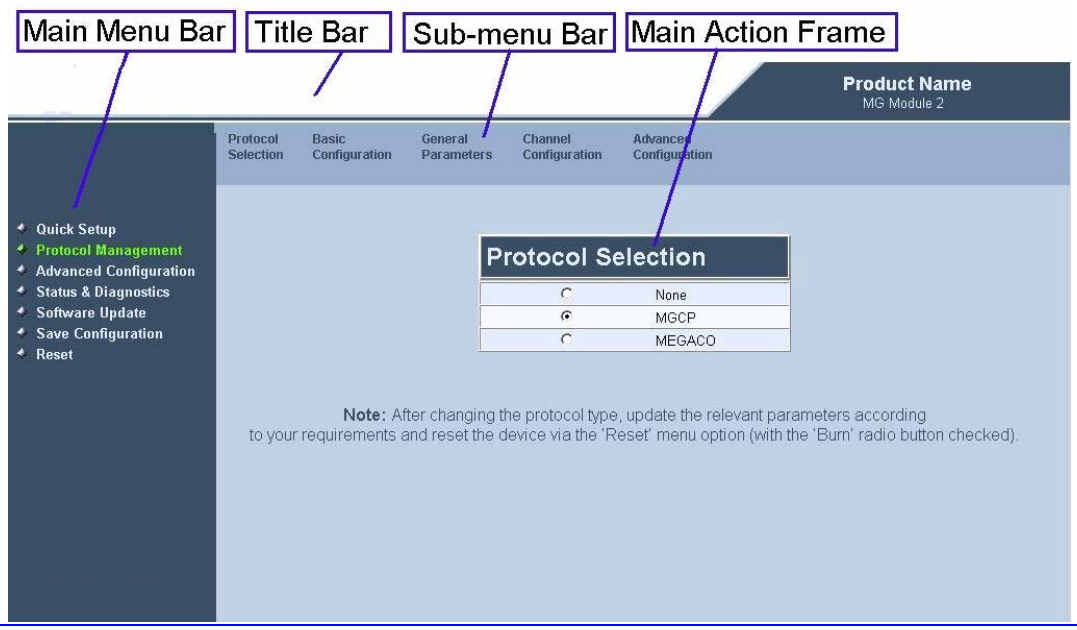
1. Delete all cookies from the Temporary Internet files folder. If this does not clear up the problem, the security settings may need to be altered. (Continue to Step 2).
2. In Internet Explorer, from the Tools menu, select **Internet Options**. The Internet Options dialog box appears.
3. Select the Security tab, and then, at the bottom of the dialog box, click the **Custom Level** button. The Security Settings dialog box appears.
4. Scroll down until the Logon options are displayed and change the setting to **Prompt for user name and Password**. Then Click **OK**.
5. Select the Advanced tab.
6. Scroll down until the HTTP 1.1 Settings are displayed and verify that the **Use HTTP 1.1** option is checked.
7. Restart the browser. This fixes any issues related to domain use logon policy.

8.4 Getting Acquainted with the Web Interface

8.4.1 About the Web Interface Screen

The figure below is an example of the General layout of the Web Interface screen.

Figure 8-2: Web Interface Screen - Example



The Web Interface screen contains the following parts:

- **Title bar** - contains the corporate logo, background images and product name
- **Main menu bar** - always appears to the left on every screen for quick access to the other main modules
- **Sub-menu bar** - always appears at the top on every screen and contains links to the sub-menus of the main module selected in the main menu bar to the left
- **Main action pane** - The main area of the screen in which information is viewed and configured

The Web interface is divided into the following 7 modules in the main menu bar to the left:

- **Quick Setup** - Use this module to configure the device's basic settings. (For the full list of configurable parameters go directly to the Protocol Management and Advanced Configuration menus.)
- **Protocol Management** - Use the menus in this module to configure the device's control protocol parameters.
- **Advanced Configuration** - Use the menus in this module to set the device's advanced configuration parameters (for advanced users only).
- **Status & Diagnostics** - Use the menus in this module to view and monitor the device's channels, Syslog messages and hardware / software product information.

- **Software Update** - Use the menus in this module when you want to load new software or configuration files onto the device.
- **Save Configuration** - Use this menu to save configuration changes to the non-volatile (flash) memory.
- **Reset** - Use this menu to remotely reset the device.

Note: When positioning your curser over a parameter name for more than 1 second, a short description of this parameter is displayed.

8.4.2 Saving Changes

To save changes to the volatile memory (RAM) press the **Submit** button (changes to parameters with on-the-fly capabilities are immediately available, other parameters are updated only after a device reset). Parameters that are only saved to the volatile memory revert to their previous settings after hardware reset (software reset i.e. via the Web Interface offers the option to save the changes to the non-volatile memory prior to the reset). To save changes so they are available after a power fail, you must save the changes to the non-volatile memory (flash). When **Save Configuration** is performed, all parameters and loaded files are saved to the non-volatile memory.

➢ To save the changes to non-volatile, take the next 2 steps:

1. From the main menu on the left, click the **Save Configuration** link. The Save Configuration screen appears.
2. Click the **Save Configuration** button in the middle of the screen. A confirmation message appears when the save is complete.

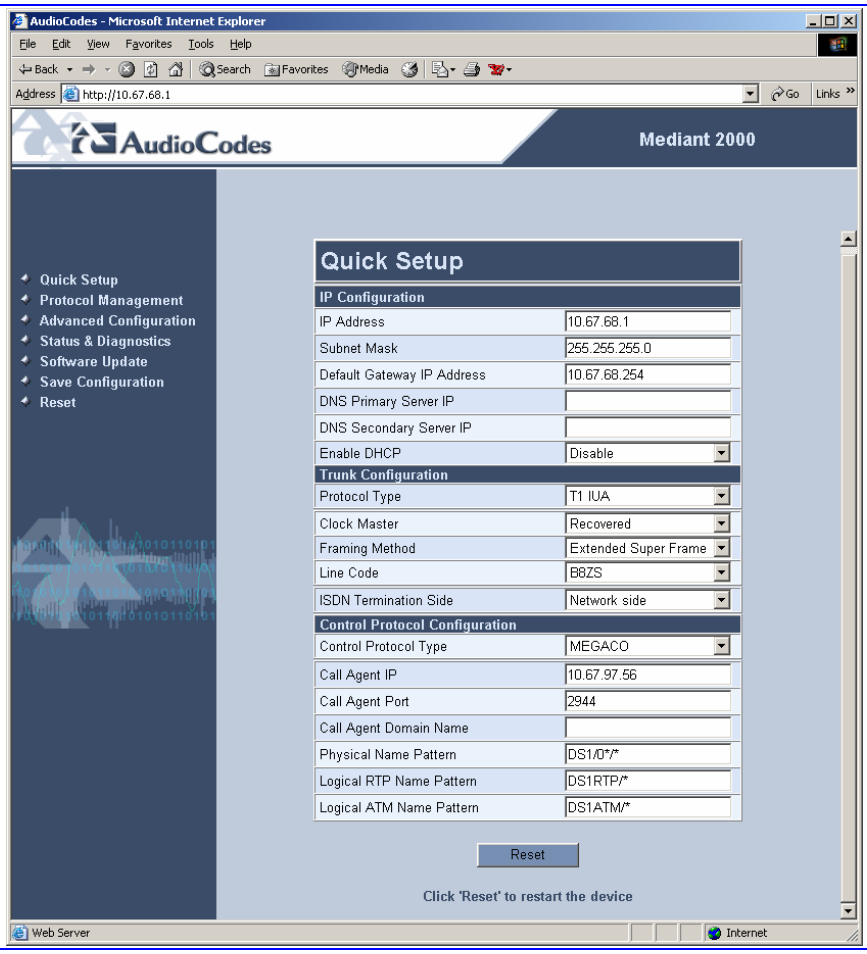
➢ To quickly setup a MG 3200, take these 14 steps:

1. Access the Web Server Interface (refer to "Accessing the Embedded Web Server" on page 144.)
2. Enter the Administrator level **Username** (default: **Admin**) and **Password** (default: **Admin**).

Note: The Username and Password fields are case-sensitive.

3. Click **OK.** The Quick Setup screen appears.

Figure 8-3: Quick Setup Screen



4. In the Quick Setup screen, enter or modify appropriate information for the IP Configuration, Trunk Configuration and Control Protocol (per type).

5. In the **IP Configuration** section, **IP Address** and **Subnet Mask** fields, enter the appropriate addresses, which must correspond with your network IP Address settings, or you can enable the DHCP negotiation to start after reset. Refer to "Correlating PC /MG 3200 IP Address & Subnet Mask" on page 143.

6. For the **Default Gateway Address**, **DNS Primary Server IP** and **DNS Secondary Server IP** fields, enter appropriate addresses. (If your network features a DNS server, clarify with your Network Administrator).

7. In the **Trunk Configuration** section, **Protocol Type** drop-down menu, select the appropriate option. In the **Clock Master Type** (the trunk clock source) drop-down menu, select either **Recovered** (the clock is recovered from the trunk; default) or **Generated** (the trunk clock source is provided by the internal/TDM bus clock source. The clock source depends on the parameter 'TDM Bus Clock Source' (**Advanced Configuration > TDM Bus Settings**).

8. For the **Framing Method** dropdown menu, select the appropriate option. (For E1 trunks, always set the Framing Method to **Extended Super Frame.** For J1, keep the default setting.)

Note: The Trunk Configuration parameters are global, and apply to all trunks. To configure trunks individually (per trunk), refer to "Trunk Settings" on page 173

9. For the **Line Code** dropdown menu, select either **B8ZS** (bipolar 8-zero substitution) for T1 trunks only; **HDB3** (high-density bipolar 3) for E1 trunks only; or **AMI (Alternate Mark Inversion)**, which applies to both T1 and E1.

10. In the **Control Protocol Type** section, for the **Call Agent IP** field, if your network does not feature a DNS server that automatically defines the Call Agent's IP address, enter the appropriate IP address. If you have a DNS server, the field is optional.

11. In the **Call Agent Port** field, enter the appropriate port ID. The default is **2944** for H.248.

12. In the **Call Agent Domain Name** field, when using the DNS server option, enter the Domain Name of the Call Agent operating with the MG 3200. The DNS server automatically detects the Call Agent's IP address from the Domain Name.

13. For the Trunk naming scheme, enter appropriate definitions for the **Physical Name Pattern, Logical RTP Name Pattern, and Logical ATM Name Pattern** fields. Ensure that the definitions you choose are the definitions that the Call Manager/Agent is configured with to identify your MG 3200

14. At the bottom of the screen, click the **Reset** button. A dialog box appears in which you confirm the reset action. The new information is added to the system configuration while the system is restarted. A message informing you of the waiting period appears. On the MG 3200, the Ready and LAN LEDs are lit green.

8.4.3 Protocol Management

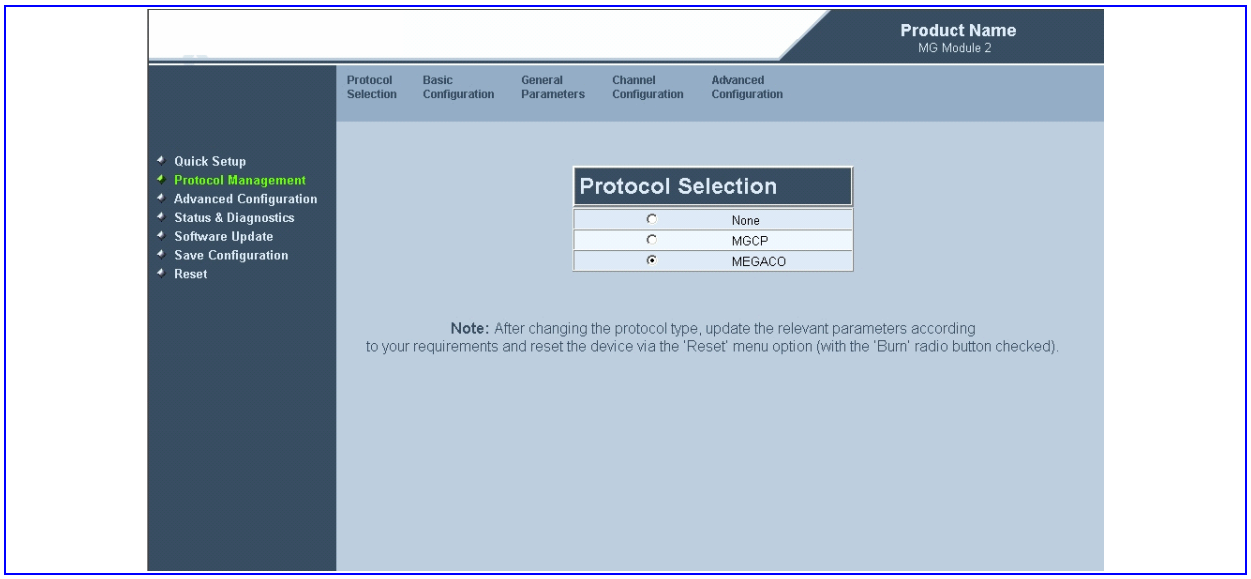
The Protocol Management screen offers access to the following Protocol configuration screens using the Sub-menu bar at the top of the screen:

- **Protocol Selection** - Refer to "Protocol Selection below
- **Basic Configuration** - Refer to 'Basic Configuration'
- **General Parameters** - Refer to 'General Parameters'
- **Channel Configuration** - Refer to 'Channel Configuration'
- **Advanced Configuration** - Refer to 'Advanced Configuration'
- **Media Server** - Refer to 'Media Server'

➢ To access the Protocol Management menu, take this step:

- From the main menu list on the left, click on the Protocol Management link. The Protocol Management screen with the sub-menu bar on the top is displayed.

Figure 8-4: Protocol Management Screen



8.4.3.1 Protocol Selection

➢ To select the protocol type, take these 2 steps:

1. From the main menu list on the left, click on the Protocol Management link. The Protocol Management screen appears.
2. Click the radio button of the desired protocol.

Note: Changing the protocol type requires a device reset. When you have completed configuring the desired parameters, the MG 3200 must be reset using the Reset screen (refer to "Reset Button" on page 205) for the changes to be implemented.

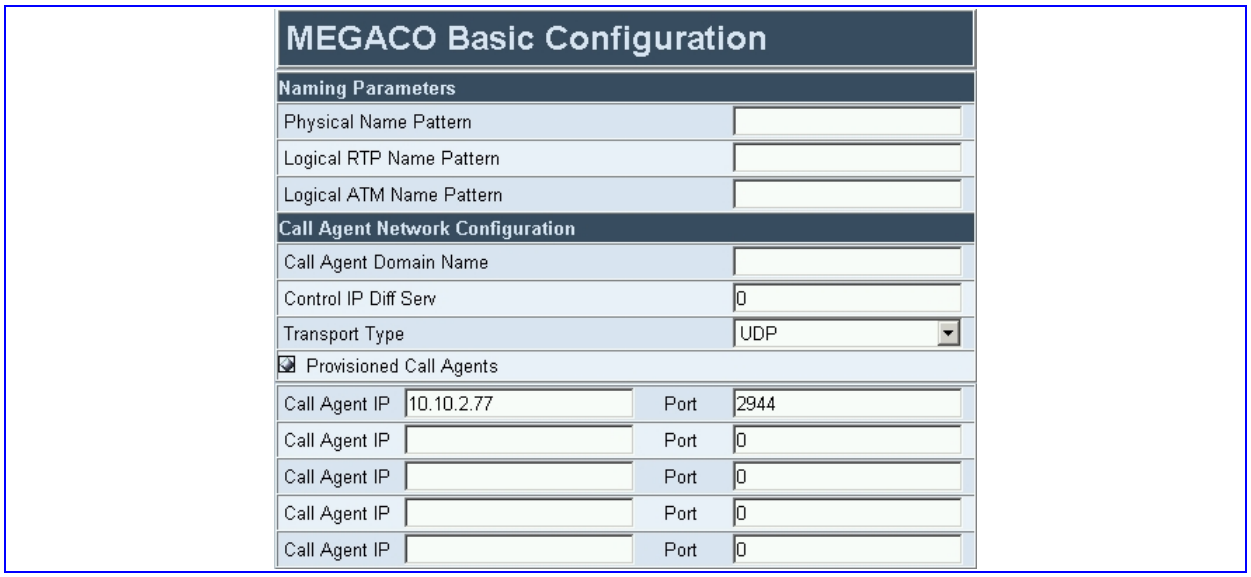
8.4.3.2 Basic Configuration

➢ To configure the Basic Configuration take these 4 steps:

1. From the main menu list on the left, click on the Protocol Management link. The Protocol Selection screen appears.

2. From the sub-menu bar on the top, click the Basic Configuration link. The Basic Configuration screen appears.

Figure 8-5: Basic Configuration Screen (H.248)



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the Basic Configuration parameter fields in the 'Basic Configuration' screen.

4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

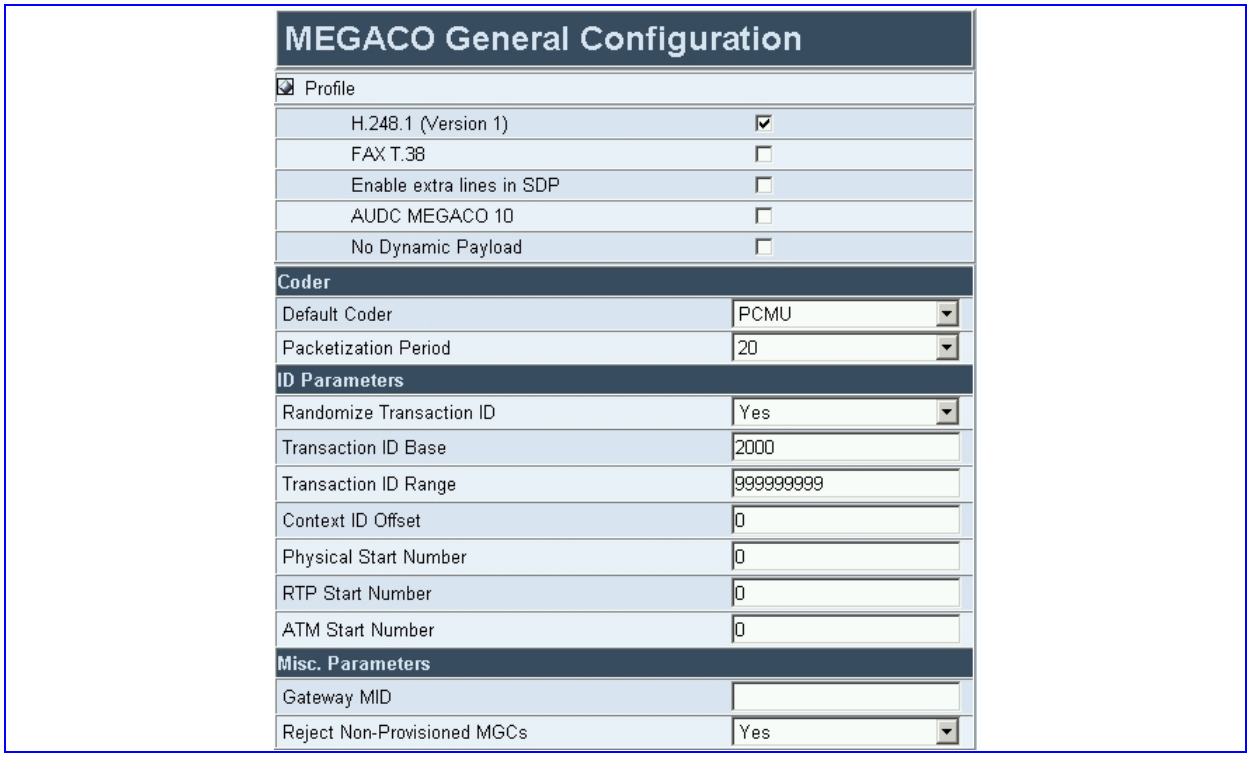
8.4.3.3 General Parameters

➢ To configure the General Parameters take these 2 steps:

1. From the main menu list on the left, click on the **Protocol Management** link. The Protocol Selection screen appears.

2. From the sub-menu bar on the top, click the **General Parameters** link. The General Parameters screen appears.

Figure 8-6: General Parameters Screen (H.248)



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the General Configuration parameter fields in the General Parameters screen.

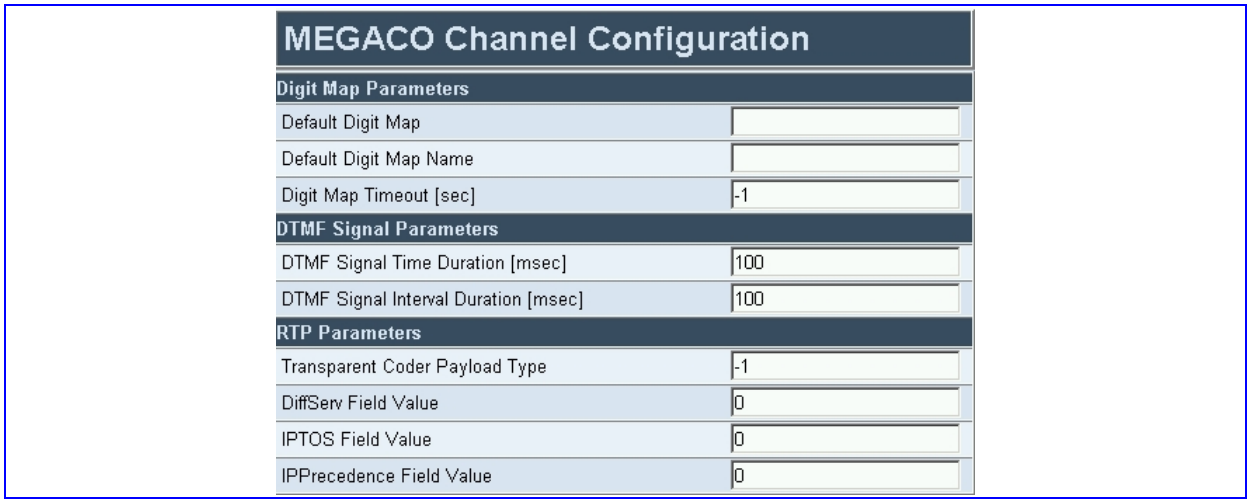
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

8.4.3.4 Channel Configuration

➢ To configure the Channel Configuration take these 4 steps:

1. From the main menu list on the left, click on the **Protocol Management** link. The Protocol Selection screen appears.
2. From the sub-menu bar on the top, click the **Channel Configuration** link. The Channel Configuration screen appears.

Figure 8-7: Channel Configuration Screen (H.248)



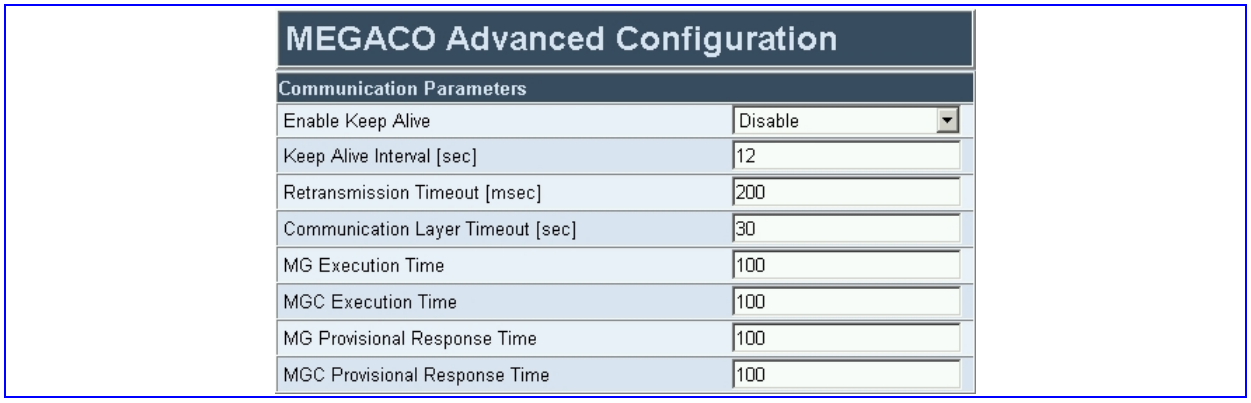
3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the Channel Configuration parameter fields in the 'Channel Configuration' screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

8.4.3.5 Advanced Configuration

➢ **To configure the Advanced Configuration take these 4 steps:**

1. From the main menu list on the left, click on the **Protocol Management** link. The Protocol Selection screen appears.
2. From the sub-menu bar on the top, click the **Advanced Configuration** link. The Advanced Configuration screen appears.

Figure 8-8: Advanced Configuration Screen (H.248)



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the Advanced Configuration parameter fields in the 'Advanced Configuration' screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

8.4.4 Advanced Configuration Screen

➢ **To access the Advanced Configuration screen take this step:**

■ To access the device's advanced configuration parameters, from the main menu list on the left, click the **Advanced Configuration** link. The Advanced Configuration Parameters screen appears with the sub-menu bar on the top displaying the following menu options:

- **Network Settings -** Contains a drop-down list with the following options:
  - **IP Settings** - Refer to "IP Settings" on page 157
  - **Application Settings** - Refer to "Application Settings" on page 158
  - **Web & Telnet Access List** - Refer to "Web & Telnet Access List" on page 159

- **Security Settings** - Refer to "Security Settings" on page 160
- **RTP Settings** - Refer to "RTP Settings" on page 166
- **Routing Table** - Refer to "Routing Table" on page 167
- **Ethernet Port Information** - Refer to "Ethernet Port Information" on page 168

Figure 8-9: Network Settings Drop-Down Menu

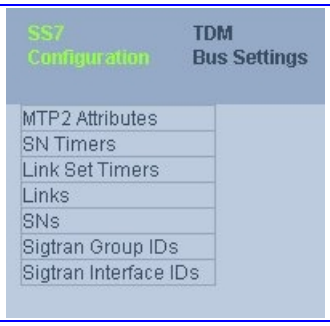
- **Channel Settings** - Contains a drop-down list with the following options:
  - **Voice Settings** - Refer to "Voice Settings" on page 168
  - **Fax/Modem/CID Setttings** - Refer to "Fax/Modem/CID Setttings" on page 169
  - **RTP Settings** - Refer to "RTP Settings" on page 170
- **IPmedia Settings** - Refer to "IPmedia Settings" on page 171

Figure 8-10: Channel Settings Drop-Down Menu

- **Trunk Settings** - Refer to "Trunk Settings" on page 172
- **SS7 Settings** - Contains a drop-down list with the following options:
  - **MTP2 Attributes** - Refer to "SS7 Parameters" on page 265
  - **SN Timers** - Refer to "SS7 Signaling Node Timers Table Parameters" on page 281
  - **Link Set Timers** - Refer to "SS7 Signaling LinkSet Timers Table Parameters" on page 285
  - **Links** - Refer to "SS7 Signaling Link Table Parameters" on page 287
  - **SNs** - Refer to "SS7 Signaling Node Table Parameters" on page 281
  - **SigTran Group IDs** - Refer to "SigTran Interface GroupsTable Parameters" on page 295

- **SigTran Interface IDs** - Refer to 'SigTran Interface IDs Table Parameters'

Figure 8-11: SS7 Settings Drop-Down Menu



- **TDM Bus Settings** - Refer to "TDM Bus Settings" on page 176
- **Configuration File** - Refer to "Configuration File" on page 177
- **Regional Settings** - Refer to "Regional Settings" on page 178
- **Change Password** - Refer to "Change Password" on page 180

Figure 8-12: Advanced Configuration Parameters Screen (SS7 disabled)

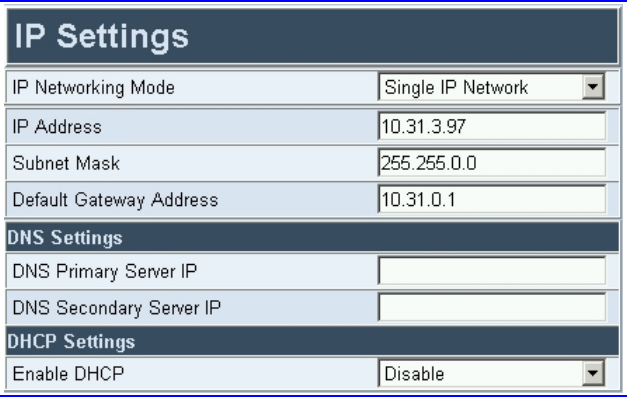
Figure 8-13: Advanced Configuration Parameters Screen (SS7 enabled)

8.4.4.1 IP Settings

➢ To configure the IP Settings, take these 4 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click on the **IP Settings** option. The IP Settings screen appears.

Figure 8-14: IP Settings Screen



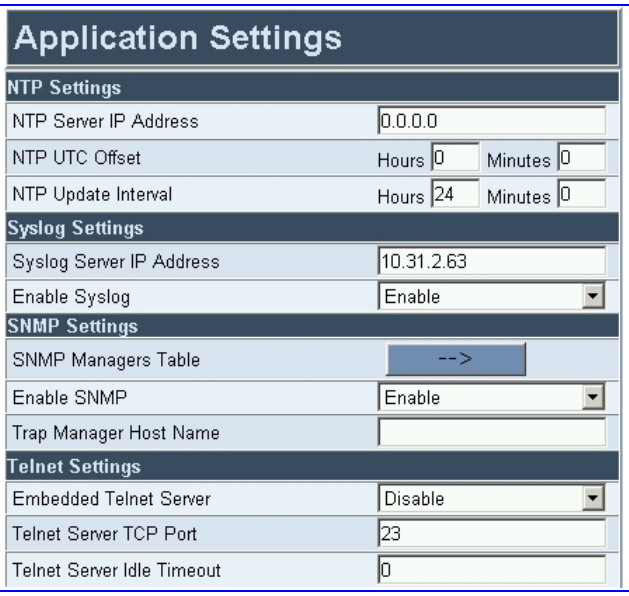
3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the IP Settings parameter fields in the IP Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

8.4.4.2 Application Settings

➢ To configure the Application Settings, take these 6 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click on the **Application Settings** option. The Application Settings screen appears.

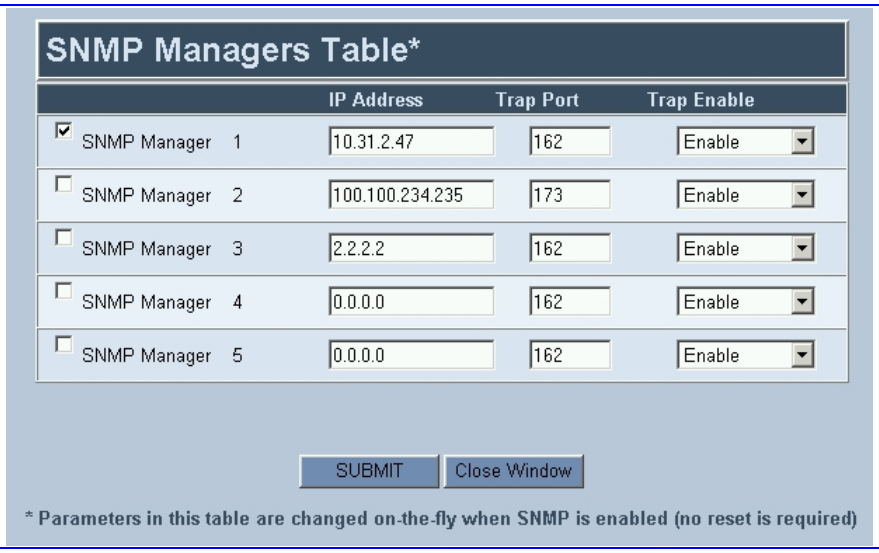
Figure 8-15: Application Settings Screen



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the network parameter fields in the Application Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

5. To access the SNMP Managers table, click the --> arrow button. The SNMP Manager's Table screen appears.

Figure 8-16: SNMP Manager's Table Screen



The SNMP Managers table allows you to configure the SNMP manager's attributes.

Note: By un-checking a checkbox and clicking submit, the whole table row is deleted. By checking the checkbox and clicking submit, the whole table row is created with the current field inputs in that row.

6. Configure the table as desired and click the **SUBMIT** button and then click the **Close Window** button. The lines appear in the Application Settings screen.

8.4.4.3 Web & Telnet Access List

➢ **To configure the Web & Telnet Access List, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click on the **Web & Telnet Access List** option. The Web & Telnet access List screen appears.

Figure 8-17: Web & Telnet Access List Screen

3. To add a new authorized IP address, in the **New Authorized IP Address** field at the bottom portion of the screen, enter the desired IP address and click the **Add New Address** button.

4. To delete an authorized IP address, in the upper portion of the screen, click a checkmark into the checkbox of the desired IP address row (checkmarks in more than one row is permissible) and click the **Delete Selected Addresses** button.

Note 1: When all authorized IP addresses are deleted this security feature becomes disabled.

Note 2: When adding the first authorized IP address, you should add your own terminal's IP address in order to be able to connect to the web server after adding the first IP address that is not your current terminal's IP address.

8.4.4.4 Security Settings

➢ **To configure the Security Settings, take these 15 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click the **Security Settings** option. The Security Settings screen appears.

Note: IPSec Security Settings availability is in accordance with the MG 3200's Software Upgrade Key.

Figure 8-18: Security Settings Screen

3. Configure the parameters using the following info as a guide:
   - Default Access Level

     200 – This is the default setting for the Security Administrator. (Refer to Table 8-2 on page 162)
   - Require Secured Web Connection (HTTPS)

     Disable (HTTP and HTTPS) – This is the default setting and allows both HTTP and HTTPS.

Enable (HTTPS only) – This mode allows only HTTPS communication.

- HTTP Authentication Mode

  Basic – Clear text is used during authentication.

  Digest when possible – This is the default setting. MD5 authentication is used.

  Basic if HTTPS, Digest if HTTP – This setting is required for Nortel IEMS Interworking. Digest is not required when using HTTPS since the channel is already encrypted.

4. Refer to Section 17.3 RADIUS Support for Radius Configuration.
5. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

Table 8-2: Available Access Levels and their Privileges

Access Levels	Numeric Representation*	Privileges
Security Administrator	200	Read / write privileges for all screens
Administrator	100	Read-only privilege for security-related screens and read / write privileges for the others
User Monitor	50	No access to security-related and file-loading screens and read-only access to the others
No Access	0	No access to any screen
* The numeric representation of the access level is used only to define accounts in a RADIUS server (the access level ranges from 0 to 255).		

6. To access the IPSec table, on the IPSec Table row, click the --> arrow button. The IPSec Table screen appears.

Figure 8-19: IPSec Table Screen (Existing Table Row)

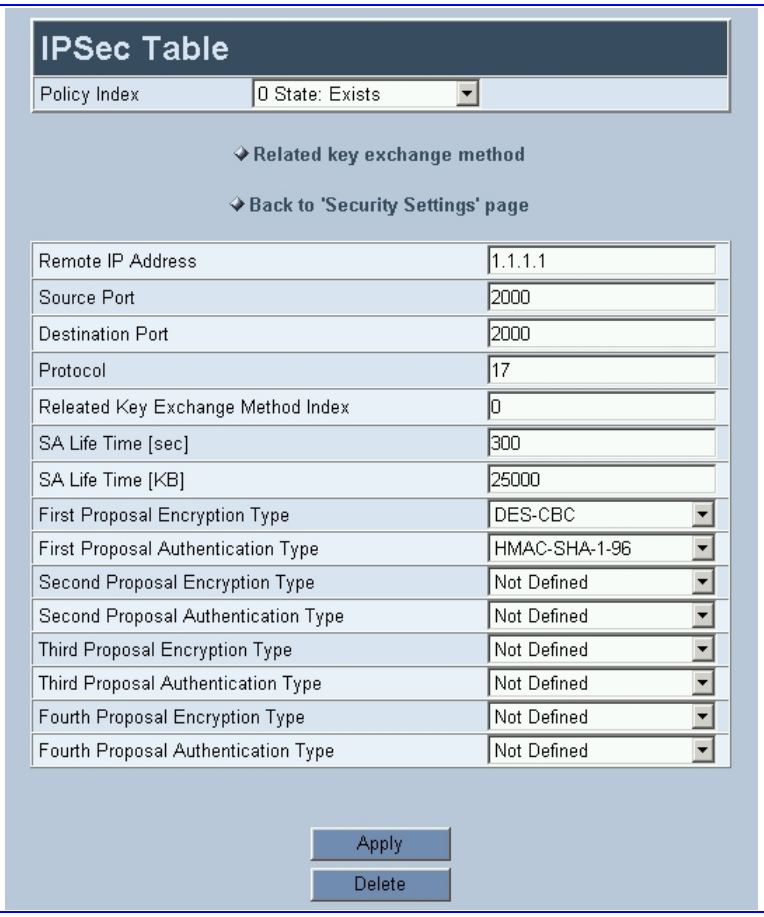
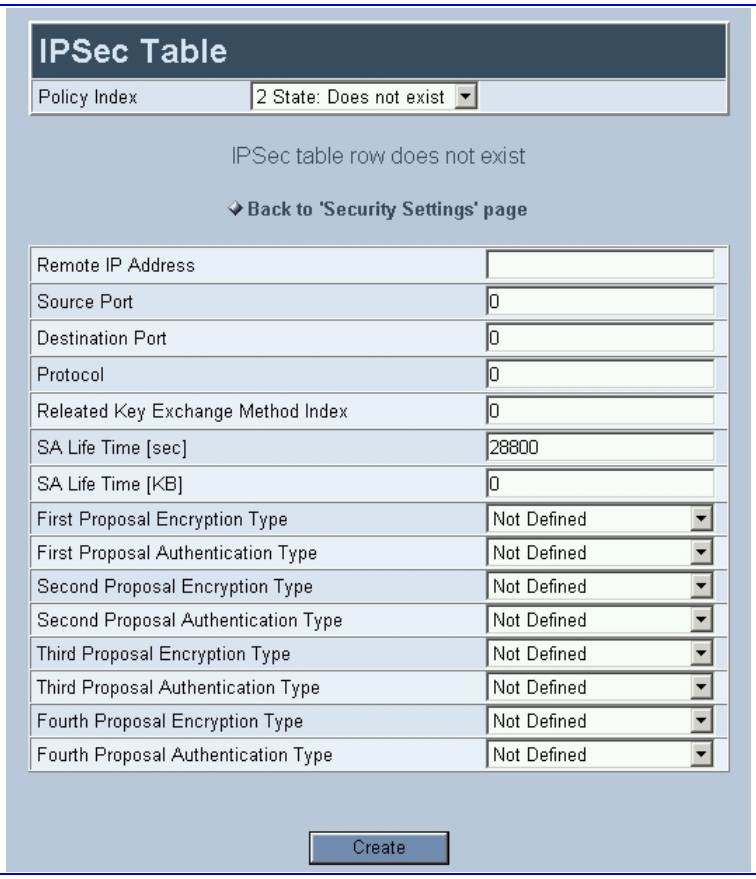


Figure 8-20: IPSec Table Screen (Non -Existing Table Row)



7. Each screen represents a single row in the Security Settings table. User can navigate between rows by selecting the desired row index in the **Policy Index** drop-down list at the top of the screen.
8. Table rows may be in 2 states – existent or non-existent – as stated in option showing in the **Policy Index** drop-down list.
9. For an existent row you may delete it by clicking the **Delete** button, or you may re-configure it by configuring the desired parameters and clicking the **Apply** button.
10. For a non existent row you may create it by configuring the parameters and clicking the **Create** button.

11. To access the IKE table, click the --> arrow button. The IKE Table screen appears.

Figure 8-21: IKE Table Screen (Existing Table Row)

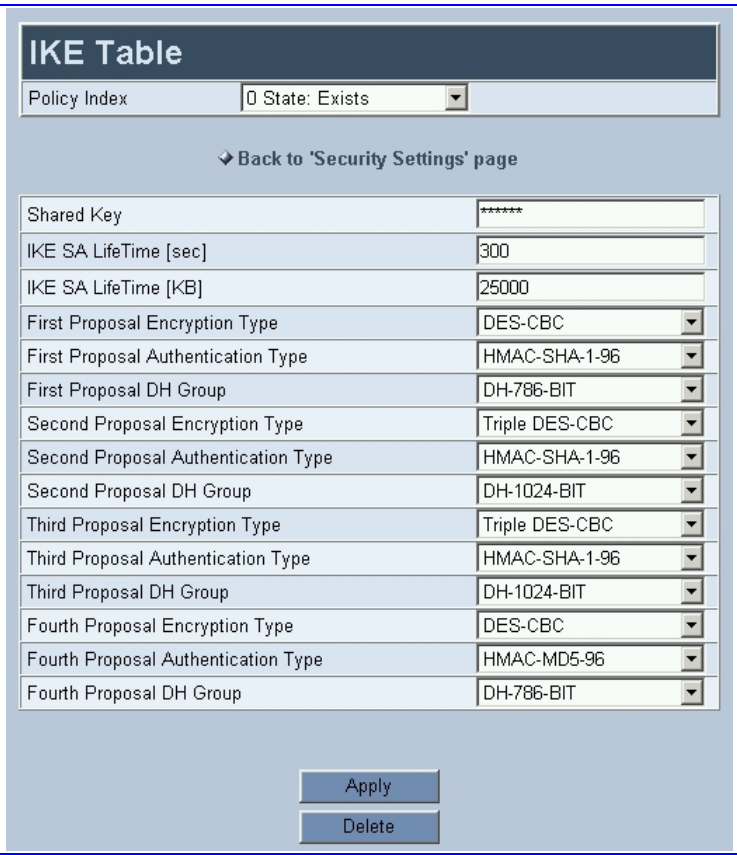
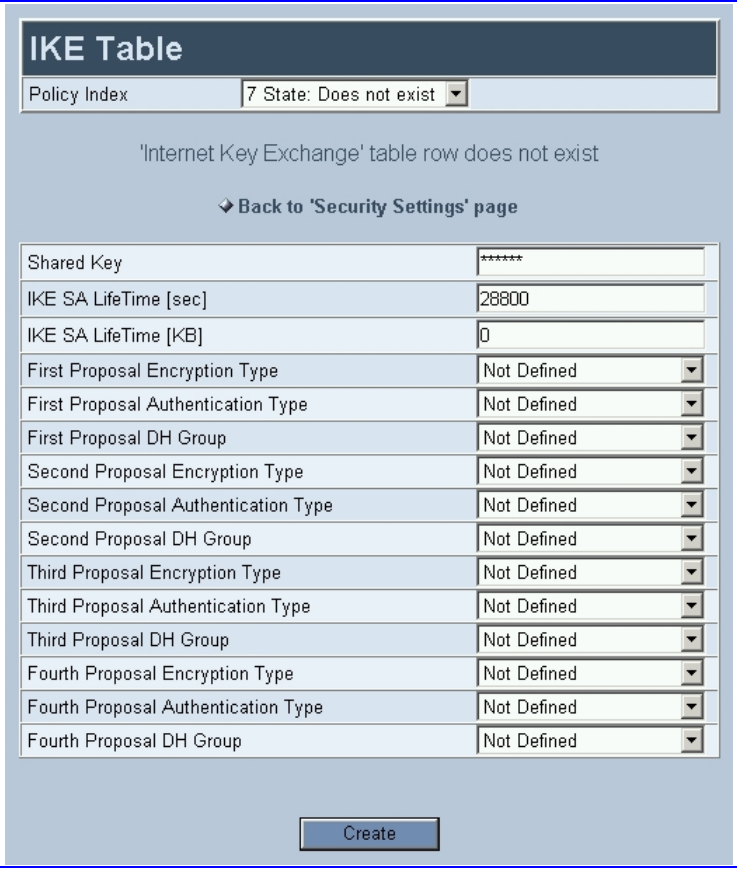


Figure 8-22: IKE Table Screen (Non -Existing Table Row)



12. Each screen represents a single row in the IKE table. User can navigate between rows by selecting the desired row index in the **Policy Index** drop-down list at the top of the screen.
13. Table rows may be in 2 states – existent or non-existent – as stated in the options showing in the **Policy Index** drop-down list.
14. For an existent row you may delete it by clicking the **Delete** button, or you may re-configure it by configuring the desired parameters and clicking the **Apply** button.
15. For a non existent row you may create it by configuring the parameters and clicking the **Create** button.

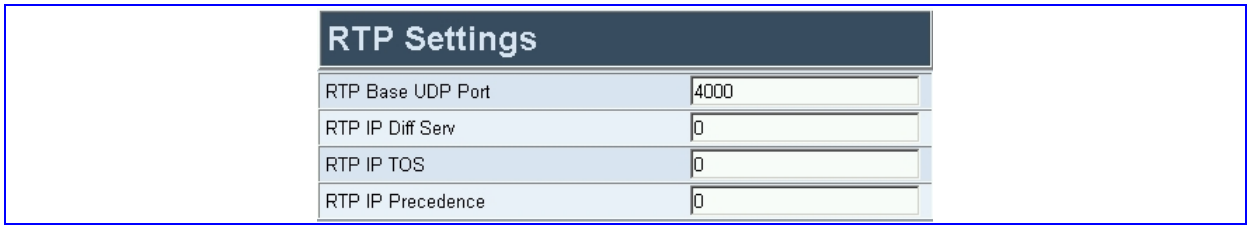
8.4.4.5 RTP Settings

➢ **To configure the RTP Settings, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click ON the **RTP Settings** option. The RTP Settings screen appears.

Figure 8-23: RTP Settings Screen (Network Settings)



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the RTP Settings parameter fields in the RTP Settings screen.

4. After configuring/modifying the parameter fields, click the SUBMIT button. The changes are entered into the system and the screen is refreshed.

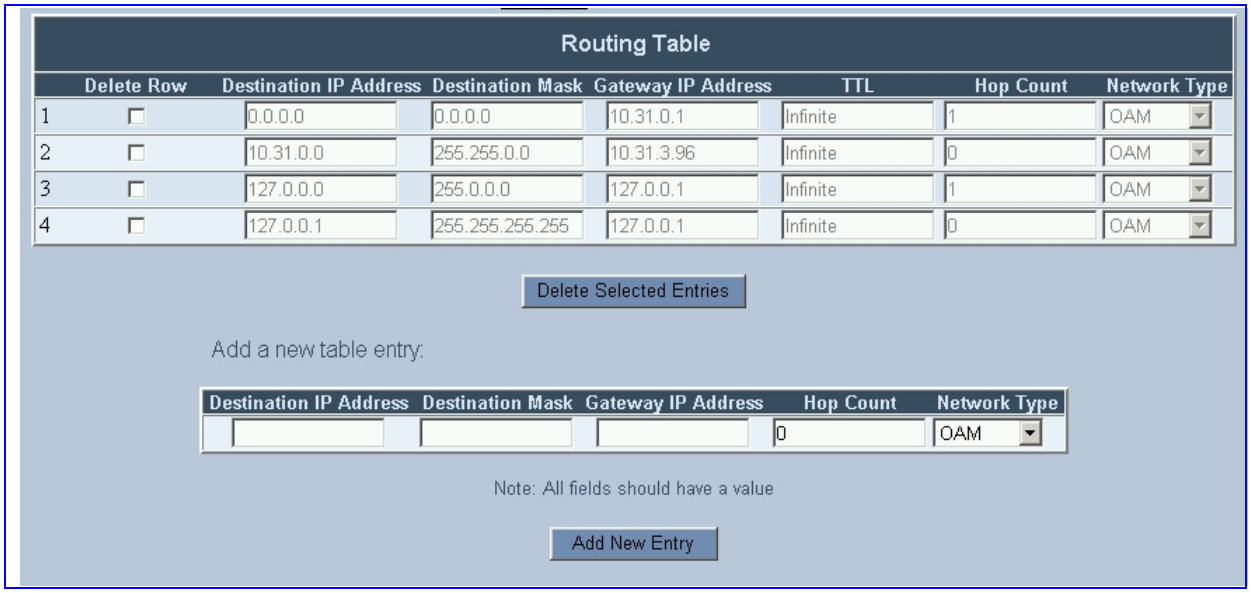
8.4.4.6 Routing Table

➢ To configure the Routing Table, take these 4 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click ON the **Routing Table** option. The Routing Table screen appears.

Figure 8-24: Routing Table Screen



3. To add a new routing entry, in the **Add a new table entry** fields at the bottom portion of the screen, enter a the entry data and the click the **Add New Entry** button.

4. To delete an existing entry in the upper portion of the screen, click a checkmark in the checkbox of the desired IP address row (more than one checkmark is permissible) and then click the **Delete Selected Entries** button.

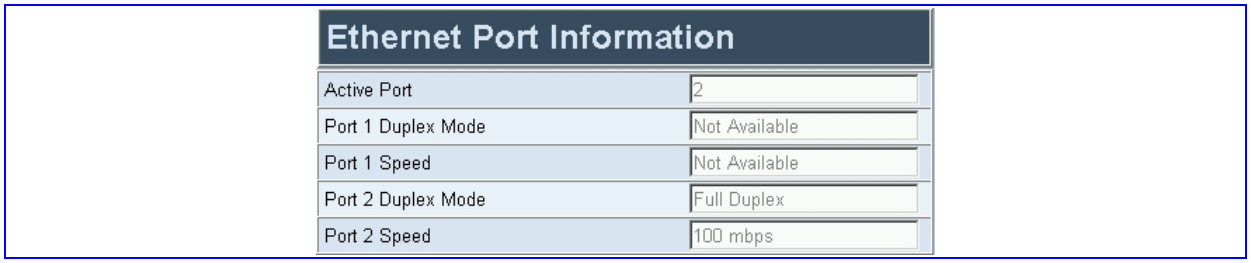
8.4.4.7 Ethernet Port Information

➢ To view the Ethernet Port Information, take these 2 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click the **Ethernet Port Information** option. The Ethernet Port Information screen appears.

Figure 8-25: Ethernet Port Information Screen

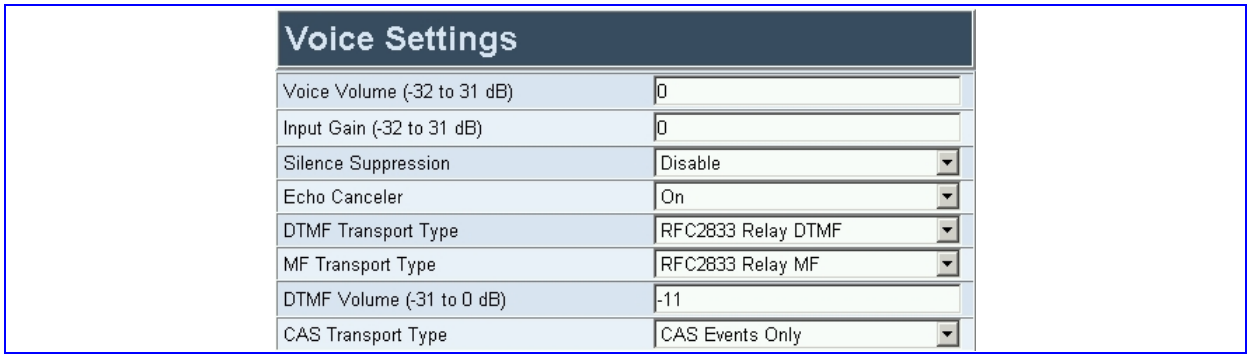


8.4.4.8 Voice Settings

➢ To configure the Voice Settings, take these 4 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, move the cursor on the **Channel Settings** link. A drop down menu appears. Click the **Voice Settings** option in the drop down list. The Voice Settings screen appears.

Figure 8-26: Voice Settings Screen



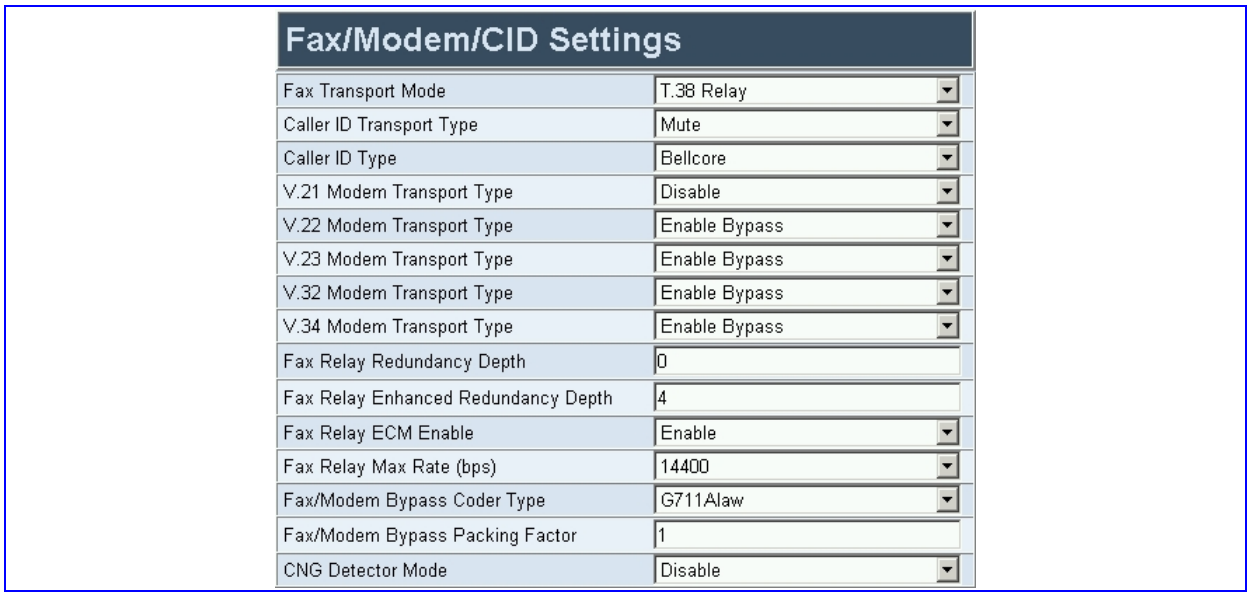
3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the **Voice Settings** parameter fields in the Voice Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

8.4.4.9 Fax/Modem/CID Settings

➢ To configure the Fax/Modem/CID Settings, take these 4 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, move the cursor on the **Channel Settings** link. A drop-down menu appears. Click on the **Fax/Modem/CID Settings** option. The Fax/Modem/CID Settings screen appears.

Figure 8-27: Fax/Modem/CID Settings Screen



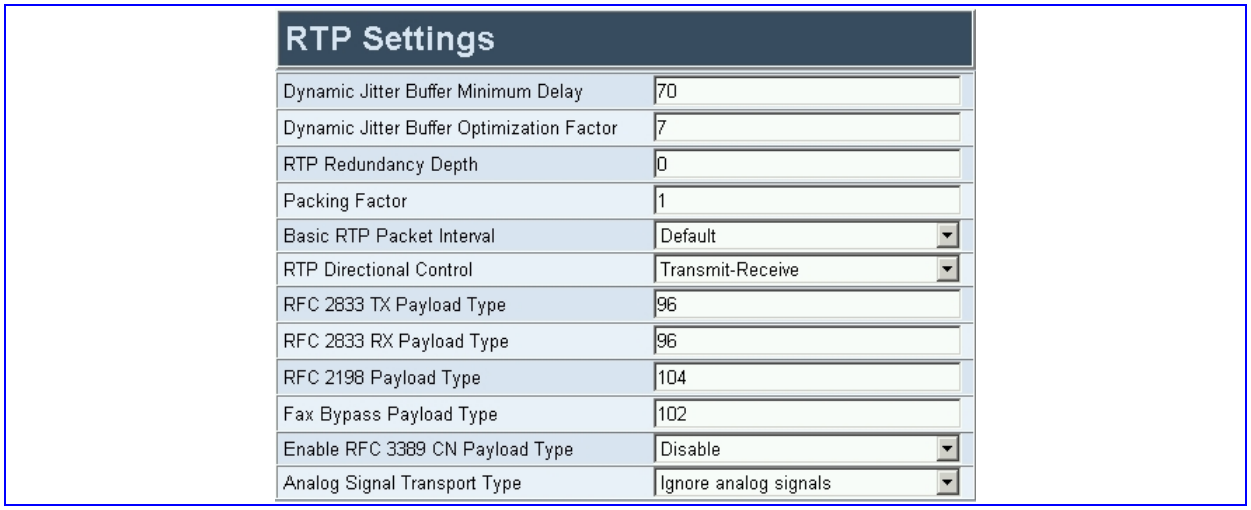
3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the Fax/Modem/CID Settings parameter fields in the Fax/Modem/CID Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

8.4.4.10 RTP Settings

➢ To configure the RTP Settings, take these 4 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, move the cursor on the **Channel Settings** link. A drop-down menu appears. Click on the **RTP Settings** option. The RTP Settings screen appears.

Figure 8-28: RTP Settings Screen (Channel Settings)



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the RTP Settings parameter fields in the RTP Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

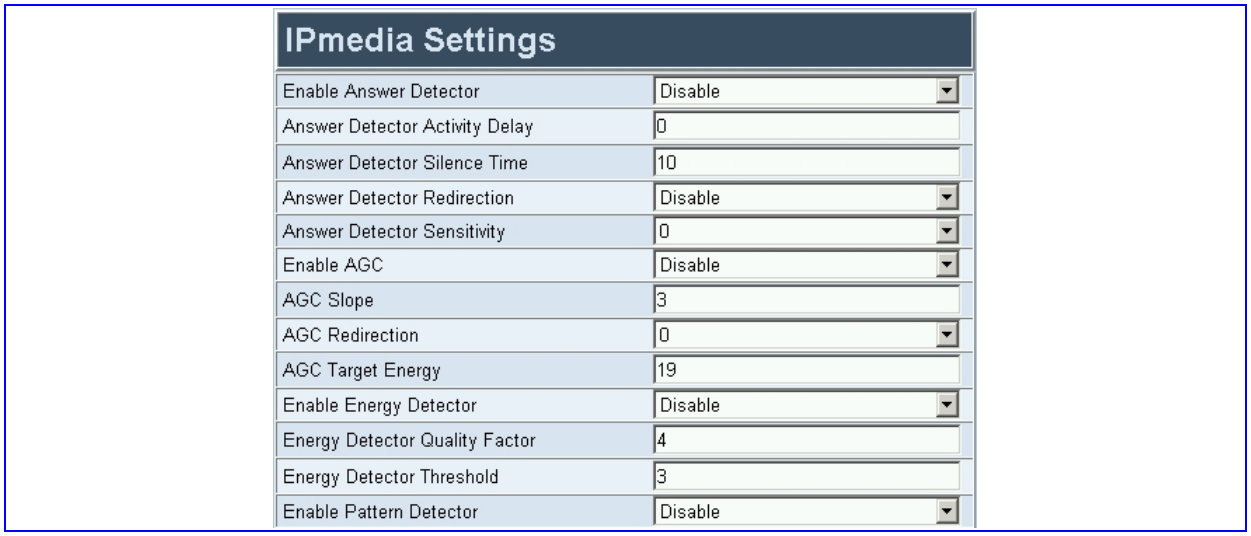
8.4.4.11 IPmedia Settings

➢ To configure the IPmedia Settings, take these 4 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Channel Settings** link. A drop-down menu appears. Click on the **IPmedia Settings** option. The IPmedia Settings screen appears.

Figure 8-29: IPmedia Settings Screen



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the IPmedia Settings parameter fields in the IPmedia Settings screen.

4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

8.4.4.12 Trunk Settings

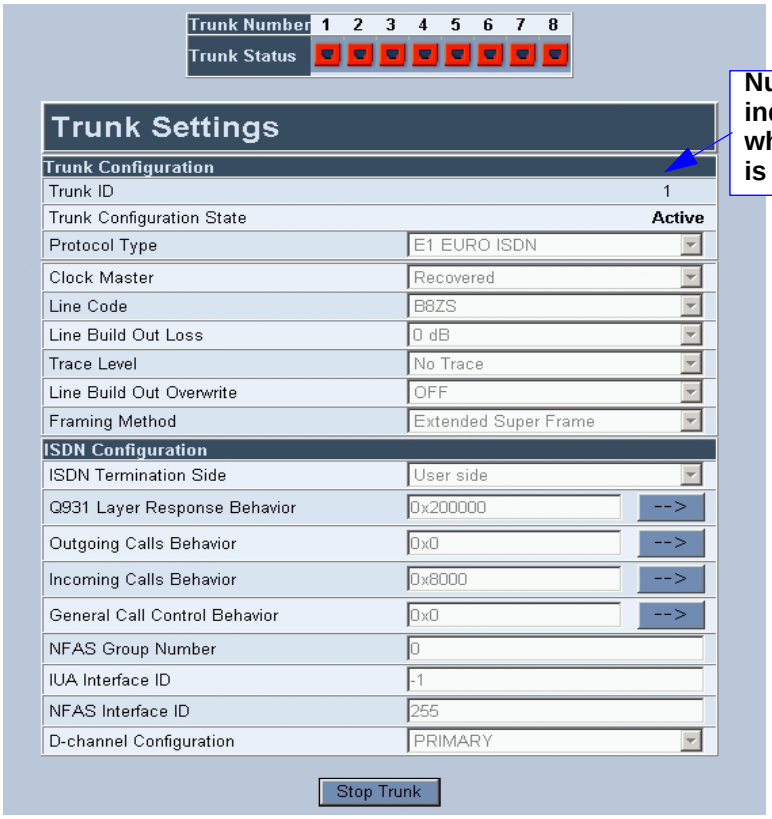
➢ To view the Trunk Settings, take these 11 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen.

2. From the Advanced Configuration screen, click the **Trunk Settings** option in the sub-menu bar on the top. The Trunk Settings screen appears.

   Initially, the screen appears with the parameters fields grayed (indicating read-only). The **Stop Trunk** button appears at the bottom of the screen.

Equation 1: Trunk Settings Screen



3. To configure a specific trunk's parameters or make a change to any of the parameters, from the Trunks displayed on the top, click the Trunk Status indicator  to select a **Trunk.** The number of the Trunk is displayed in the upper-right-hand corner of the Trunk Configuration display. The parameters displayed are for the selected Trunk only.

   The Trunk Status indicators can appear colored. The table below shows the possible indicators and their descriptions.

Table 8-3: Trunk Status Color Indicator Key

Indicator	Color	Status	Description
	Gray	Disabled	
	Green	Active - OK	
	Yellow	RAI Alarm	Remote Alarm Indication (the yellow alarm)
	Red	LOS/LOFS	Loss of Signal or Loss of Frame – move the cursor on trunk to view the alarm type
	Blue	AIS Alarm	Alarm Indication Signal (the blue alarm)
	Orange	D-Channel Alarm (ISDN only)	D-Channel Alarm (ISDN only)

When modifying the Protocol Type, there are three different menu types that match the following 3 protocol families:

- Transparent
- ISDN
- CAS

When traversing between these 3 protocol families, the menu is modified to include additional parameters appropriate to the family type selected.

1. At the bottom of the screen, click the **Stop Trunk** button to return the screen to a modifiable state. The parameters are no longer grayed. When all trunks are stopped (in a modifiable mode), two buttons are displayed at the bottom of the screen:

   - **Apply Trunk Settings** button
   - **Apply to all Trunks** button

   When at least one trunk has an Active trunk configuration state), only the **Apply Trunk Settings** button appears.

2. In the **Trunk Configuration** section, from the **Protocol Type** and **Framing Method** drop-down lists, select the appropriate option. Since in the example displayed in the figure below, **Protocol Type** is configured as E1 EURO ISDN, the ISDN parameters are displayed. Configure the parameter **ISDN Termination Side** as “User side” when the PSTN or PBX side is configured as “Network side”, and vice versa. If you do not know the MG 3200 ISDN termination side, choose “User side” and refer to the Status & Diagnostics screen. If the D-channel alarm is indicated, choose “Network side”. For E1 trunks, always set the **Framing Method** to Extended Super Frame.

3. For each of the **Bit** line items, enter the direct Hex value of the bits in the text box,

   or,

   configure the bit map directly by clicking the 

   arrow button, a new window appears, with the specific bits (refer to the figure below).

Figure 8-30: Q931 Bit Map Screen

4. For the **Clock Master** (the trunk clock source) drop-down list, select either 'Recovered' (the clock is recovered from the trunk; default) or 'Generated' (the trunk clock source is provided by the internal/TDM bus clock source) the above selection depends on the parameter 'TDM Bus Clock Source'. Refer to "TDM Bus Settings" on page 176.

5. For the **Line Code** drop-down list, select either **B8ZS** (bipolar 8-zero substitution) for T1 trunks only; **HDB3** (high-density bipolar 3) for E1 trunks only; or **AMI** for both T1 and E1.

6. After modifying any parameters, do one of the following:

   - To apply the changes to the selected trunk only, click the **Apply Trunk Settings** button.
   - When configuring the device for the first time, or when no protocol is specified for any trunk, To apply the changes to all trunks, click the **Apply To All Trunks** button.

   The screen is refreshed. Parameters become read-only (shown grayed). The **Stop Trunk** button is displayed at the bottom of the screen.

   To make a change to any of the parameters, click the **Stop Trunk** button to return the screen to a modifiable state.

7. To commit the changes to the non-volatile (flash) memory, in the main menu on the left, click the **Save Configuration** link. The Save Configuration screen appears.

8. Click the **Save** button. The configuration is saved to non-volatile (flash) memory.

Note 1: A device reset may be needed in certain circumstances for the setup to be activated, if a reset is needed the Web interface alerts the user. In case such a device reset is needed, click the **Reset** link in main menu to the left, choose the **Burn** option and click the **Reset** button to restart the device with the new configuration.' (Refer to 'Rese't Button' on page 205.)

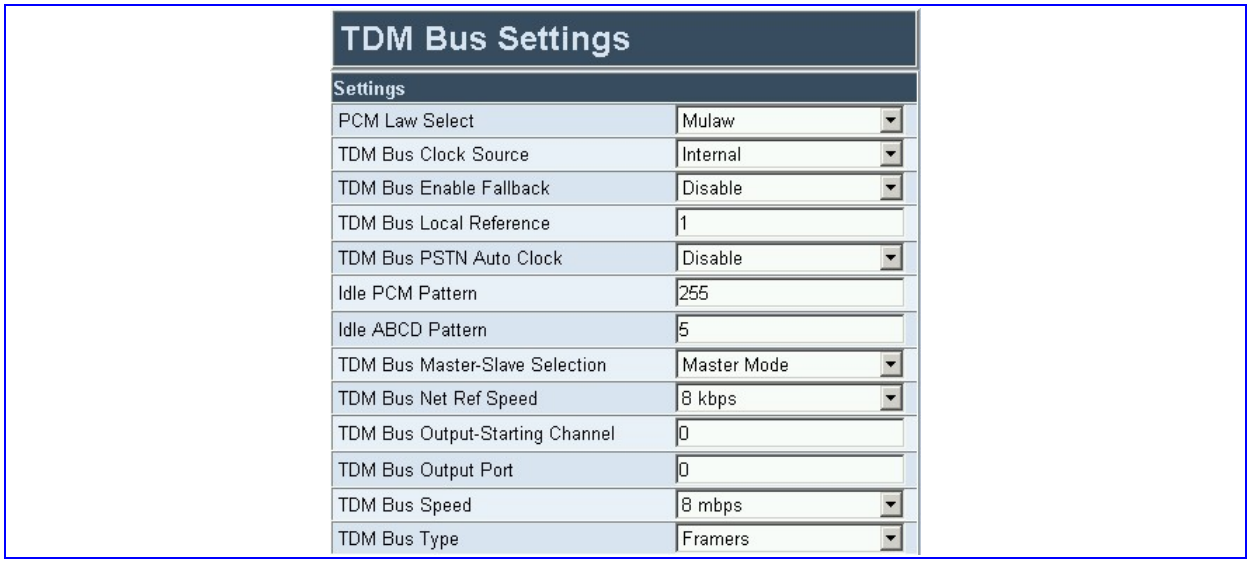
Note 2: If you are modifying multiple screens, and a reset is required in a certain screen, perform the reset after you are finished modifying all of the screens you intended and NOT after each screen.

8.4.4.13 TDM Bus Settings

➢ **To configure the TDM Bus settings, take these 6 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the Advanced Configuration screen, click the **TDM Bus Settings** option in the sub-menu bar on the top. The TDM Bus Settings screen appears.

Figure 8-31: TDM Bus Settings Screen



3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 233 as a reference when configuring/modifying the parameter fields in the 'TDM Bus Settings' screen.
4. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the screen is refreshed.
5. To commit the changes to non-volatile (flash) memory, on the main menu to the left, click the **Reset** link. The Reset screen appears.
6. Select the **Burn** option and click the **Reset** button. (Refer to "Reset Button" on page 205.)

Note 1: A device reset may be needed in certain circumstances for the setup to be activated. Reset can be scheduled for a later time period when call traffic is at a minimum. If you choose to schedule the Reset for a later time, be sure to use' the 'Save Configuration scre'en' on page 204 to retain the changes to the MG 3200's non-volatile memory.

Note 2: If you are modifying multiple screens, perform the reset after you are finished modifying all of the screens you intended and NOT after each screen.

8.4.4.14 Configuration File

The Configuration File screen enables you to restore/change (download a new *ini* file to the Device) or backup the current configuration file that the device is using (make a copy of the VoIP device's *ini* file and store it in a directory on your PC).

- Restore your configuration - If the VoIP device has been replaced or has lost its programming information, you can restore the VoIP device configuration file from a previous backup or from a newly created *ini* file. To restore the VoIP Device configuration from a previous backup you must have a backup of the VoIP device information stored on your PC. (For information about restoring *ini* file defaults or backup files, refer to' 'Restoring and Backing Up the MG 3200 Configuration' on page 207'.)
- Back up your configuration - If you want to protect your VoIP device programming. . The generated backup *ini* file contains values that have been set by the user or are other than the default values.

In the Configuration File screen, you can bring an *ini* file from the device to a directory in your PC, and send the *ini* file from your PC to the device.

Protect the device configuration by bringing the *ini* file from the device to your PC. Later, if another device is replaced or loses its programming data, you'll be able to restore / send the *ini* file backed up on your PC to the device.

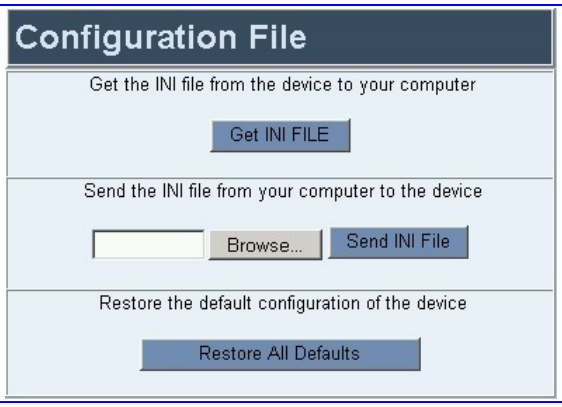
The *ini* file is a proprietary configuration text file containing configuration parameters and data. Sending the *ini* file to the device only provisions parameters that are contained in the *ini* file.

The *ini* file with parameters set at their default values is on the CD accompanying the device. The *ini* file can also be received as an e-mail attachment from Nortel Technical Support. Users can also generate their own *ini* file using The **DConvert** utility (refer to the Appendix, "Utilities" on page 353).

➢ To save the *ini* file to the PC, take these 3 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the Advanced Configuration screen, click the **Configuration File** link in the sub-menu bar on the top. The Configuration File screen appears.

Figure 8-32: Configuration File Screen



3. Click the **Get** *ini* **File** button. You are prompted to select a location in which to save it.

Note: The *ini* file that you save from the device to the PC contains only those parameters whose values you modified following receipt of the device. It does not contain parameters unchanged at their (original) default value.

➢ To load an ini file from the PC to the device, take these 4 steps:

1. Click on the **Browse** button next to the **Send the** *ini* **file from your computer to the device** field and navigate to the location of the predefined *ini* file. Refer to the figure below.
2. Click the **Send File** button. The file loading process is activated. When the loading is complete, a verification message is displayed at the bottom of the screen: **File XXXX was successfully loaded into the device**.
3. From the main menu list on the left, click **Reset**. The Reset screen appears.
4. Select the **Burn** option and click the **Restart** button. Wait for the device to reset. After self-testing, the Ready and LAN LEDs on the device's front panel are lit green. Any malfunction causes the Ready LED to change to red.

Users can restore default parameters by clicking the **Restore All Defaults** button.

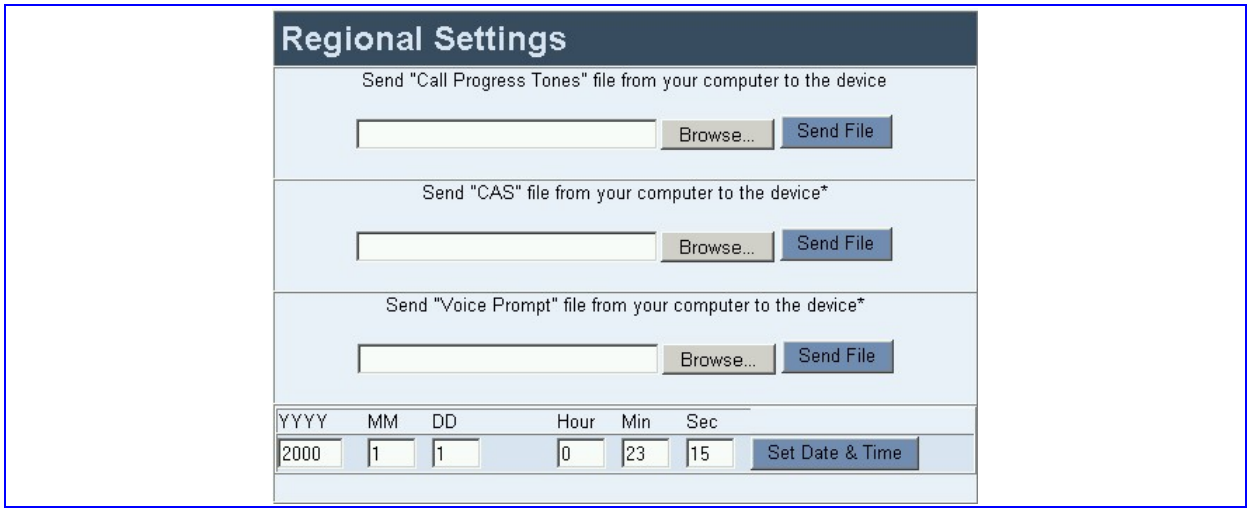
8.4.4.15 Regional Settings

From the Regional Settings screen users can send a Call Progress Tones *dat* file, a CAS *dat* file and/or a Voice Prompts *dat* file to the device from their PC.

➢ To access the Regional Settings screen, take these 2 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, click the **Regional Settings** link. The Regional Settings screen appears.

Figure 8-33: Regional Settings Screen - Sending CPT, CAS and/or Voice Prompt File to the Device



The files are available on the CD accompanying your device. They can also be received as an e-mail attachment from Nortel Technical Support. A Call Progress Tones *txt* file can be modified and converted into the binary *dat* file (refer to 'Converting a CPT *ini* File to a Binary *dat* File' in the Appendix, 'Utilities'). When modifying the Call Progress Tones File, only the *dat* file can be sent from your PC to the device. (Refer to "Modifying the Call Progress Tones File" on page 74 and the Appendix, "Utilities" on page 353.)

- The Call Progress Tones *dat* file is a region-specific, telephone exchange-dependent file. It provides call status/call progress to Customers, operators, and connected equipment. Default Tone: U.S.A.
- E1/T1 CAS signaling files, such as *E_M_WinkTable.dat*. These files are needed for CAS protocols only.

  (Note: For release prior to 5.0, it is recommended to always use a unique filename when downloading CAS files to the MG3200 gateway. For example, alter the filename by including a unique release identifier, date time string, or other meaningful text. Failure to do so will result in difficulty managing the CAS files due to having several entries with the same name in the CAS file selection box which may or may not be functionally identical).
- The *dat* Voice Prompts file is played by the device during the phone conversation on Call Agent request. Download if you have an application requiring Voice Prompts. The Voice Prompt buffer size in the board is 10 Mbyte.

➢ To send a Call Progress Tone, CAS, or Voice Prompt file to the board, take these 6 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, click the **Regional Settings** link. The Regional Settings screen appears. (Refer to the figure below.)
3. Click the **Browse** button to locate the predefined **Call Progress Tone**, **CAS**, or **Voice Prompt** file as appropriate. (A new software file package may be issued from Nortel or your local supplier.)
4. Click the **Send File** button. The file is sent to the board, overwriting the previous one. The screen is refreshed and a message informs you about the waiting period. When the loading is complete, a verification message is displayed at the bottom of the screen: **File XXX was successfully loaded into the device.**
5. For CPT file downloading only - (The rest of files do not require a device reset.) From the main menu list on the left, click **Reset**. The Reset screen appears.
6. Select the **Burn** option and click the **Restart** button. Wait for the device to reset. After self-testing, the Ready and LAN LEDs on the device's front panel are lit green. Any malfunction causes the Ready LED to change to red.

➢ To set the date and time, take these 2 steps:

1. Enter the date and/or time using the **YYYY**, **MM**, and **DD** field for Year, Month and Day and **HH**, **MM**, and **SS** fields for Hour, Minutes and Seconds.
2. Click the **Set Date and Time** button. The date and time is set on the device, accordingly.

Note: When the NTP feature is enabled (the NTP server is defined in the Network Settings screen), the date and time are in **Read Only** mode as they are set by the NTP server.

8.4.4.15.1 Change Password

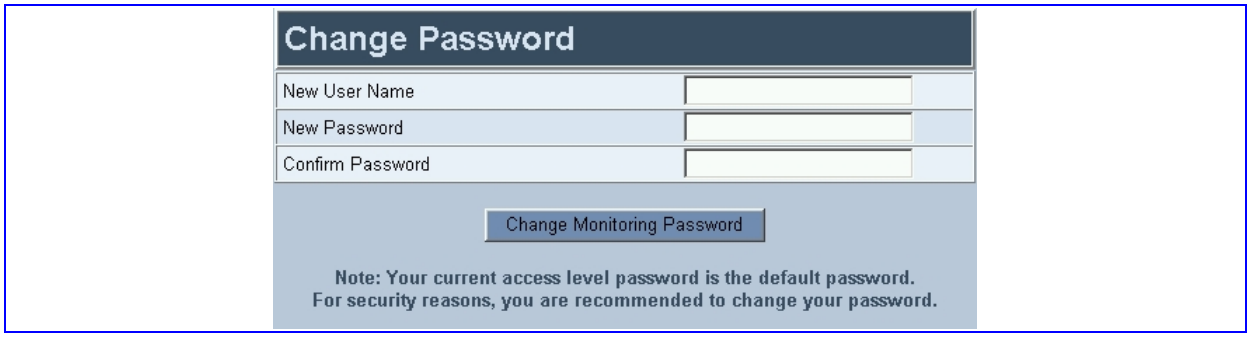
➢ **To change the Password, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, click the **Change Password** link. The Change Password screen appears.

Note: A user with Administrator privileges may change both Administrator and Monitoring level passwords. A user with Monitoring privileges may change only the Monitoring level password.

Figure 8-34: Change Password Screen - For Users with Administrator Privileges

Figure 8-35: Change Password Screen - For Users with Monitoring Privileges



3. Enter a User Name and New Password into the fields and confirm the New Password in the **Confirm Password** field.
4. To apply new settings to the Administrator level, click the **Change Administrator Password** button. You are prompted to enter a new username and password. The new username/password takes effect immediately.

To apply new settings to the Monitoring level, click the **Change Monitoring Password** button. The new username/password takes effect immediately.

When making a change, note that the Password and Username can be up to 7 characters and that they are case sensitive. The new password takes effect immediately.

➢ To reset the username and password to their defaults:

- Set the *ini* file parameter ResetWebPassword to **1** and use the BootP/TFTP Server to load the *ini* file to the device (refer to the Appendix, "BootP/TFTP Server" on page 223). After loading, the username and password automatically revert to their default values (Admin).

Note: This procedure resets both Administrator and Monitoring level passwords to their defaults.

8.4.5 Status and Diagnostic Menu

➢ To access the Status and Diagnostics menu, Take this step:

- From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen with the sub-menu bar on the top is displayed.

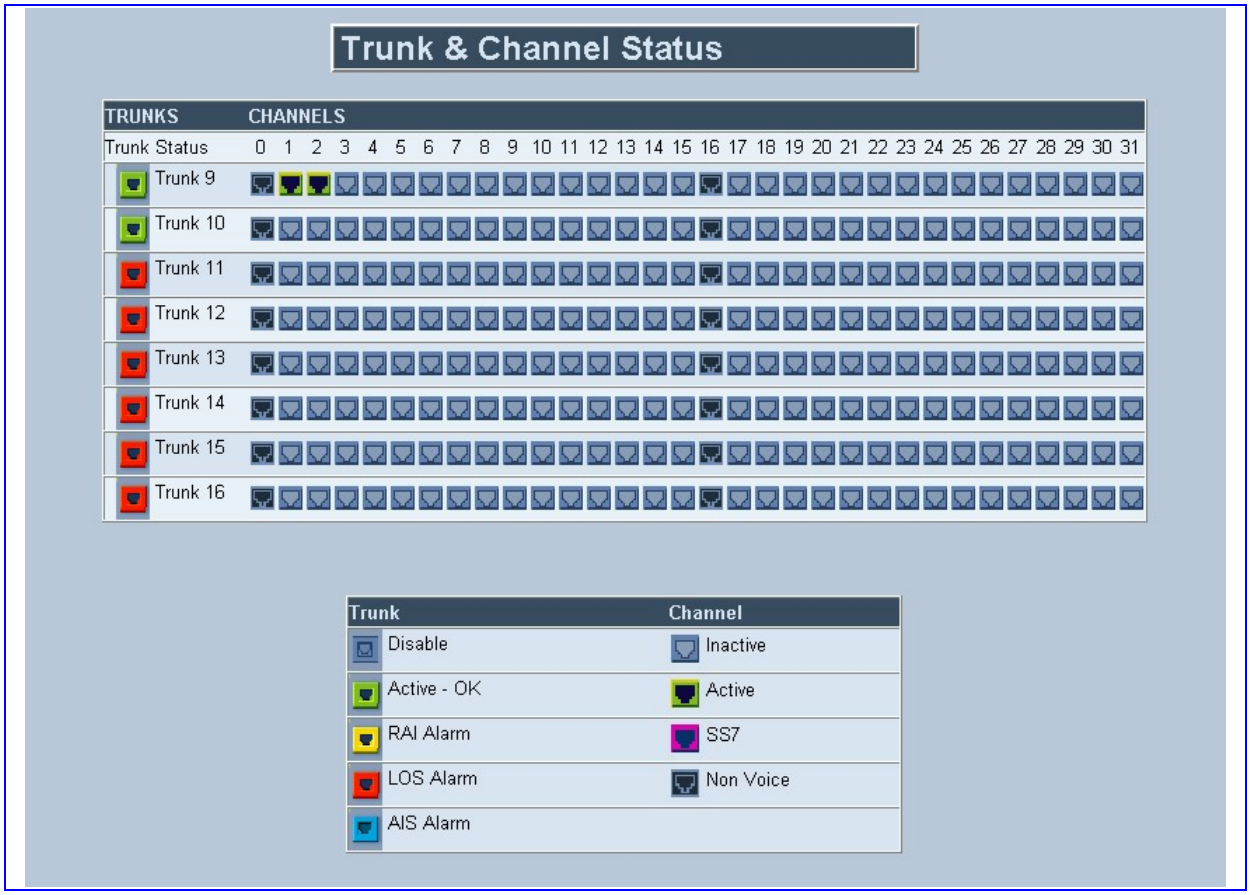
Figure 8-36: Status and Diagnostic Menu Screen

8.4.5.1 Trunk and Channel Status

➢ **To access the Trunk and Channel Status screen, take these 3 steps:**

1. From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears.
2. From the sub-menu bar on the top, click the **Channel Status** link. The Trunk and Channel Status screen appears. The screen is Read-only.

Figure 8-37: Trunk and Channel Status Screen



The number of trunks and channels that appear on the screen depends of the system configuration.

The Trunk and Channel Status indicators can appear colored. The table below shows the possible indicators and their descriptions.

Table 8-4: Trunk and Channel Status Color Indicator Key

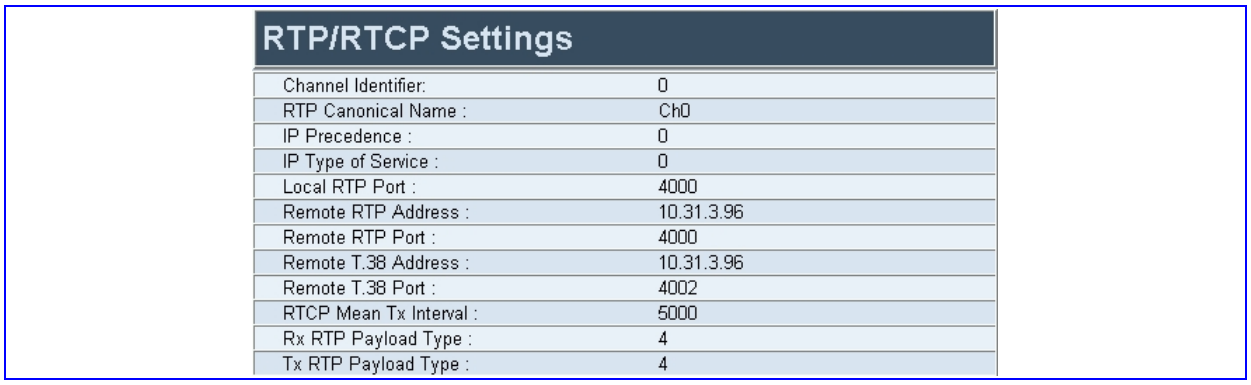
Trunk			Channel		
Indicator	**Color**	**Description**	**Indicator**	**Color**	**Description**
	Gray	Disabled		Gray	Inactive
	Green	Active - OK		Green	Active
	Yellow	RAI Alarm		Purple	SS7
	Red	LOS/LOF Alarm		Black	Non-Voice
	Blue	AIS Alarm			
	Orange	D-Channel Alarm			

3. To display a screen with a summary of parameter information relevant to a channel, click on the channel.

The following 'per channel' screen information is available when clicking on a specific channel:

Figure 8-38: Channel Status Screen

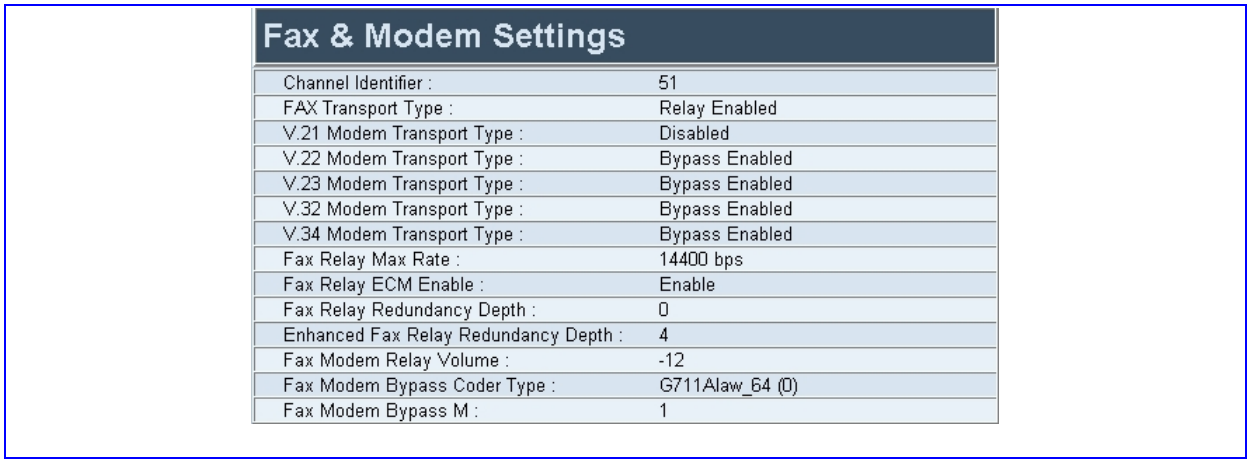
Figure 8-39: RTP/RTCP Settings Screen



RTP/RTCP Settings

Channel Identifier:	0
RTP Canonical Name :	Ch0
IP Precedence :	0
IP Type of Service :	0
Local RTP Port :	4000
Remote RTP Address :	10.31.3.96
Remote RTP Port :	4000
Remote T.38 Address :	10.31.3.96
Remote T.38 Port :	4002
RTCP Mean Tx Interval :	5000
Rx RTP Payload Type :	4
Tx RTP Payload Type :	4

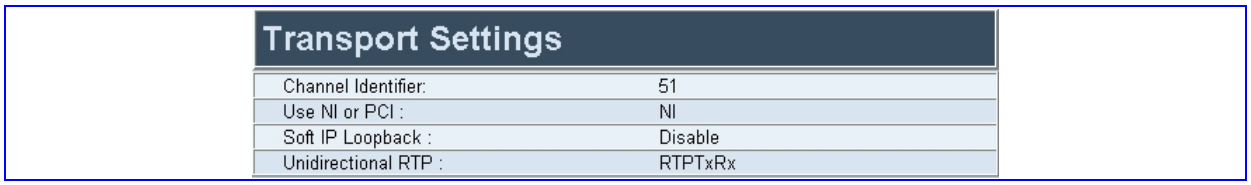
Figure 8-40: Fax & Modem Settings Screen



Fax & Modem Settings

Channel Identifier :	51
FAX Transport Type :	Relay Enabled
V.21 Modem Transport Type :	Disabled
V.22 Modem Transport Type :	Bypass Enabled
V.23 Modem Transport Type :	Bypass Enabled
V.32 Modem Transport Type :	Bypass Enabled
V.34 Modem Transport Type :	Bypass Enabled
Fax Relay Max Rate :	14400 bps
Fax Relay ECM Enable :	Enable
Fax Relay Redundancy Depth :	0
Enhanced Fax Relay Redundancy Depth :	4
Fax Modem Relay Volume :	-12
Fax Modem Bypass Coder Type :	G711Alaw_64 (0)
Fax Modem Bypass M :	1

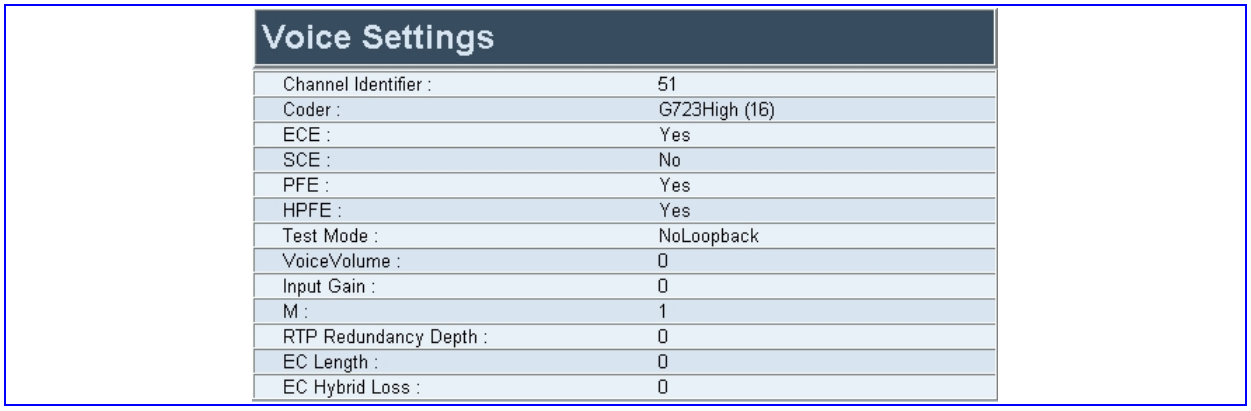
Figure 8-41: Transport Settings Screen



Transport Settings

Channel Identifier:	51
Use NI or PCI :	NI
Soft IP Loopback :	Disable
Unidirectional RTP :	RTPTxRx

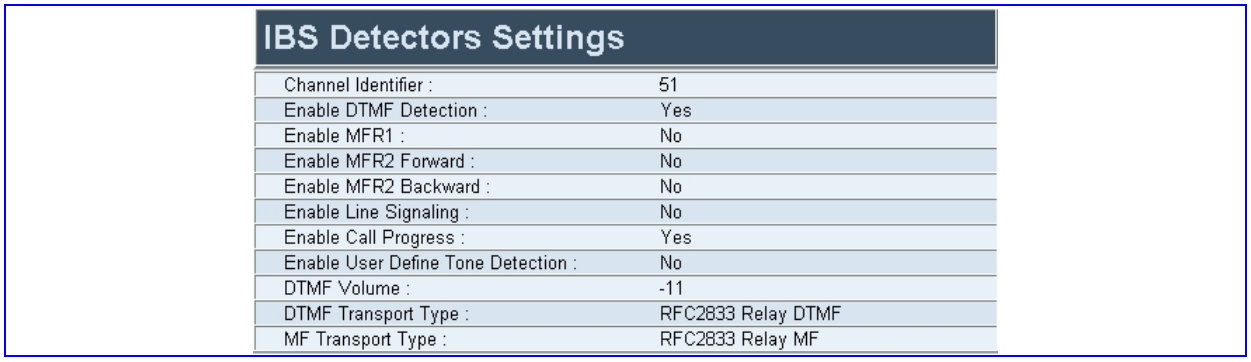
Figure 8-42: Voice Settings Screen



Voice Settings

Channel Identifier :	51
Coder :	G723High (16)
ECE :	Yes
SCE :	No
PFE :	Yes
HPFE :	Yes
Test Mode :	NoLoopback
VoiceVolume :	0
Input Gain :	0
M :	1
RTP Redundancy Depth :	0
EC Length :	0
EC Hybrid Loss :	0

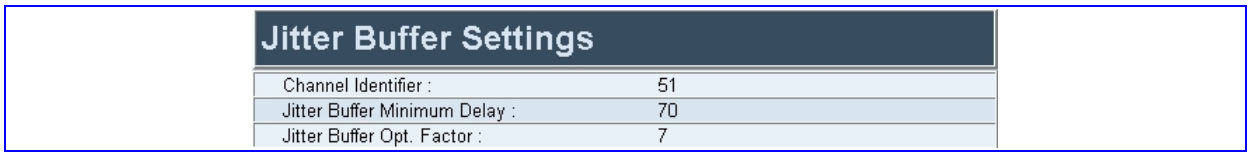
Figure 8-43: IBS Detector Settings Screen



IBS Detectors Settings

Channel Identifier :	51
Enable DTMF Detection :	Yes
Enable MFR1 :	No
Enable MFR2 Forward :	No
Enable MFR2 Backward :	No
Enable Line Signaling :	No
Enable Call Progress :	Yes
Enable User Define Tone Detection :	No
DTMF Volume :	-11
DTMF Transport Type :	RFC2833 Relay DTMF
MF Transport Type :	RFC2833 Relay MF

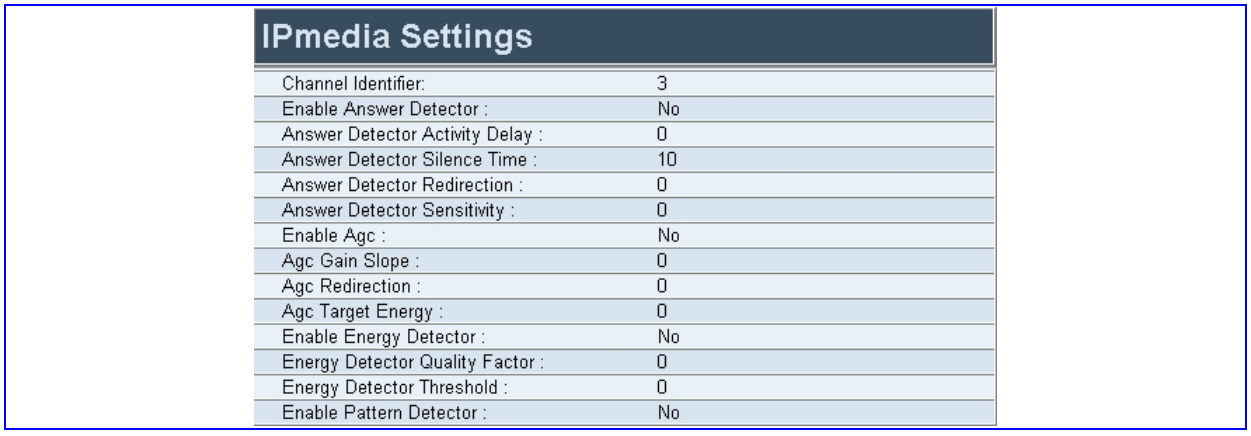
Figure 8-44: Jitter Buffer Settings Screen



Jitter Buffer Settings

Channel Identifier :	51
Jitter Buffer Minimum Delay :	70
Jitter Buffer Opt. Factor :	7

Figure 8-45: IPmedia Settings Screen



IPmedia Settings

Channel Identifier:	3
Enable Answer Detector :	No
Answer Detector Activity Delay :	0
Answer Detector Silence Time :	10
Answer Detector Redirection :	0
Answer Detector Sensitivity :	0
Enable Agc :	No
Agc Gain Slope :	0
Agc Redirection :	0
Agc Target Energy :	0
Enable Energy Detector :	No
Energy Detector Quality Factor :	0
Energy Detector Threshold :	0
Enable Pattern Detector :	No

8.4.5.2 Message Log

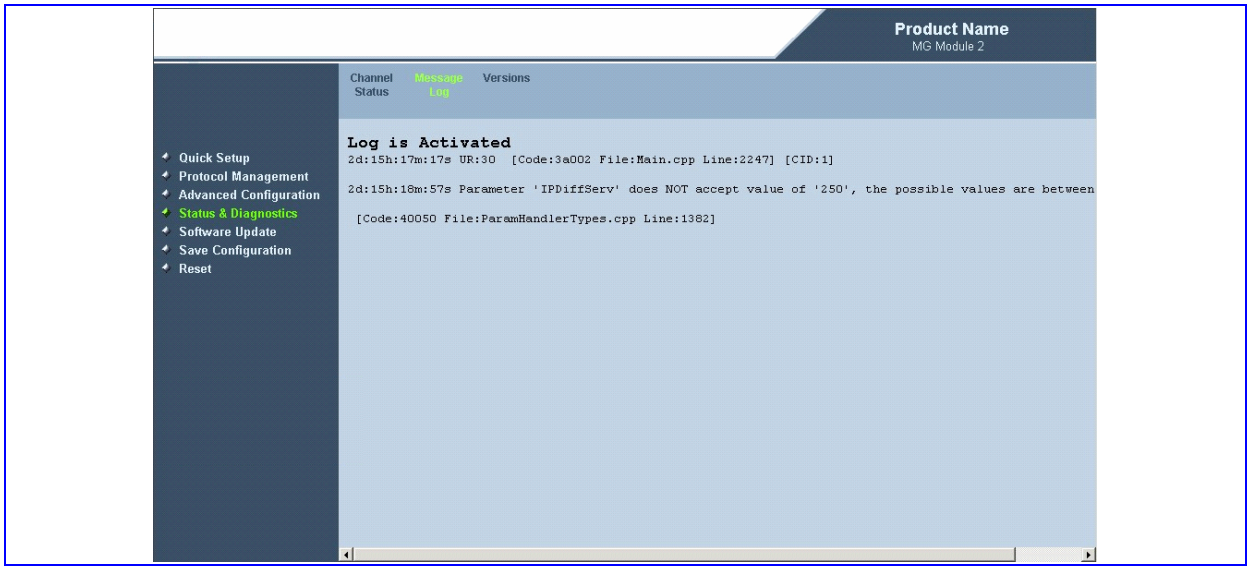
The Message Log is similar to a Syslog. It provides debug messages useful in pursuing troubleshooting issues.

The Message Log serves the Web Server and is similar to a Syslog server. It displays debug messages. It is not recommend to use the Message Log screen for logging errors and warnings because errors can appear over a prolonged period of time, e.g., a device can display an error after running for a week. Similarly, It is not recommend to keep a Message Log session open for a prolonged period (refer to the Note below). For logging of errors and warnings, refer to "Syslog" on page 209.

➢ To activate the Message Log, take these 4 steps:

1. From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears and Log is activated.
2. From the sub-menu bar on the top, click the **Message Log** link. The Message Log screen appears.

Figure 8-46: Message Log Screen



3. After receiving messages - Using the scroll bar, select the messages, copy them and paste them into a text editor such as Notepad. Send this *txt* file to Technical Support for diagnosis and troubleshooting as needed.
4. To clear the screen of messages, click on the sub-menu Message Log. The screen is cleared. A new session is activated and new messages begin appearing.

Note: Do not keep the Message Log screen activated and minimized for a prolonged period as a long session may cause the PC workstation to overload. While the screen is open (even if minimized), a session is in progress and messages are sent. Closing the window or moving to another link stops the messages and terminates the session.

8.4.5.3 Device Information

The Device Information screen displays hardware, software product information and Device state information.

Note: This information can help you to expedite any troubleshooting process. When required, capture a screenshot of the Device Information screen and email it to Technical Support personnel to ensure quick diagnosis and effective corrective action.

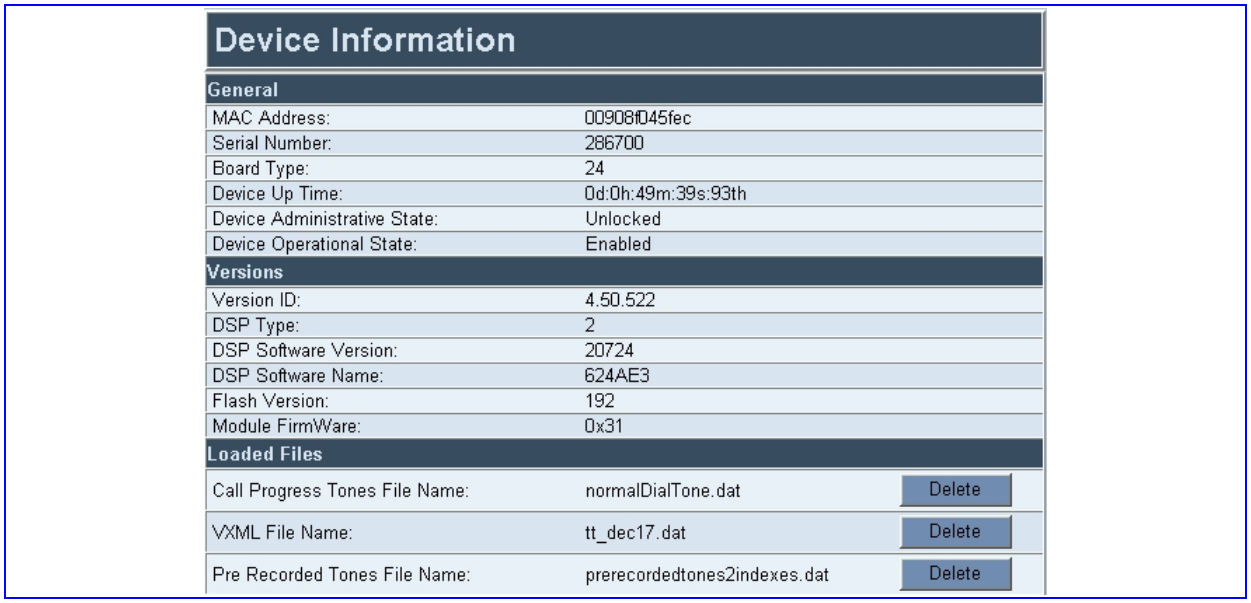
.

The screen also displays any loaded files in the device.

➢ To display the Device Information screen, take these 2 steps:

1. From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears.
2. From the sub-menu bar on the top, click the **Device Information** link (Note: on older version, it is the **Versions** link). The Device Information screen appears.

Figure 8-47: Device Information Screen



➢ To delete any loaded files, take these 5 steps:

1. From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears.
2. From the sub-menu bar on the top, click the **Device Information** link. The Device Information screen appears.
3. In the Device Information table, click the **Delete** button. The file deletion takes effect only after a device reset is performed.
4. In main menu to the left, click the **Reset** link. The Reset screen appears.
5. Select the **Burn** option and click the **Reset** button to restart the device with the new settings. (Refer to "Reset Button" on page 205.)

8.4.6 Software Update

The Software Update screen offers two options for downloading current software update files: the Software Upgrade Wizard and Load Auxiliary Files screen.

In addition, the Software Upgrade Key screen is provided for users to enter their updated Software Upgrade keys.

- Software Upgrade Wizard - Refer to ‘Software Upgrade Wizard’ on page 190
- Load Auxiliary Files - Refer to ‘Auxiliary Files Download’ on page 199
- Software Upgrade Key - Refer to ‘Software Upgrade Key’ on page 200

8.4.6.1 Software Upgrade Wizard

The Software Upgrade Wizard allows the user to upgrade the MG 3200's software by loading a new **.cmp* file together with the *ini* and a full suite of auxiliary files.

Loading a **.cmp* file is mandatory in the Software Upgrade Wizard process. During the process, users can choose to load the *ini* and the auxiliary files but this option cannot be pursued without loading the *cmp* file. For the *ini* and each auxiliary file type, you can choose between reloading an existing file, loading a new file or not loading a file at all.

8.4.6.1.1 Pre-Checks

Users or Upgrade engineer(s) performing upgrade for their customers should perform the following tasks in advance prior to Upgrade:

- Back up the current device configuration. Refer to 8.5 Restoring and Backing Up the Device Configuration, for procedure of backing up the *ini* file.
- Back up the existing Software Upgrade Key. Note that the Software Upgrade Key does not get erased or replaced through the Upgrade process, however for extra assurance, it is recommended this step is taken to ensure the data is saved. Refer to 8.4.6.3 Software Upgrade Key and follow the procedure described in "Backing up the current Software Upgrade Key".
- Save a screenshot of the Device Information screen. Again, the data on the Device Information screen should not be affected by the Upgrade process, however for extra assurance, it is recommended this step is taken. Refer to 8.4.5.3 Device Information for instructions on how to display the Device Information screen.
- Determine (or find out from your customers as applicable) whether the existing *ini* file is to be used or loading of a newer customized *ini* file provided by customer is required.

  (Note: The ini file from the CD is the default *ini* file which remains unchanged since SN07 release. This default *ini* file should only be used for new install. For upgrade, the existing *ini* file which is currently being used in the system is to be re-used. The Software Upgrade Wizard will guide you through how to load the ini file).
- Likewise, determine (or find out from your customers as applicable) which auxiliary files are required, whether the existing ones are to be used, or loading of newer customized files provided by customer are required.

  (Note: If customer has no specific request to use new files then assume to use the existing files which are the ones that are currently being used in the system. The Software Upgrade Wizard will guide you through how to load the auxiliary files).
- The Software Upgrade Wizard allows user to load the .cmp file from CD or located on user’s PC where the MG3200 Web GUI is launched. If the latter method is used, the .cmp file should be placed (e.g. via ftp or any other applicable method) onto a folder on user’s PC.
- Should any **new** *ini* and/or auxiliary files be required, they should also be placed on user’s PC in the same manner described above for .cmp file. (Note: This is not applicable if existing *ini* and auxiliary files are to be re-used).

Special Note for CAS file: For release prior to 5.0, it is recommended to always use a unique filename when downloading CAS files to the MG3200 gateway. For example, alter the filename by including a unique release identifier, date time string, or other meaningful text. Failure to do so will result in difficulty managing the CAS files due to having several entries with the same name in the CAS file selection box which may or may not be functionally identical. For this reason, for the case if a new CAS file is to be loaded during the software upgrade, ensure to rename the file after placing it on user's PC. (Note: This is not applicable if existing CAS file is to be re-used).

Refer to Table 6-4 for a description of the *ini* file and auxiliary files.

8.4.6.1.2 Software Upgrade Wizard Guided Procedure

➢ **To use the Software Upgrade Wizard take the following steps:**

Note: The Software Upgrade Wizard requires the device to be reset at the end of the process, which disrupts any existing traffic on the device. To avoid disrupting traffic, disable all traffic on the device before initiating the Software Upgrade Wizard. Traffic should be disabled/diverted off the MG 3200 from the Call Server side by the customer. Refer to Appendix – Disable MG 3200 Traffic Prior to Software Upgrade on page 405.

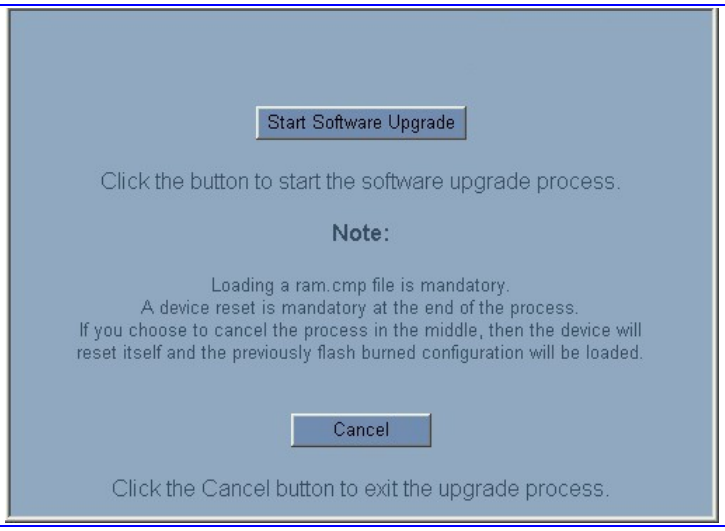
Note: It is recommended to perform the upgrade when low call traffic is known to occur.

1. Stop all traffic on the device (refer to the note above.)
2. From the main menu list on the left, click on the **Software Update** link. The Software Upgrade screen with the sub-menu bar on the top is displayed. (Figure 8-48)

Figure 8-48: Software Upgrade Screen

3. On the sub-menu bar on the top, click the **Software Upgrade Wizard** link. The Start Software Upgrade screen appears. (Figure 8-49)

Figure 8-49: Start Software Upgrade Screen

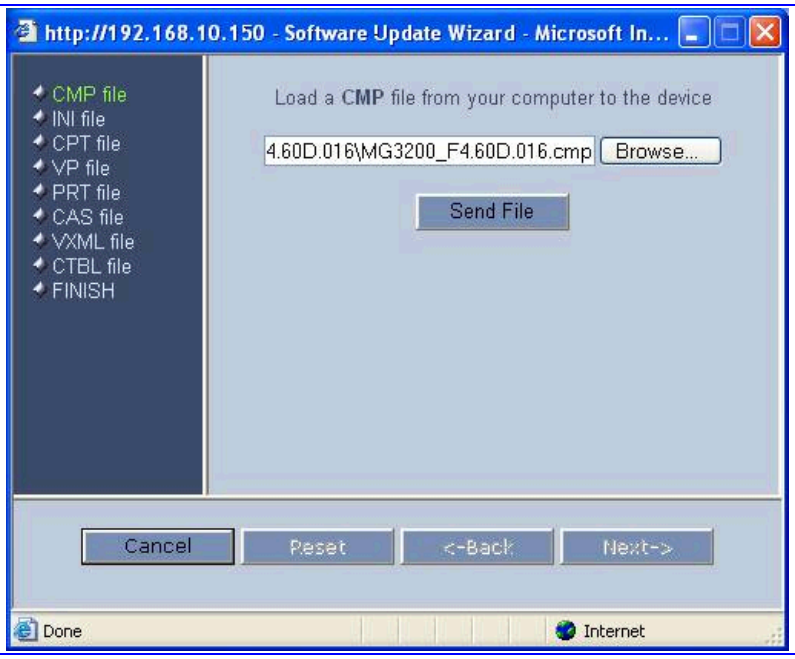


Note: At this point you may cancel the Software Upgrade process with no consequence to the device by using the cancel button. If you continue with the Software Upgrade process by clicking the **Start Software Upgrade** button, the process must be followed through and completed with a device reset at the end of the process. If you use the **Cancel** button, in any of the subsequent screens, the Software Upgrade process causes the device to be reset.

4. Click the **Start Software Upgrade** button to initiate the upgrade process. The 'Load a CMP file' appears. (Figure 8-50).

Note: When in the Wizard process, the rest of the Web application is unavailable and the background Web screen is disabled. After the process is completed, access to the full Web application is restored.

Figure 8-50: Load CMP File Screen



Note the file type list in the left side of the screen. This list contains the relevant file types that can be loaded via the wizard for this device type. The highlighted file type in the file type list indicates which file type is being displayed in the main part of the screen. As you continue through the Software Upgrade process by clicking on the **Next** button, each of the relevant file type screens are presented, going down the list until the Finish screen appears.

Note: The file type list may not be the same release after release. It may contain additional new file types in newer releases.

Note: The **Next** button is disabled until you load a **.cmp* file. After a **.cmp* file is selected, the wizard upgrade process continues and the Next button is enabled.

5. Click the **Browse** button and navigate to the location of the **.cmp* file to be loaded. The path and file name appears in the field.

6. Click the **Send File** button to send the file to the device. The File Loading screen appears with a progress bar indicating the loading period (Figure 8-51). When the loading is complete, a message is displayed indicated the file was successfully loaded into the device. (Figure 8-52)

Figure 8-51: File Loading Screen

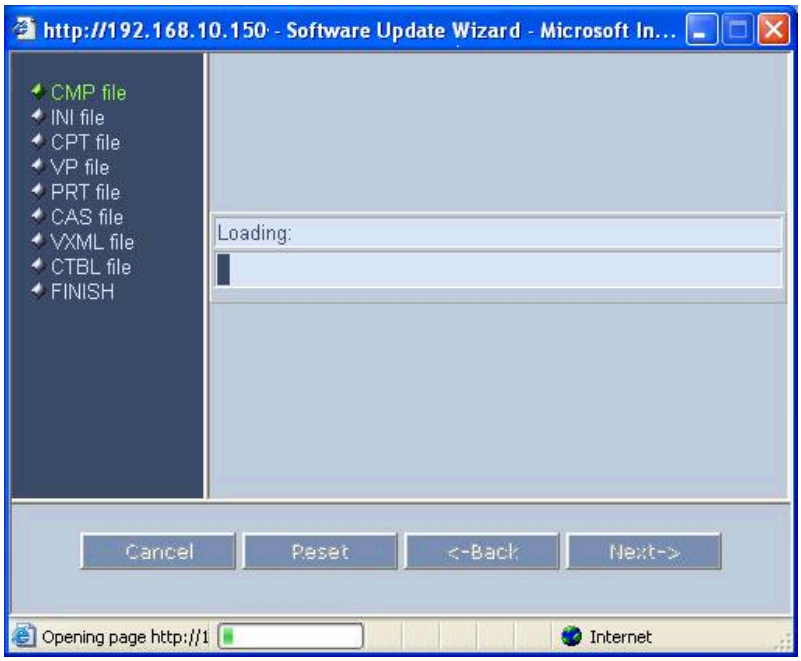
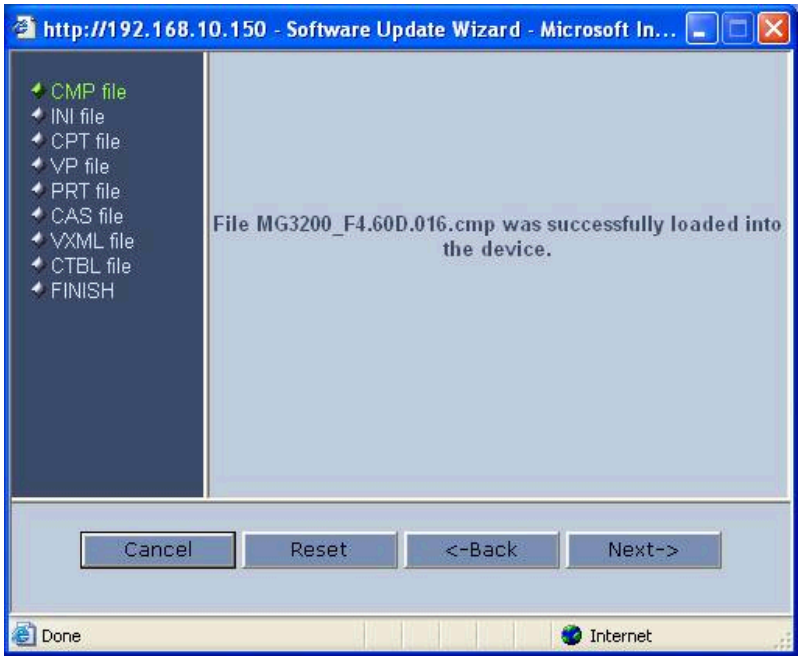


Figure 8-52: *cmp* file successfully loaded Notification Screen



All four buttons (**Cancel**, **Reset**, **Back**, and **Next**) in the bottom portion of the screen are now activated.

7. You may choose between these options:

- Loading the *ini* file and/or additional Auxiliary Files
- Completing the Software Upgrade Process

- Cancel Upgrade Process and revert to the Previous Configuration Files

8. Loading *ini* file and/or additional Auxiliary Files

To move to the next file type on the list to the left, click the **Next** button. The File Loading screen appears with the next relevant file type highlighted.

For each file type the user has three options:

- Load a new file to the device using the Browse and Send File button as described above. (Note: By clicking the 'Browse' button, the checkbox 'Use existing configuration', checked by default, becomes unchecked.)
- Load the existing file - The checkbox 'Use existing configuration' (checked by default as shown in the figures below) appears if relevant to the device. If this checkbox is checked, the existing file is used in the upgraded system. (Note: If this option is chosen, ignore the 'Browse' and 'Send File' button, just ensure the checkbox is checked)
- Avoid loading any file at all - Clear (ie. Uncheck) the checkbox (if the checkbox appears). (Note: If this option is selected for the *ini* file, the MG 3200 uses its factory-preconfigured values).

Continue through each of the file type screens by clicking **Next** and selecting one of the above options.

As an example, the figures below display the File Loading screen of the *ini* file and CPT file.

Figure 8-53: File Loading Screen - *INI* file

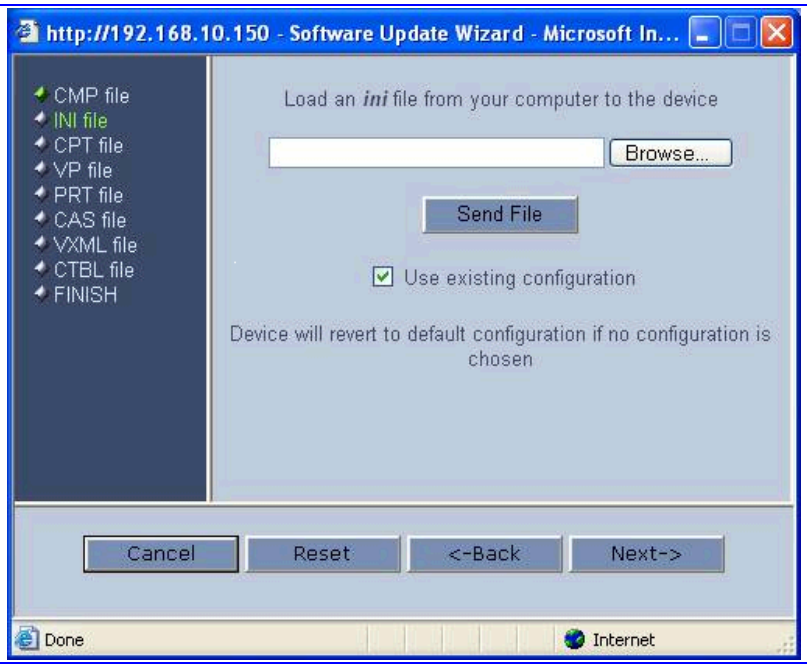
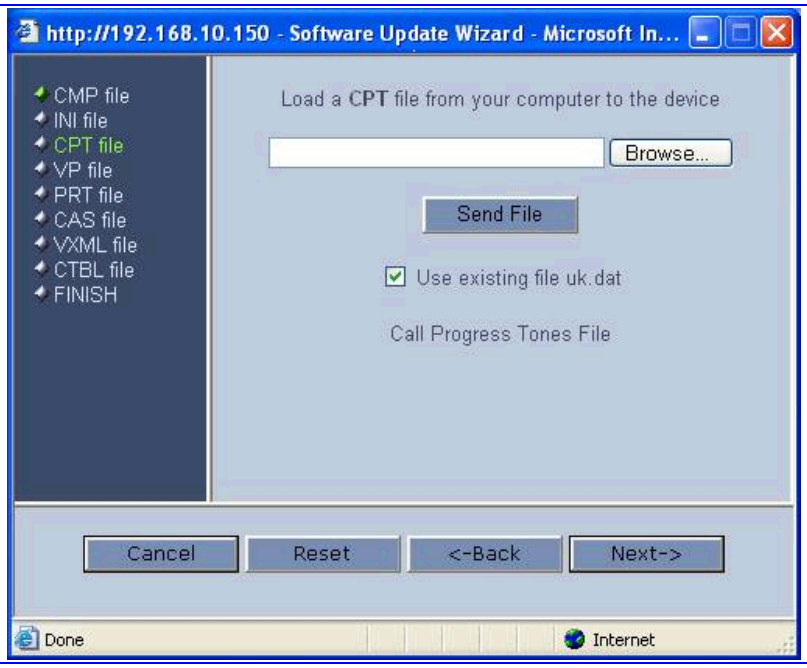


Figure 8-54: File Loading Screen – CPT file



From any of the file type screens, you can choose to complete the Software Upgrade Process (Refer to Step 9 **Completing the Software Upgrade Process**) or cancel the Upgrade to revert back to the previous configuration (Refer to Step 10 **Revert to the Previous Configuration Files**).

9. Completing the Software Upgrade Process

From any of the file type screens, you can complete the Software Upgrade process by clicking the **Reset** button. The device is reset utilizing the new files you have loaded **up to that point**, as well as using the existing files according to the checkbox status of each file type.

10. Revert to the Previous Configuration Files

From any of the file type screens, you can revert to the previous configuration by clicking the **Cancel** button. The Software Upgrade process is terminated and the device is reset utilizing the previous flash burned configuration.

11. When continuing through the Software Upgrade process, you complete the process from the Finish screen (Figure 8-59) by clicking the **Reset** button (the **Next** button is disabled). (Figure 8-60)

Figure 8-55: FINISH Screen

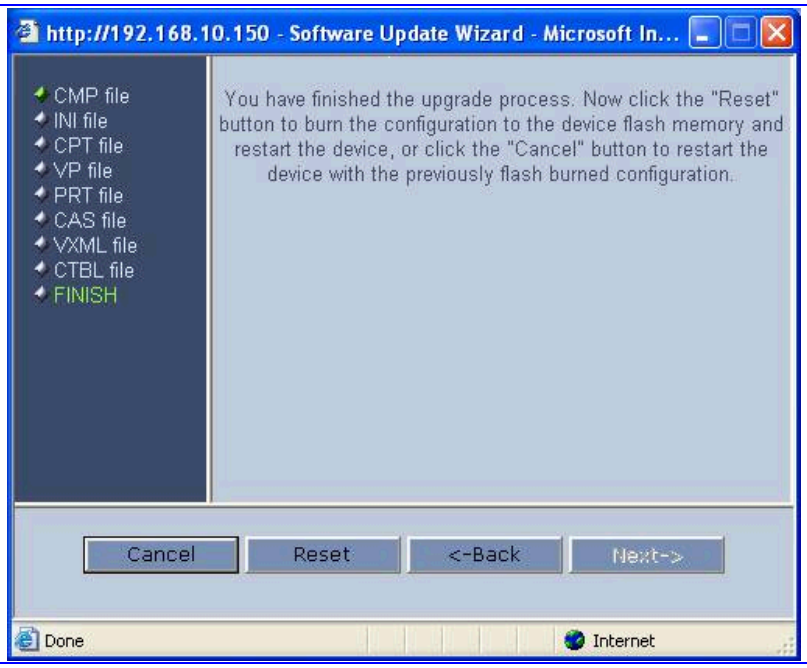
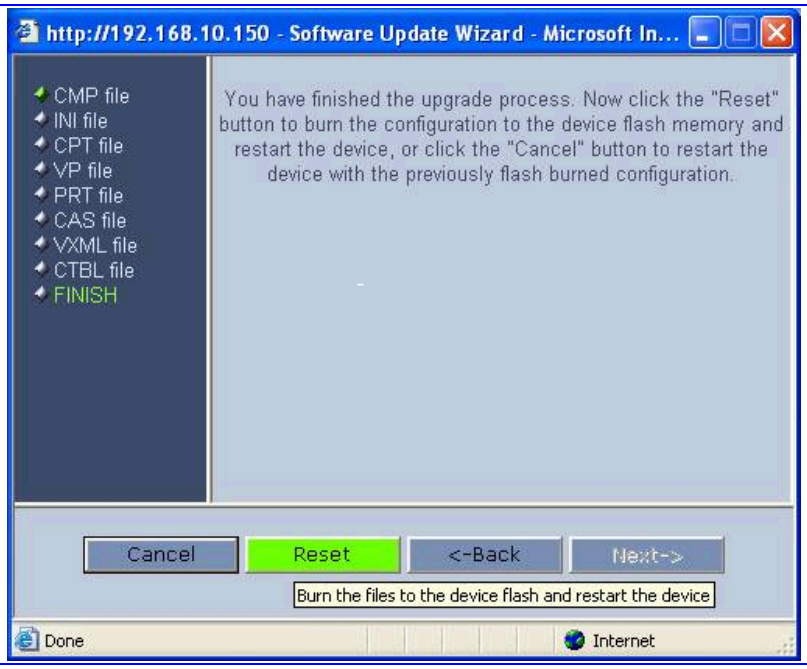


Figure 8-56: FINISH Screen - Reset



During the Reset process, the device 'burns' the newly loaded configuration to the non-volatile memory. The File Burning screen appears displaying the File Burning to Flash Memory progress bar (Figure 8-57). When this is completed, the End Process screen appears displaying the current configuration information. (Figure 8-58)

Figure 8-57: File Burning Screen

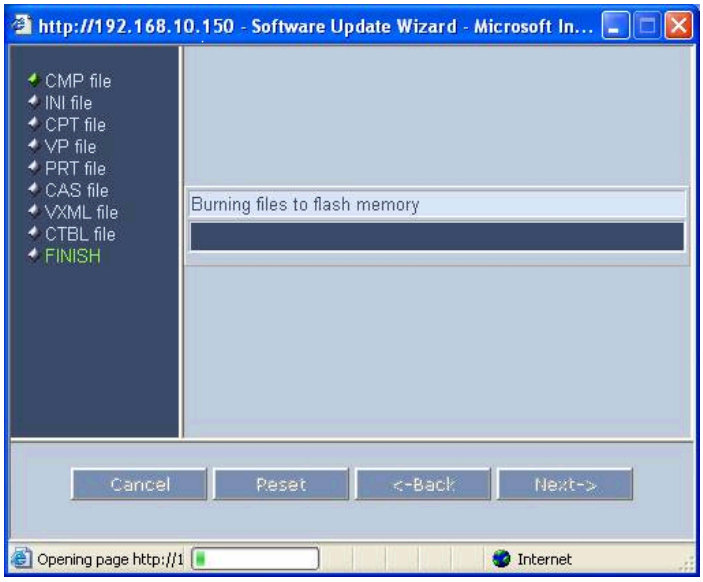
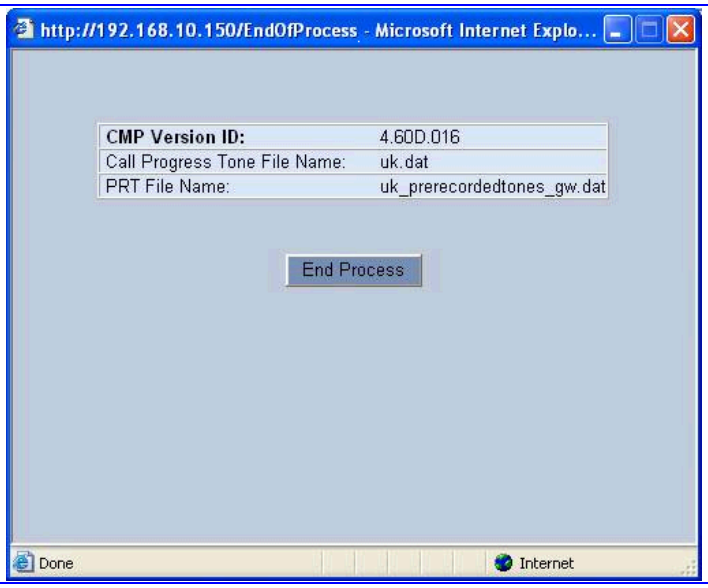


Figure 8-58: End Process Screen



12. Click the **End Process** button. A window indicating the device is now loaded with the new load. Click **OK**. The Quick Setup screen appears and the full Web application is reactivated.

The software upgrade process is now completed.

Note: Ensure to enable the traffic after Upgrade is complete. Refer to Appendix – Resume MG 3200 Traffic after Software Upgrade is Completed on page 409.

8.4.6.2 Auxiliary Files Download

The Auxiliary Files Download screen facilitates the download of software updates using the HTTP protocol. Types of software file updates include:

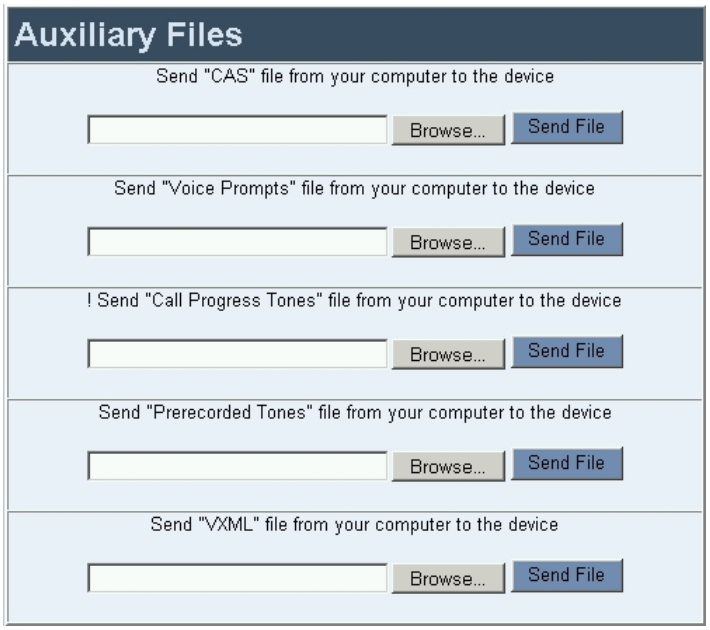
- Voice Prompt - The *dat* Voice Prompts file is played by the device during the phone conversation on Call Agent request. Download if you have an application requiring Voice Prompts.
- Call Progress Tone - *usa_tones.dat* - This is a region-specific, telephone exchange-dependent file. Call Progress Tones provide call status/call progress to customers, operators, and connected equipment. Default Tones: U.S.A. *usa_tones.ini* - The *ini* file is the value of the different Call Progress Tones files (frequency, cadence, etc.). To convert the *usa_tones.ini* file, which is a *txt* file, to a usa_*tones.dat* file that can be downloaded into the MG 3200, use the Call Progress Tones file generator utility *TPDMUtil.exe*.
- Prerecorded Tones - The *.dat PRT file enhances the devices capabilities to play a wide range of telephone exchange tones.
- CAS - *cas.dat* includes E1/T1 CAS signaling files, such as *E_M_WinkTable.dat*, These files are not needed for ISDN protocols.

➢ To download an auxiliary file, take these 5 steps:

1. From the main menu list on the left, click on the **Software Download** link. The Software Download screen is displayed.

2. From the sub-menu bar on the top, click the **Auxiliary Files Download** link. The Auxiliary Files Download screen appears.

Figure 8-59: Auxiliary Files Download Screen



3. Use the **Browse** button to locate the appropriate file on your PC.
4. Click the **Send File** button. The files are sent to the MG 3200.
5. To commit the changes to the non-volatile (flash) memory, in the main menu on the left, click the **Save Configuration** link. In the **Save Configuration** screen that appears, click the **Save Configuration** button. The changes are committed to the non-volatile memory.

Note: For release prior to 5.0, it is recommended to always use a unique filename when downloading CAS files to the MG3200 gateway. For example, alter the filename by including a unique release identifier, date time string, or other meaningful text. Failure to do so will result in difficulty managing the CAS files due to having several entries with the same name in the CAS file selection box which may or may not be functionally identical.

Note: A device reset is required to activate a loaded *CPT* file, and may be required for the activation of certain *ini* file parameters. The **Burn** option must be selected. (Refer to "Reset Button" on page 205.)

8.4.6.3 Software Upgrade Key

8.4.6.3.1 About the Software Upgrade Key

MG 3200s are loaded with a Software Upgrade Key already pre-configured for each of its TrunkPack Modules (TPM).

Users can later upgrade their MG 3200 features, capabilities and quantity of available resources by specifying what upgrades they require and the corresponding TPM's serial number (or MAC address), and ordering a new key to match their specification.

The Software Upgrade Key is sent as a string in a text file, to be loaded into the MG 3200. Stored in the MG 3200's non-volatile flash memory, the string defines the features and capabilities allowed by the specific key purchased by the user. The MG 3200 allows users to utilize *only these* features and capabilities. A new key overwrites a previously installed key.

Note: The Software Upgrade Key is an encrypted key. Each TPM utilizes a unique key. The Software Upgrade Key is provided by Nortel only.

8.4.6.3.2 Backing up the Current Software Upgrade Key

Back up your current Software Upgrade Key before loading a new key to the MG 3200. You can always reload this backed-up key to restore your MG 3200 capabilities to what they originally were if the 'new' key does not comply with your requirements.

➢ To backup the current Software Upgrade Key, take these 5 steps:

1. Launch the MG3200 Web GUI (for details on how to lauch the Web GUI, refer to "Accessing the Embedded Web Server" on page 144).
2. Click the **Software Update** button.
3. On the sub-menu bar on the top, click the **Software Upgrade Key** link (Note: on older version, it is the **License** link). The Software Upgrade Key screen is displayed (shown in the figure, 'Software Upgrade Key Screen' below).
4. Copy the string from the **Current Key** field and paste it in a new text file on your PC machine.
5. Save the text file with a name of your choosing in any folder on your PC, as long as you remember how to reaccess the data should it be needed later.

8.4.6.3.3 Loading the Software Upgrade Key

After receiving the Software Upgrade Key file (do not modify its contents in any way), ensure that its first line is [LicenseKeys] and that it contains one or more lines in the following format:

S/N<Serial Number of TPM> = <long Software Upgrade Key>

For example: S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj...

One S/N must match the S/N of your MG 3200 module (TPM). The MG 3200's S/N can be viewed in the Device Information screen (refer to "Device Information" on page 188).

You can load a Software Upgrade Key using:

- The Embedded Web Server (refer to "Loading the Software Upgrade Key Using the Embedded" below).
- The BootP/TFTP configuration utility (refer to "Loading the Software Upgrade Key Using BootP/TFTP" on page 83).
- The EMS (refer to the EMS User's Manual or EMS Product Description).

8.4.6.3.4 Loading the Software Upgrade Key Using the Embedded Web Server

➢ To load a Software Upgrade Key using the Web Server, take these 5 steps:

1. Access the MG 3200's Embedded Web Server (refer to “Accessing the Embedded Web Server” on page 144).
2. Click the **Software Update** button.
3. Click the **Software Upgrade Key** link; the Software Upgrade Key screen is displayed (shown in the figure, 'Software Upgrade Key Screen' below).
4. **When loading a single key S/N line to a MG 3200:**

   Open the Software Upgrade Key file (it should open in Notepad), select and copy the key string of the MG 3200’s S/N and paste it into the Web field **New Key**. If the string is sent in the body of an Email, copy and paste it from there. Press the **Add Key** button.
5. **When loading a Software Upgrade Key text file containing multiple S/N lines to a MG 3200:**

   (Refer to the figure, ''Example of a Software Upgrade Key File Containing Multiple S/N Lines'' on page 83)

   Click the **Browse** button in the **Send “Upgrade Key” file from your computer to the device** field, and navigate to the Software Upgrade Key text file.
   Click the **Send File** button.

The new key is loaded to the MG 3200, validated and if valid is burned to memory. The new key is displayed in the **Current Key** field.

Validate the new key by scrolling through the ‘Key features:’ panel and verifying the presence / absence of the appropriate features.

6. After verifying that the Software Upgrade Key was successfully loaded, reset the MG 3200; the new capabilities and resources are active.

Figure 8-60: Software Upgrade Key Screen

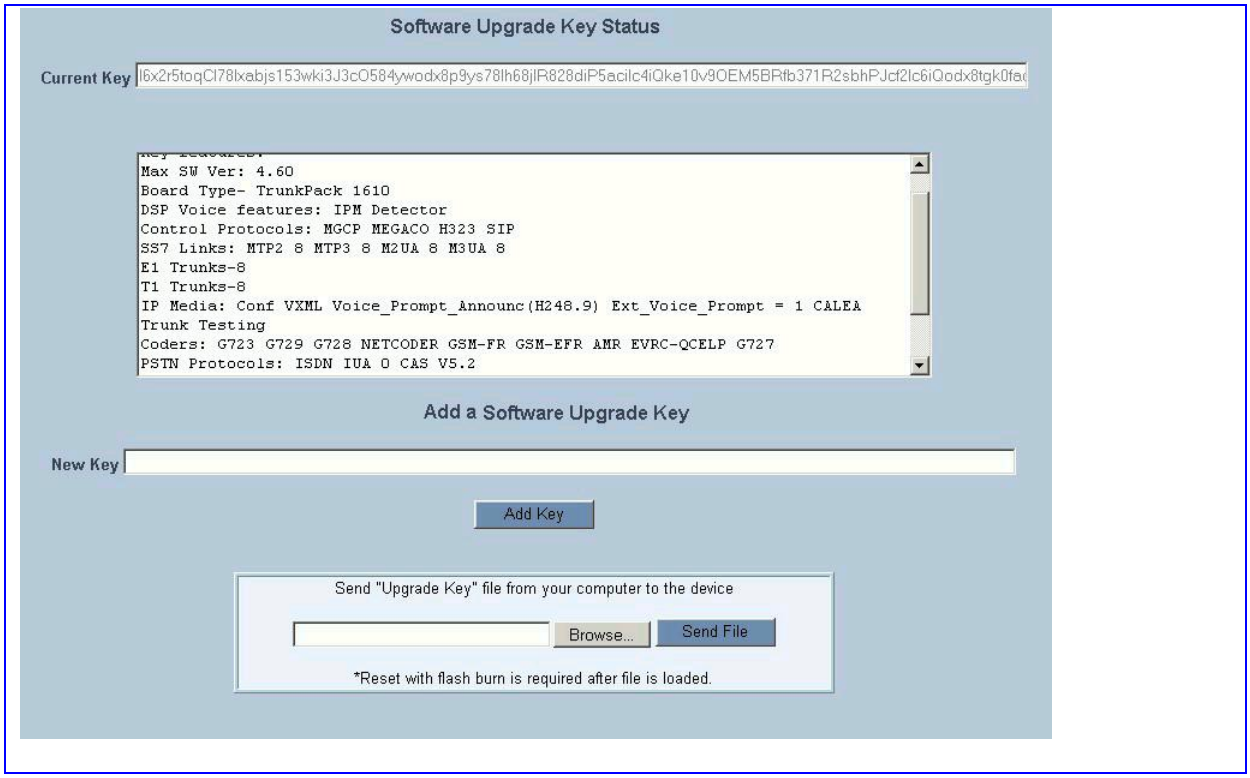
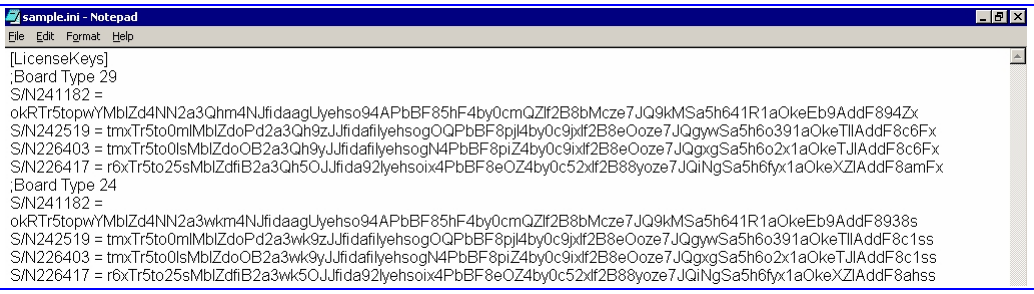


Figure 8-61: Example of a Software Upgrade Key File Containing Multiple S/N Lines



8.4.6.3.5 Loading the Software Upgrade Key Using BootP/TFTP

➢ **To load the Software Upgrade Key file using BootP/TFTP, take these 5 steps:**

1. Place the file in the same location you've saved the *MG 3200's cmp* file.
2. Start the BootP/TFTP configuration utility and from the **Services** menu in the main screen, choose option **Clients**; the Client Configuration screen is displayed (refer to the' 'Client Configuration Screen" on page 229).
3. From the drop-down list in the **INI File** field, select the Software Upgrade Key file instead of the MG 3200's *ini* file. Note that the MG 3200's *cmp* file must be specified in the **Boot File** field.

4. Configure the initial BootP/TFTP parameters required, and click **OK** (refer to the Appendix, "BootP/TFTP Server" on page 223).

5. Reset the MG 3200; the MG 3200's *cmp* and Software Upgrade Key files are loaded to the MG 3200.

8.4.6.3.6 Verifying that the Key was Successfully Loaded

After installing the key, you can determine in the Embedded Web Server's read-only 'Key features:' panel (**Software Update** menu > **Software Upgrade Key**) (refer to Figure H-1) that the features and capabilities activated by the installed string match those that were ordered.

You can also verify that the key was successfully loaded to the MG 3200 by accessing the Syslog server. For detailed information on the Syslog server, refer to "Syslog" on page 209. When a key is successfully loaded, the following message is issued in the Syslog server:

"S/N___ Key Was Updated. The Board Needs to be Reloaded with *ini* file\n"

8.4.6.3.7 Troubleshooting an Unsuccessful Loading of a Key

If the Syslog server indicates that a Software Upgrade Key file was unsuccessfully loaded (the SN_ line is blank), take the following preliminary actions to troubleshoot the issue:

- Open the Software Upgrade Key file and check that the S/N line of the specific MG 3200 whose key you want to update is listed in it. If it isn't, contact Nortel.
- Verify that you've loaded the correct file and that you haven't loaded the MG 3200's *ini* file or the CPT *ini* file by mistake. Open the file and ensure that the first line is [LicenseKeys].
- Verify that you did not alter in any way the contents of the file.

8.4.6.3.8 Abort Procedure

Reload the key you backed-up in "Backing up the Current Software Upgrade Key" on page 81 to restore your device capabilities to what they originally. To load the backed-up key use the procedure described in "Loading the Software Upgrade Key".

8.4.7 Save Configuration

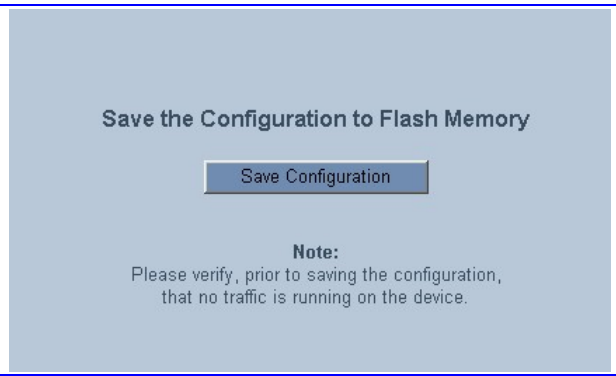
The Save Configuration screen allows users to save the current parameter configuration and the loaded files to the MG 3200's non-volatile (flash) memory.

Note: If you perform a reset with the **Burn** option selected *immediately* after making the changes to the configuration, there is no need to use the Save Configuration function prior to the reset.

➢ To use the Save Configuration screen, take these 2 steps:

1. From the main menu list on the left, click on the **Save Configuration** link. The Save Configuration screen is displayed.

Figure 8-62: Save Configuration Dialog Screen



2. Click the **Save Configuration** button. The new/modified configuration and any HTTP loaded files are saved to the non-volatile (flash) memory on the device. A message informing you that it has been saved appears.

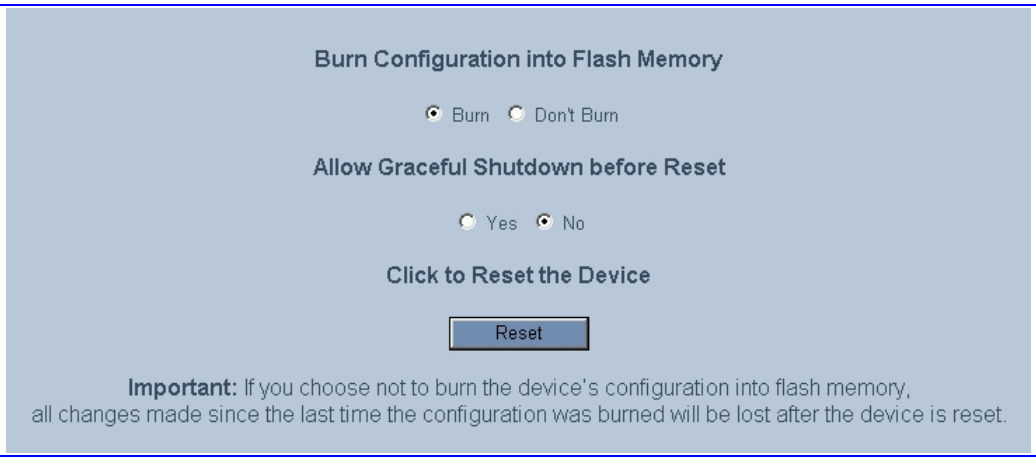
8.4.8 Reset Button

The **Reset** link in the main menu on the left allows the user to initiate a device reset following which the device utilizes the new configuration stored in the non-volatile (flash) memory.

➢ To use the Reset Button screen, take these 3 steps:

1. From the main menu list on the left, click on the **Reset** button. The Reset screen is displayed.

Figure 8-63: Reset Screen



2. Select either of the following Burn options:
   - **Burn** - (Default setting) burns the current configuration to non-volatile (flash) prior to reset
   - **Don't Burn** - Resets the device without first burning the current configuration to non-volatile (discards all modifications to the configuration that were not saved to non-volatile memory)
3. Select either of the following Graceful Shutdown options:
   - **Yes** - a **timer configuration input** field appears - Reset starts only after the timer expires or no more active traffic exists (the earliest thereof)
   - **No** - immediate reset, any existing traffic is terminated at once
4. Click the **Restart** Button. If Graceful shutdown was selected, the reset is delayed and a screen displaying the number of remaining calls and the timer count is displayed. If Graceful shutdown was not selected the reset starts immediately.

   When the reset initiates, If the **Burn** option is selected, all of the changes made to the configuration are saved to the non-volatile memory of the device. If the **Don't Burn** option is selected, all of the changes made to the configuration are discarded. The device is shut down and re-activated. A message about the waiting period is displayed. The screen is refreshed.

8.5 Restoring and Backing Up the Device Configuration

The 'Configuration File' screen enables you to restore (load a new *ini* file to the device) or to back up (make a copy of the *ini* file and store it in a directory on your PC) the current configuration the device is using.

Back up your configuration if you want to protect your device's programming. The backup *ini* file includes only those parameters that were modified and contain other than default values.

Restore your configuration if the device has been replaced or has lost its programming information, you can restore the device's configuration from a previous backup or from a newly created *ini* file. To restore the device's configuration from a previous backup you must have a backup of the device's information stored on your PC.

➢ To restore or back up the *ini* file, take this step:

- Open the 'Configuration File' screen (Advanced Configuration menu > Configuration File). The 'Configuration File' screen is displayed. (Refer to "Configuration File" on page 177.)

➢ To back up the *ini* file take these 4 steps:

1. Click the **Get INI FILE** button; the 'File Download' dialog opens.
2. Click the **Save** button. The 'Save As' dialog opens.
3. Navigate to the folder where you want to save the *ini* file.
4. Click the **Save** button. The VoIP gateway copies the *ini* file into the folder you selected.

➢ To restore the ini file take these 4 steps:

1. Click the **Browse** button.
2. Navigate to the folder that contains the *ini* file you want to load.
3. Click the file and click the **Open** button. The name and path of the file appear in the field beside the **Browse** button.
4. Click the **Send ini File** button, and click **OK** in the prompt. The gateway is automatically reset (from the *cmp* version stored on the flash memory).

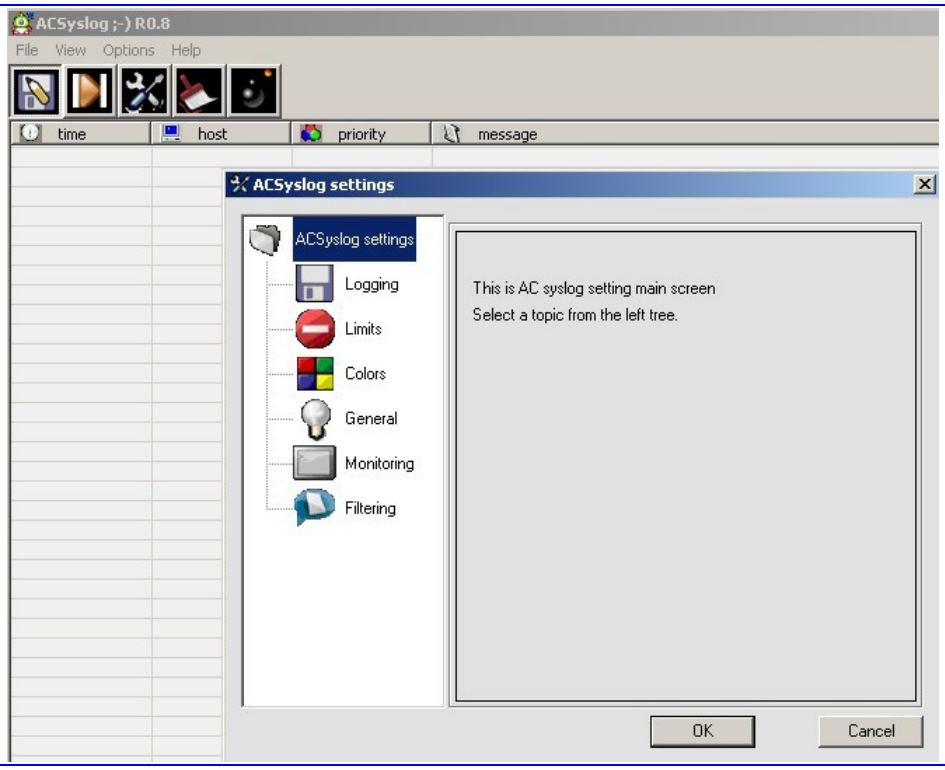
9 Diagnostics & Troubleshooting

9.1 Syslog

The Syslog server (refer to the figure below), now available with version 4.6, enables filtering of messages according to priority, IP sender address, time, date, etc. Customers can alternatively choose to download and use the following examples of the many Syslog servers available as shareware on the Internet:

- Kiwi Enterprises: http://www.kiwi-enterprises.com/software_downloads.htm
- The US CMS Server: http://uscms.fnal.gov/hanlon/uscms_server/
- TriAction Software: http://www.triaction.nl/Products/SyslogDaemon.asp
- Netal SL4NT 2.1 Syslog Daemon: http://www.netal.com

Figure 9-1: Syslog Server Main Settings Screen



Syslog protocol is an event notification protocol that allows a machine to send event notification messages across IP networks to event message collectors - also known as Syslog servers. Syslog protocol is defined in the IETF RFC 3164 standard.

Since each process, application and operating system was written independently, there is little uniformity to Syslog messages. For this reason, no assumption is made on the contents of the messages other than the minimum requirements of its priority.

Syslog uses User Datagram Protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to Syslog is 514.

The Syslog message is transmitted as an ASCII message. The message starts with a leading "<" ('less-than' character), followed by a number, which is followed by a ">" ('greater-than' character). This is optionally followed by a single ASCII space.

The number described above is known as the Priority and represents both the Facility and Severity as described below. The Priority number consists of one, two, or three decimal integers.

Example:

<37> Oct 11 16:00:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8

9.1.1 Operating the Syslog Server

9.1.1.1 Sending the Syslog Messages

The Syslog client, embedded in the firmware of the device, sends error reports/events generated by the device application to a Syslog server, using IP/UDP protocol.

There are presently five error levels reported by the Syslog client:

- Emergency level message:

<128>sctp socket setsockopt error 0xf0 [File:sctp.cpp Line:453]

- Warning level message

<132>Release contains no h.225 Reason neither q.931 Cause information stateMode:1 [File: Line:-1];

- Notice level message:

<133>(lgr_flow)(2546) | #0:ON_HOOK_EV

- Info level message:

<134>document http://ab.pisem.net/RadAAIP.txt was not found in documents table [File:vxml_handleDB.cpp Line:2348]

- Debug level message:

<135>SCTP port 2905 was initialized [File:csAPI.cpp Line:150] [CID:0]

9.1.1.2 Setting the Syslog Server IP Address

➢ To set the address of the Syslog server:

- Use the Embedded Web Server GUI (Advanced Configuration>Network Settings screen - section Logging Settings). (Refer to "Embedded Web Server" on page 141 and to the figure below)

Figure 9-2: Setting the Syslog Server IP Address

- Alternately, use the Embedded Web Server GUI or the BootP/TFTP Server to send the *ini* configuration file containing the address parameter SyslogServerIP to the device. Before sending the *ini* file to the device, specify the address parameter. For

detailed information on the BootP/TFTP Server, refer to the Appendix, "BootP/TFTP Server" on page 223. For an *ini* file example showing this parameter, refer to "Setting Syslog Server IP Address, Enabling Syslog, in an ini File" on page 211 and to the Example of Setting Syslog Server IP Address, Enabling Syslog, in an *ini* File below.

9.1.1.3 Activating the Syslog Client

➢ **To activate the Syslog client:**

- Use the Embedded Web Server GUI (Advanced Configuration>Network Settings screen - section Logging Settings). (Refer to "Accessing the Embedded Web Server" on page 144 and to the figure above.
- Alternately, use the Embedded Web Server GUI or the BootP/TFTP Server to send the *ini* configuration file containing the parameter EnableSyslog to the device. For detailed information on the BootP/TFTP Server, refer to the Appendix, "BootP/TFTP Server" on page 223. For an *ini* file example showing this parameter, refer to "Setting Syslog Server IP Address, Enabling Syslog, in an ini File" on page 211 and to the Example of Setting Syslog Server IP Address, Enabling Syslog, in an *ini* File below.

9.1.1.4 Setting Syslog Server IP Address, Enabling Syslog, in an *ini* File

The example below shows an *ini* file section with an example configuration for the address parameter SyslogServerIP and an example configuration for the client activation parameter EnableSyslog.

```
[Syslog]
SyslogServerIP=10.2.0.136
EnableSyslog =1
```

9.2 The Embedded Web Server's 'Message Log' (Integral Syslog)

The 'Message Log' screen in the Embedded Web Server GUI, similar to a Syslog server only integral to the web server, displays debug messages useful for debugging. For detailed information, refer to "Message Log" on page 187. The Message Log screen is not recommended for logging of errors and warnings because errors can appear over a prolonged period of time, e.g., a device can display an error after running for a week, and it is not recommended to prolong a 'Message Log' session. For logging of errors and warnings, refer to "Syslog" on page 209.

9.3 CommandShell - The Embedded CLI

An embedded Command Line Interface (CLI) is available for basic configuration and diagnostics. The CLI (or CommandShell) can be accessed via Telnet and the embedded Web server.

To enable Telnet access, set the parameter TelnetServerEnable to 1 or 2.

CLI commands are organized in folders. When first entering the CLI, the user is located at the root folder. The CLI lists the available commands and sub folders. Enter 'h' at the CommandShell prompt for help on the global commands. 'h <command name>' will provide help on a specific command.

The following CLI commands are available:

/CONFiguration folder:

SaveAndReset	Save all ini-file parameters to non-volatile memory, and reset the board
RestoreFactorySettings	Restore factory settings of all ini-file parameters
SetConfigParam	Set ini file parameters from the shell
GetParameterDescription	Display description of an ini-file parameter
GetConfigParam	Query ini file parameters from the shell
ConfigFile	Retrieve or set current configuration file via Telnet
AutoUPDate	Check for new ini/CMP files, configured in INIFILEURL and CMPFILEURL

/MGmt/FAult folder:

ListActive	List the currently active alarms
ListHistory	Show the alarm history table

/IPNetworking/Ping folder:

Ping	Ping a remote IP address
PingGetStat	Get the status of active ping sessions
PingStop	Stop active ping sessions

/TPApp folder:

BoardInfo	Display general information about the product
LoadVersion	Display the current SW version number
TimeOfDay	Display the system's date and time of day

/BSP/EXCeption folder:

ExceptionInfo	Display information on the last SW exception
PrintHistory	Display the SW exceptions history

9.4 Control Protocol Reports

9.4.1 H.248 Error Conditions

When working with H.248, the TP-1610 reports error conditions via the Call Manager (or via a Call Manager of the customer's choice) using the standard H.248 facilities, through the network interface. For more information on H.248 error conditions, refer to the IETF web site at URL http://www.ietf.org/rfc/ and refer to RFC RFC 3015 for H.248.

9.4.2 SNMP Traps

TP-1610 boards support various SNMP traps via the SNMP Agent running on the board. Among these traps are Trunk MIB traps, acBoardStarted and acResetingBoard traps. Refer to 'Using SNMP' on page 123 for more details on all SNMP traps available on the board.

9.5 TP-1610 Self-test

The TP-1610 features two self-testing modes: rapid and detailed.

- **Rapid self-test mode** - Used each time the TP-1610 completes the initialization process. This is a short test phase in which the only error detected and reported is failure in initializing hardware components. All Status and Error reports in this self-test phase are reported through the PCI interface and network interface ports.
- **Detailed self-test mode** - Used when initialization of the TP-1610 is completed and if the configuration parameter EnableDiagnostics is set to 1. (This parameter can be configured through the *ini* file mechanism or via PCI.) In this mode, the TP-1610 tests all the hardware components (memory, DSP, etc.) When EnableDiagnostics is set to **1**, flash is tested thoroughly, and when EnableDiagnostics is set to 2, flash is partially tested only. Test results are reported in the status output. The board sends EV_END_BIT containing information on the test results for each hardware component. To continue operational running, reset the board but this time with the EnableDiagnostics parameter set to **0**.

9.6 Solutions to Possible Problems

9.6.1 Possible Common Problems

Solutions to possible common problems are described in the table below.

Table 9-1: Solutions to Possible Common Problems

Problem	Possible Cause	Solutions
No communication	Software does not function in the device	Try to “ping” the board/module. If ping fails, check for network problems/definitions and try to reset the board/module
	Network problem	Check the cables.
	Network definitions	Check if the default gateway can reach the IP of the board/module.
		Check if the board/module got the correct IP.
		Check the validity of the IP address, subnet and default gateway. If the default gateway is not used, enter 0.0.0.0
	BootP did not reply to the board/module	Check if the BootP server replied to the board/module at restart by viewing the log of the BootP server.
		Try to restart the BootP server.
		Check the MAC address of the board/module in the BootP server.
ini **file was not loaded**	TFTP server down	Check if the TFTP server is working.
	TFTP server didn’t get the request	Check the log of the TFTP server.
	TP-1610 didn’t request the file from your TFTP	Check that the TFTP server’s IP address is the one that the TP-1610 is trying to use by viewing the Syslog.
	TFTP server bug	Try to restart the TFTP server.
	BootP sent to a board with the wrong TFTP server address	Check the IP address of the TFTP server being used.
	ini file does not exists in the default directory of the TFTP server	Check the default directory of the TFTP server and check that the *ini* file exists there.

Table 9-1: Solutions to Possible Common Problems

Problem	Possible Cause	Solutions
	Wrong *ini* file name	Verify in Windows Explorer that file extensions are displayed and the *ini* file is not *XXX.ini.ini* by mistake. Also verify that the extension *ini* is in lowercase letters.
	TFTP server's timeout is too short	Verify that the TFTP server settings are as follows: Timeout = 2 sec, # of retransmission = 10
Wrong *ini* file loaded	*ini* file is not in the correct position	An old *ini* file was probably loaded. Check which *ini* file was loaded by using the Syslog server. The Gateway displays contents of *ini* file before it began.
	ini file corrupted	Check the *ini* file syntax
BootP reply from wrong BootP server	Other BootP servers contain the MAC address of the board/module	Check that only your BootP server contains the TP-1610's MAC address.

9.6.2 Possible Voice Problems

Solutions to possible voice problems are described in the table below.

Table 9-2: Solutions to Possible Voice Problems

Problem	Possible Cause	Solutions
G.711 voice quality is bad (clicks)	Silence compression is not compatible (when working with different Gateway other than the MG 3200Gateway)	Disable it and check if the quality is better.
	The Packet size is not compatible (with G.711)	Check that the packet period in the remote side is 20 msec.
		Check that the correct μ-law or A-law compression is in use
No voice	There is no match in the codecs	Change the codec definition.

Reader's Notes

10 Functional Specifications

10.1 MG 3200 Selected Technical Specifications

The table below includes selected technical specification for both wireline application support.

Table 10-1: Selected Technical Specifications

Item	Characteristic
Channel Capacity	
Network Ports/DSP Calls (independent digital voice, fax or data ports)	Up to 480 All media processing ports can be tied to IP-RTP, PSTN-DS0 Time Slots independently
DSP Channel Configuration Options	60, 120, 240, 480 ports
Voice Messaging	
Playback from Local Storage	Prompts and announcements playback (10 MB integral memory for 20 min. of G.711 or 200 min. for G.723 recorded prompts)
Media Processing	
IP Transport	VoIP (RTP/ RTCP) per IETF RFC 1889 and RFC 1890
DTMF/MF Transport	DTMF/MF RTP Relay per RFC-2833, Mute, Transparent (transfer in coder as voice) DTMF Relay per I.366.2, Mute, transfer in coder as voice
Voice Processing	All voice processing features are supported simultaneously on all ports
	Dynamic Network Jitter Buffer with reordered RTP packets correction
	Call Progress Tones generation and detection
	Transcoding of a G.711 RTP stream to any Low Bit-Rate Coder RTP stream using one DSP channel resource
	Mediation between two IP endpoints of the same coder without using any DSP channel resource
	Media duplication (one source to many destinations) using the same coder without using additional DSP channel resources
Output Gain Control	Programmable: -31 dB to +31 dB in steps of 1 dB
Input Gain Control	Programmable: -31 dB to +31 dB in steps of 1 dB

Table 10-1: Selected Technical Specifications

Item	Characteristic
Voice Compression (Independent dynamic vocoder selection per channel)	G.711 PCM, 64 kbps (µ-law/A-law)
	G.726/G.727 ADPCM/E-ADPCM (16 to 40 kbps)
	G.723.1 MP-MLQ, 6.3 kbps ACELP, 5.3 kbps
	G.729A CS-ACELP, 8.0 kbps
	G.729 and G.723 should not be used simultaneously on the same board when using cellular coder templates
Silence Suppression	G.723.1 Annex A
	G.729 Annex B
Voice Activity Detection (VAD) Comfort Noise Generation (CNG)	PCM and ADPCM – Per RFC 3389 or Proprietary
Echo Cancellation	G.165 & G.168-2000 compliant 32, 64, 128 msec echo tail (64 and 128 may reduce channel capacity)
Fax and Modem Transport	
Fax Relay and Bypass	Supported on all ports
	Group 3 real-time Fax Relay to 14.4 kbps with auto fallback
	Tolerant of delays of up to 9 seconds
	T.30 (PSTN) and T. 38 (IP) compliant (real-time fax)
	CNG tone detection & Relay per T.38
	Automatic Fax ByPass to G.711 or ADPCM
Modem Bypass	Automatic switching to PCM or ADPCM for modem signals (V.34 or V.90 modem detection)
Signaling	
In-band/Out-of-band Signaling (DTMF & Tone Detection/Generation)	DTMF per TIA 464B
	DTMF over RTP per RFC 2833
	MFC-R2
	Packet side or PSTN side generation/detection of DTMF and User Defined Call Progress Tones (PSTN, IP) & Country Test Tones (per ITU-t Q.724)
CAS Relay	ABCD signaling over RTP per RFC 2833
SS7	MTP-2 and MTP-3 (ITU/ANSI/China) link termination
SigTran	IUA (RFC 3057) over SCTP (RFC 2960) M2UA, (RFC 3331) over SCTP (RFC 2960) transferring MTP-2 payload

Table 10-1: Selected Technical Specifications

Item	Characteristic
	(RFC 3332) over SCTP (RFC 2960) transferring MTP-3 payload
PSTN Protocols	CAS - T1 robbed bit: WinkStart, delay dial, immediate start, FGB, FGD, etc. MFC-R2 numerous country variants Unique script for each county variant, enabling maximum flexibility of the entire state machine of each CAS protocol.
	CCS - ISDN PRI: ETSI EURO ISDN, ANSI NI2, DMS, 5ESS, Japan INS1500, QSIG Basic Call, Australian Telecom, New Zealand Telecom, Hong Kong Variant, Korean MIC
Management Interfaces	
SNMP V2	Standard MIB-2, RTP MIB, Trunk MIB, the proprietary MIBs
Embedded Web Server	Enabling device configuration and run-time monitoring with an Internet browser
Firmware Download Options	
Firmware download	Remote TFTP or Web or via PCI
Boot option (for network control)	Locally from Flash or Remotely via BootP/DHCP and TFTP
Control Protocols	
H.248	Call control, CAS and R2 package, Basic announcements package, Conferencing
Processor	
Control Processor	Motorola PowerQUICC 8260
Control Processor Memory	SDRAM – 64 – 128 MB
Signal Processors	AC486 VoIP DSP based on: TI DSP TMS5541 – each core at 133 MHz
Interfaces	
Ethernet	Dual redundant 10/100 Base-TX ports RJ-45 connectors off rear I/O, PICMG 2.16 cPSB backplane for media streaming and call control. Half or Full duplex with auto-negotiation
PSTN	Either: Up to 16 E1 or 16 T1 spans via RTM rear panel I/O module two 50-Pin Telco connectors (DDK 57AE-40500-21D), each handling 8 E1/T1/J1 ports. Or: 1,2, 4 or 8 spans with RJ-48 shielded connectors

Table 10-1: Selected Technical Specifications

Item	Characteristic
Physical Characteristics	
Enclosure Dimensions	1U, 19-inch rack mount, shelf or desk top, 2-slot cPCI chassis 44.5 x 445 x 300 mm; 1.75 x 17.5 x 12 inch (h x w x d) 2 rear mounting flanges - Optional
Supply Voltages and Power Consumption (typical)	40.7 W, 3 A at 5 V, 7.8 A at 3.3 V 24 W, 1.5 A at 5 V, 5 A at 3.3 V (120 channels)
AC Power Supply	Universal 90 to 260 VAC 1A max, 47-63 Hz Option for a dual redundant power supply.
DC Power Supply	36 to 72 VDC (nominal 48 VDC), 4A max, floating input.
Environmental	Operational: 0° to 45° C 32° to 113° F (DC) Short Term (16 hour) 0° to 55° C / 32° to 131° F Storage: -10° to 70° C 14° to 158° F Humidity: 10 to 90% non-condensing
Hot Swap	Full hot swap supported boards Redundant Power Supplies provide protection but are non Hot Swappable
Host Interface	Via cPCI bus, using provided libraries
LED Indicators	
LED Indications on Front Panel	Power, Ready/Fail T1/E1/J1 per trunk status, LAN statusATM Interface status Swap ready indication
Connectors and Switches	
Rear Panel	Power: (model dependent) - Standard AC power socket or - DC power - MSTB2.5/2-STF (5.08mm) of Phoenix Contact E1/T1 Trunk and Ethernet connectors
Front Panel	Hardware Reset button
Type Approvals	
Telecommunication Standards (Chassis and hosted Telecom boards)	IC CS03, FCC part 68 CTR4, CTR12 , CTR13, JATE, TS.016, TSO, Anatel, Mexico Telecom
Safety and EMC Standards	UL 60950, FCC part 15 Class B, CE Mark (EN55022, EN60950, EN55024, EN300 386)

Table 10-1: Selected Technical Specifications

Item	Characteristic
Environmental	NEBS Level 3: GR-63-Core, GR-1089-Core, Type 1&3 (approved) For DC powered version Complies with ETS 300019-1, -2, -3 (T1.1, T2.3 & T3.2)
Diagnostics	
Front panel LEDs	Provide visual status indications and alarms
Syslog events	Supported by Syslog servers

Reader's Notes

11 Appendix - BootP/TFTP Server

11.1 Introduction

The **BootP/TFTP Server** enables easy configuration and provisioning MG 3200 Media Gateways. The BootP and TFTP servers contain specific adaptations as per manufacturer requirements. The latest version of the BootP/TFTP application is 2.3.0.5.

11.1.1 Key Features

- Internal BootP server supporting hundreds of entities
- Internal TFTP server
- Contains all required data for the MG 3200 in predefined format
- Provides a TFTP server address, enabling network separation of TFTP and BootP servers
- Tools to backup and restore the local database
- Templates
- User-defined names for each entity
- Option for changing MAC address
- Protection against entering faulty information
- Remote reset
- Unicast BootP respond
- User-initiated BootP respond, for remote provisioning over WAN
- Filtered display of BootP requests
- Location of other BootP servers that contain the same MAC entity
- Common log screen for both BootP and TFTP sessions
- Display of manufacturer vendor specific information parameters
- Support for manufacturer's selective BootP feature (The BootP server inserts manufacturer specific vendor information that includes the text, AUDC)
- Compatible with Windows™ 98, Windows™ NT, Windows™ 2000, Windows™XP

11.1.2 Specifications

- **BootP standards**: RFC 951 and RFC 1542
- **TFTP standards**: RFC 1350 and RFC 906
- **Operating System**: Windows 98, Windows NT and Windows 2000, Windows XP
- **Maximum number of MAC entries**: 200
- **BootP Fields:**
  - Hardware address (MAC): 12 hex digits
  - IP address
  - Subnet
  - Default Gateway
  - TFTP server IP (Using the TFTP server IP field enables download of firmware from a different Host)
  - Boot File
  - *ini* File
  - Call Agent IP
  - New MAC (optional)
- **Screens:**
  - File Upload and Message screen
  - Preferences screen
  - Client Configuration screen
  - Template Definition screen

11.1.3 BootP/TFTP Server Installation

The BootP/TFTP Server can be installed on a PC from the MG 3200 Software & Documentation CD.

➢ To install the BootP/TFTP Server, take these 3 steps:

1. Navigate to the BootP *zip* file under .\Utilities\.
2. Double click on the BootP *zip* file and run *setup.exe*. The installation procedure begins. After completing the procedure, open Start>Programs>BootP. **The BootP/TFTP Server** main screen is displayed.

   At first run, the user is requested to fill in the fields displayed on the Preferences screen.
3. To open the Preferences screen, from the main screen, select **Edit>Preference.** Follow the directions detailed in 'Preferences Screen' on page 228 to configure the screen.

11.1.4 Logging Screen

The BootP/TFTP Server main screen (refer to the figure, 'Main Screen' on page 227) includes the Log line, printed per BootP request with the following parameters:

- Hardware (MAC) address
- Status (found or not found in cache)
- Date and Time
- Assigned IP address (if found)
- Client name
- Client specific Information - contains vendor specific information, which includes: Board type, last IP, bootload version, flash *cmp* version, Analog type and number of analog channels. In order to access the board information, add -be 1 to the *ini* file selection in the BootP application. With this initial setting, even after deleting -be 1, the board continues to report its internal data.

Clicking a Log line displays all BootP reply parameters or enables entry to a new entity.

Right clicking a Log line opens up a menu.

Selecting **Reset** causes a soft reset of the board. Reset is available only for client MACs that are configured on the BootP server. The second option on the menu is View Client, which produces the same display as when clicking on the Log line.

11.1.5 Preferences Screen

The Preferences screen (refer to the figure, 'Preferences Screen' on page 228) is used to define BootP and TFTP configuration parameters:

- TFTP directory
- *ini* File Mask
- Boot File Mask
- TFTP timeout and number of retransmissions
- BootP replay type (Broadcast or Unicast)
- BootP ARP mode (dynamic or static)
- Number of initiated BootP replies (send after remote reset), optionally used when the MG 3200 is installed behind the firewall that blocks BootP broadcast requests.

11.1.6 Client Configuration Screen

The Client Configuration screen (refer to the figure, 'Client Configuration Screen' on page 229) shows:

- All client entities
- MAC
- Name
- IP per entity

With this screen, users can:

- Add a new entry
- Delete an existing entry
- Modify an existing entry
- Test a selected client for finding all BootP servers that respond to a BootP request with a specific MAC address

If a template is selected, any parameter can be entered manually or copied from the selected template by marking the checkbox to the right of the parameter. Usually, only an IP address is entered manually while other parameters are copied from the template.

11.1.7 Template Screen

The Template screen (refer to the figure, 'Templates screen' on page 231) enables the user to add, modify, or delete templates.

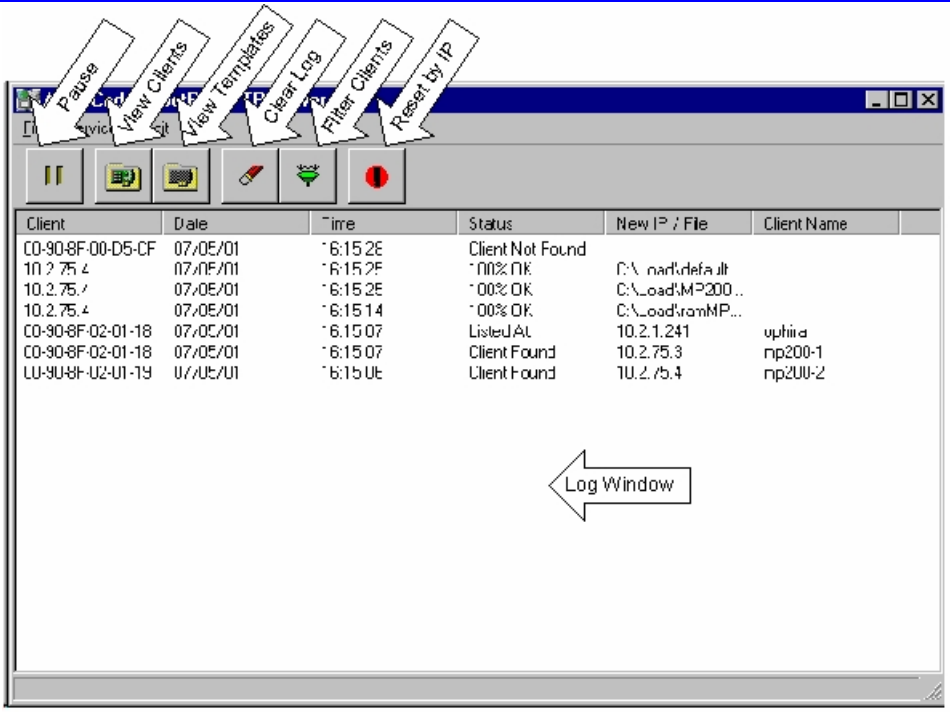
The template includes:

- Subnet
- Gateway, TFTP server
- BootFile
- *ini* file
- Call Agent fields
- Server IP

11.2 Screen Details

11.2.1 Main Screen

Figure 11-1: Main Screen



The figure above shows the main screen of the **BootP/TFTP Server**, featuring:

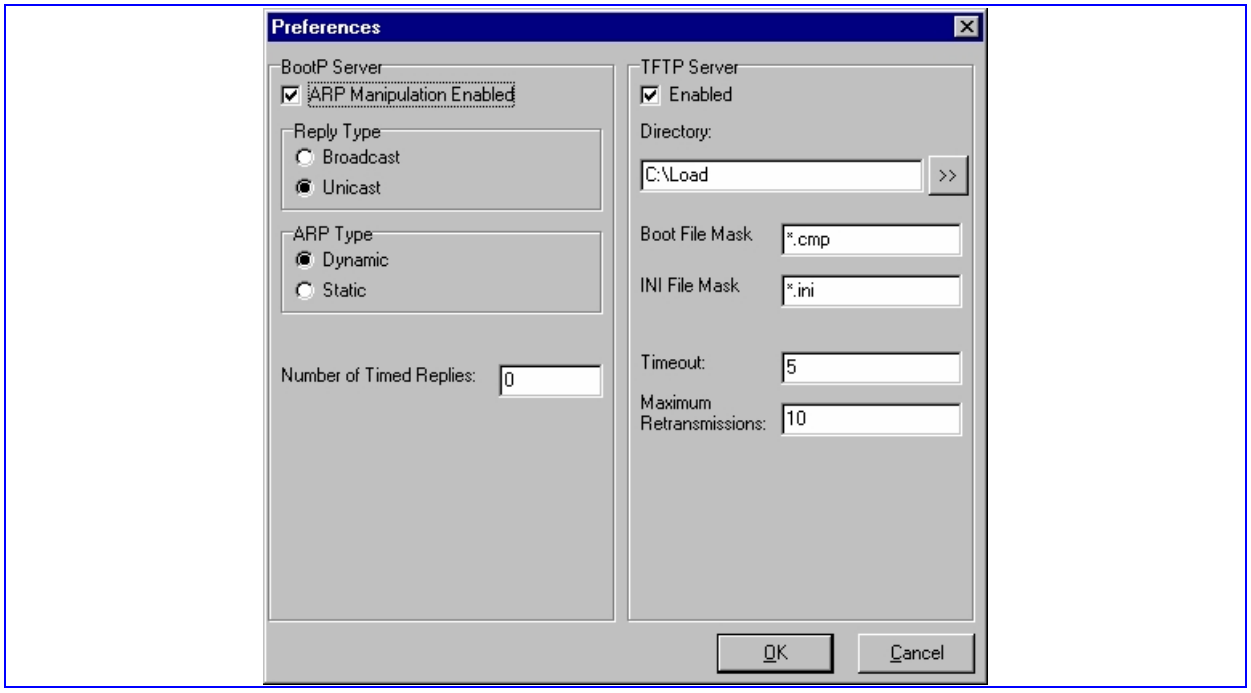
- **Program State -** Pauses the program. When the program is paused, no replies to BootP requests are sent.
- **View Clients button -** Opens up the Clients Configuration screen.
- **View Templates button -** Opens up the Templates Configuration screen.
- **Clear Log button -** Clears the log.
- **Filter Unknown Clients button -** Filters all BootP requests that are not listed in the Client Configuration screen.
- **Reset button -** Opens a dialog, in which users can enter an IP of a client. The program sends a reset command to that client.
- **Edit>Preferences -** Opens the Preferences screen for defining BootP and TFTP parameters.

- **Log Screen -** Displays all BootP requests and TFTP sessions, including the time and date of the request. In addition, the response type is also displayed:
  - Client Not Found
  - Client Found
  - Client's Mac Changed
  - Client Disabled
- **Listed at** (when using the Test Selected Clients button).
- For a TFTP session, file name and download status are displayed.
- **Pop-Up Menu -** Right-clicking on a line in the log screen displays the pop-up menu. In this menu there two options:
  - **Reset -** When this option is selected, the program searches the database for the selected MAC. When the client is found, the program adds the client's MAC to the ARP table, and then sends a reset command to the client. Note that by performing the remote reset this way, the user does not have to know the current IP address of the client. To perform this option, the user must have administrator privileges, otherwise an error message appears.
  - **View Client -** This option is the same as double-clicking on a line. When selected, the Clients Screen opens. If the Client's MAC is found in the database, it is focused. If not, a new client is added, with the MAC filled out. The remaining fields require fill in.

11.2.2 Preferences Screen

In the Preferences screen shown below, BootP and TFTP configuration parameters are defined.

Figure 11-2: Preferences Screen



In the BootP section, the user can select ARP mode: Dynamic or Static, and reply type: Broadcast or Unicast. For a typical application, use Dynamic ARP mode and Unicast, as shown above.

This option requires the **user to have administrator privileges** otherwise an error message appears**.** If you don't have administrator privileges**, uncheck** the ARP Manipulation Enabled checkbox in the Preferences Screen.

The **Number of Timed Replies** (the number of initiated timed BootP replies) can be used when the MG 3200 is installed behind a Firewall that blocks BootP broadcast requests. In a typical application, this feature can be disabled by entering **0** in this field. When selected, several BootP replies are sent to the MG 3200 immediately after the remote reset command.

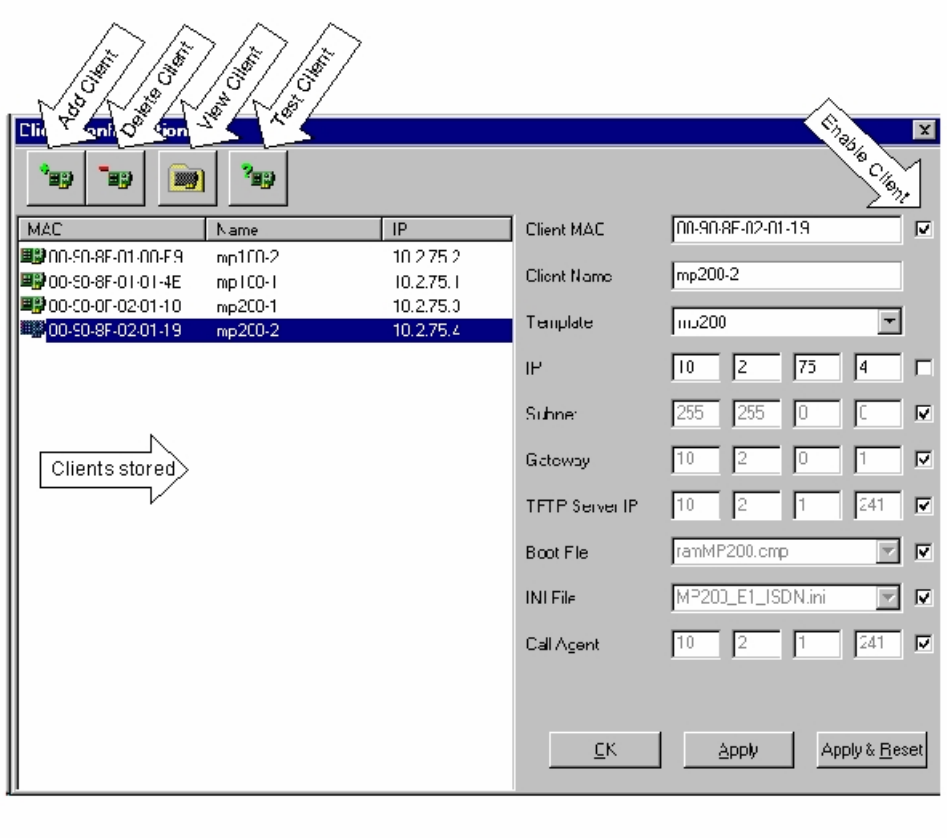
For the TFTP server, the user can configure a TFTP directory and a value for TFTP Timeout and Maximum Retransmissions. Set these values to **2** and **10** as shown above.

The TFTP server can be disabled by clearing the Enable checkbox.

11.2.3 Client Configuration Screen

The figure below is the Client Configuration Screen in which clients are added and defined.

Figure 11-3: Client Configuration Screen



In the left pane of the screen is the client list. By clicking on a client in this list, the following parameters for this client are displayed on the right side of the screen:

- **Client MAC -** This is the MAC address of the client. When the user edits the MAC, a new client is added, with the same parameters as the previous client. The client can be disabled by un-checking the check box on the right side of the Client MAC. This causes the BootP server not to reply to the BootP request. The client can be enabled by checking the check box. Click on the 'Apply' button each time the client enable check box is checked or unchecked.
- **Client Name -** A text field for entering the client description.
- **Template -** The template to be used for this client. When a template is selected, its parameters override all of the previous parameters.
- **IP, Subnet, Gateway -** Normal IP parameters.
- **TFTP Server IP -** The IP address of the TFTP Server.
- **Boot File,** *ini* **File -** The files to request from the TFTP server.

Note the seven check boxes to the right of the parameters. These enable the user to assign only the fields from the template, which have adjacent marked checkboxes. The rest can be unique for each client. When the field is assigned a value from the selected template, the field is grayed (and unmodifiable).

To save them after performing changes, click **Apply**. By clicking **Apply & Reset**, the program saves the changes to the database, performs a remote Reset to the client by adding the client's MAC to the ARP table, and then sends out a reset command. This option works **only if "ARP Manipulation Enabled"** checkbox in the "Preferences" screen is **checked** (in the figure, 'Preferences Screen' on page 228) otherwise an error message appears. It requires the user to have **administrator privileges**. The remote reset is supported for software in this version and up.

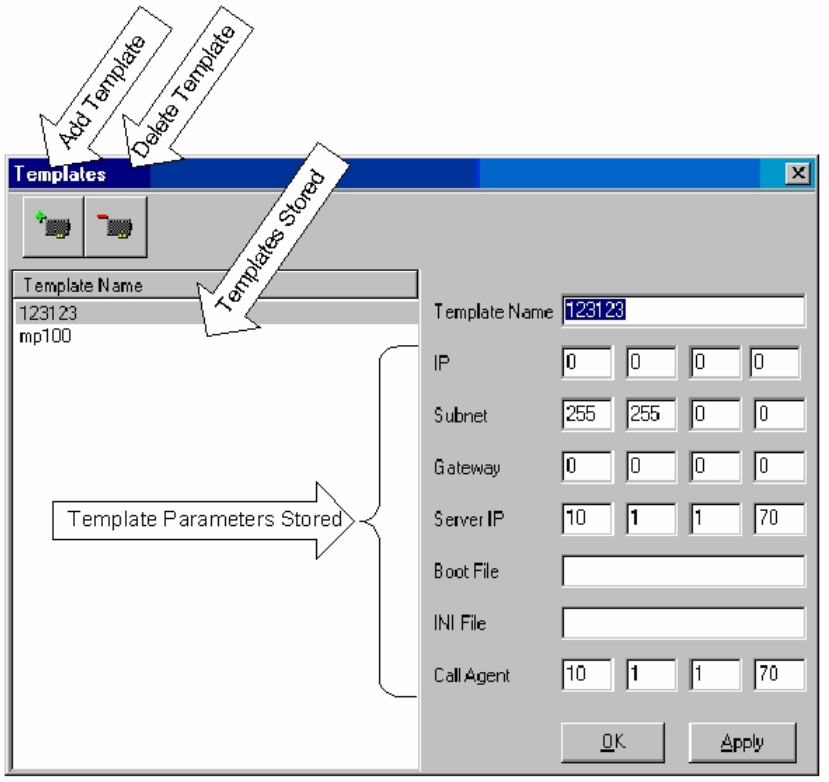
When adding a new client, click **Add Client**. A client dialog box with blank parameters is displayed. After filling out the parameters, click **Apply**. The client is added.

To find out if there is another BootP server on the net that contains a client with the same MAC address, click **Test Selected Clients.** In the log screen, view the IP addresses of all BootP servers that contain the same MAC address in the status 'Listed At'. In normal operation, BootP client MAC address should be listed only on a single BootP server. If the MAC address is listed in multiple BootP servers, it must be removed from other BootP servers.

11.2.4 Templates Screen

The figure below shows the Templates screen, which provides a fast way to configure a number of clients that have the same parameters (except for the IP address). To use the Templates screen, create a template, and then apply the template to the client by selecting it.

Figure 11-4: Templates Screen



Reader's Notes

12 Appendix - Individual ini File Parameters

12.1 Individual ini File Parameters

The individual parameters contained in the *ini* file are provided in the following parameter group tables:

- System Parameters (refer to "System Parameters" on page 233)
- Infrastructure Parameters (refer to "Infrastructure Parameters" on page 245)
- Media Processing Parameters (refer to "Media Processing Parameters" on page 254)
- PSTN Parameters (refer to "PSTN Parameters" on page 238)
- SS7 Parameters (refer to "SS7 Parameters" on page 265)
- Common Control Protocols Parameters (refer to "Common Control Protocols Parameters" on page 266)
- H.248 Specific Parameters (refer to "H.248 Specific Parameters" on page 272)
- Web Interface Parameters (refer to "Web Interface Parameters" on page 275)
- SNMP Parameters (refer to "SNMP Parameters" on page 271)
- SCTP Parameters (refer to "SCTP Parameters" on page 278)
- Names for optional configuration files (CAS signaling, Call Progress Tones and Voice Prompts files).

Users do not have to specify all (or any) of the parameters in the *ini* file. If a parameter is left unspecified in an *ini* file and the *ini* file is then loaded to the MG 3200, the MG 3200 is configured with that parameter's default value. Leaving all *ini* file parameters unspecified and loading the file to the MG 3200 is thus result in the MG 3200 being configured with its defaults (contained in the software image *cmp* file).

Note: To restore the MG 3200's default configuration parameters, use an empty *ini* file without any valid parameters or with a ";" sign preceding all lines in the file.

Array Parameters

Some parameters have array values. For each of these parameters listed in the parameter tables below, if the *ini* file field name is used as is, the parameter applies to all of its elements. To specify each element individually, add *_xx* (*xx* equals the element number) to the end of the *ini* file field name. Information about the array value's elements is contained in the Description column.

12.1.1 System Parameters

The table below lists and describes the system parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-1: System Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
ActiveBoardIPAddress	Defines the IP addresses of the active boards in a High Availability configuration, from which the redundant board receives state DB packets. Range = Any IP address		See Descr.
ActiveBoardPort	Defines the port number for the High Availability service. Range = Valid port number Default = BSP_TPNCP_UDP_CONTROL_PORT	See Descr.	See Descr.
AlarmHistoryTableMaxSize	Determines the maximum number of rows in the Alarm History table. The parameter is controllable via the Config Global Entry Limit MIB (located in the Notification Log MIB). Default = ALARM_HISTORY_DEFAULT_SIZE Range: 50 to 1000 (for MP-1xx media gateways, the range is 50 to 100).	See Descr.	See Descr.
AutoUpdateCmpFile	Updates cmp file automatically. 1 = Enable; 0 = Disable	0	0 or 1
AutoUpdateFrequency	Defines the number of minutes to wait in between automatic updates to the configuration files.	0	-
AutoUpdatePredefinedTime	Schedules the update of configuration files to a predefined time of the day (hh:mm). Range = 'HH:MM' (24-hour format)	NULL	See Descr.
CasFileUrl	Links to a Channel Associated Signaling (CAS) file to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
CmpFileURL	Links to a software image (cmp file) to be downloaded from a remote server.	NULL	See Descr.

Table 12-1: System Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Range = tftp://server_ip/file, http://server_name/file, https://server_name/file		
CptFileUrl	Links to a Call Progress Tones (CPT) file to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
DisableWebConfig	Enables or disables Web Configuration 0 = Read & Write mode (default) 1 = Read Only mode	0	0 or 1
DIsableWebtask	Enables or disables Web Server Task 0 = Enable (default) 1 = Disable	0	0 or 1
DNSPriServerIP	Defines the DNS primary server's IP address. Range = Legal IP address	0.0.0.0	See Descr.
DNSSecServerIP	Defines the DNS secondary server's IP address. Range = Legal IP address	0.0.0.0	See Descr.
EnableParametersMonitoring	enables monitoring of on-the-fly parameter changes via Syslog messages. 1 = activate; 0 = deactivate (default)	0	0 or 1
EnableSTUN	Enables the STUN module, used for NAT traversal of UDP packets.	0	0 or 1
EnableSyslog	Enables the Syslog protocol log. 1 = Activate; 0 = Deactivate	0	0 or 1
IniFileTemplateUrl	Links to an ini file to be downloaded from a remote server, in addition to IniFileUrl. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
IniFileURL	Link to an ini file to be downloaded from a remote server. Range = tftp://server_ip/file, http://server_name/file, https://server_name/file	NULL	See Descr.
InitialShellCommand	A Command Shell command to be executed during initialization. Several commands can be entered (separated	NULL	-

Table 12-1: System Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	by ";" sign).		
NATBindingDefaultTimeout	Defines the NAT binding lifetime, in seconds. STUN refreshes the binding information after this time expires. Range = 0 to 2592000	30	See Descr.
NTPServerIP	This parameter is used to define the NTP server's IP address. Range = Legal IP address	0.0.0.0	See Descr.
NTPServerUTCOffset	This parameter is used to define the NTP time to offset, in seconds. Range = -43200 to + 43200 seconds	0	See Descr.
NTPUpdateInterval	This parameter defines the NTP update interval, in seconds. Do not set it exceeding 1 month (2592000 seconds). Range = 0 to 2592000 seconds Default = 86400 seconds	See Descr.	See Descr.
PrtFileUrl	Links to a prerecorded tones dat file, to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
RedundantBoardIPAddress	Defines the IP address of the redundant board, to which state DB packets are sent. Range = Any IP address	NULL	See Descr.
ResetNow	This parameter causes an immediate restart of the device. The parameter can be used for configuration files loaded via IniFileUrl.	0	0 or 1
SaveConfiguration	Determines if the device configuration (and the loadable file) is saved in flash. Choose either: 1 = Save configuration file (the Call Progress Tones, PRT and/or coefficient file) in non-volatile memory 0 = Don't save	1	0 or 1
SendKeepAliveTrap	When Enabled, this parameter invokes the keep-alive trap and sends it out every 9/10 of the time defined in the parameter defining NAT Binding Default Timeout.	0	-
STUNServerPrimaryIP	Defines the primary STUN Server IP	0.0.0.0	See

Table 12-1: System Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	address. Range = Legal IP address		Descr.
STUNServerSecondaryIP	Defines the secondary STUN server IP address. Range = Legal IP address	0.0.0.0	See Descr.
SyslogServerIP	Defines the IP address in dotted format notation. e.g., 192.10.1.255 Range = Legal IP address	0.0.0.0	See Descr.
SystemOperationStateChange Profile	This parameter defines the System Operation state Change Profile. 0 = Disable 1 = Nortel AMS ATM Refer to the enumerator acSystemOperationStateChangeProfile enum for the possible values. Range = Integer >0	0	0 or 1
TelnetServerEnable	Enables or disables the embedded Telnet server. Telnet is disabled by default for security reasons. 0 = Disable 1= Enable 2 = SSL mode (if available - requires an SSL-aware Telnet client software) SSL mode is not available on the MP-108 / MP-124 media gateways	0	0 to 2
TelnetServerIdleDisconnect	This parameter is used to set the timeout for disconnection of an idle Telnet session (minutes). When set to zero, idle sessions are not disconnected.	0	Any number
TELNETServerPort	Defines the port number for the embedded Telnet server. Range = Valid port number	23	See Descr.
VpFileUrl	Links to a Voice Prompts file to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.

12.1.2 PSTN Parameters

The table below lists and describes the PSTN parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
CASFileName	This is a pointer to the CAS filename index (0-7). The index is CASFileName_X. CASFileName_0 through to CASFileName_7 are the path and names of the CAS protocol configuration files.	NULL	See Descr.
CASTableIndex	Determines which CAS protocol file to use on a specific trunk. The index value corresponds to the number configured for the parameter CASFileName_X. Range = not greater than the parameter defining the PSTN CAS Table Num.	0	See Descr.
CASTablesNum	This parameter defines the number of CAS tables that are loaded to the device during a reset. The quantity of CAS tables defined should match the value configured for parameter CASFILENAME_X. 0 = when there is no CAS table to be loaded	0	0 to 8
ClockMaster	Selects the trunk clock source. 0 = acCLOCK_MASTER_OFF (clock recovered from the line) 1 = acCLOCK_MASTER_ON (the trunk clock source is provided by the internal/TDM bus clock source depending on the parameter TDM Bus Clock Source)	0	0 or 1
DCHConfig	Defines D-channel configuration. This setting is only applicable to ISDN PRI protocols that support NFAS and/or D-channel backup procedures. 0 = D-channel is Primary 1 = Backup 2 = NFAS	0	0 to 2
DisableTrunkAfterReset	Used to change the transmission state of the PSTN physical device. Enable, Disable (Tri state) or Send Blue Alarm.	0	0 or 1

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	0 = Trunk Enabled 1 = Trunk Disabled		
DS3ClockSource	Selects the physical DS3 framing method to be used in this board. **Applicable only to the TP-2810.** 0 = DS3Clock is recovered from the line 1 = DS3 trunk clock source is provided by the board's internal clock 2 = Clock is taken from the local PLL which is not synchronized with any other clock	0	0 to 2
DS3FramingMethod	Used to select the physical DS3 framing method to be used in this board. **Applicable only to the TP-2810.** 0 = M23 framing 1 = C Bit Parity	0	0 or 1
DS3LineBuiltOut	Used to select the DS3 line build out. **Applicable only to the TP-2810.** 0 = For a physical DS3 line longer than 225 meters 1 = For a line shorter than 225 meters	0	0 or 1
FramingMethod	Selects the physical framing method to be used for this trunk. 0 = default according to protocol type E1 or T1 [E1 default = E1 CRC4 MultiFrame Format extended G.706B (as c)] [T1 default = T1 Extended SuperFrame with CRC6 (as D)] 1 = T1 SuperFrame Format a = E1 DoubleFrame Format b = E1 CRC4 MultiFrame Format c = E1 CRC4 MultiFrame Format extended G.706B A = T1 4-Frame multiframe C = T1 Extended SuperFrame without CRC6 D = T1 Extended SuperFrame with	See Descr.	0, 1, a, b, c, A, C, F

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	CRC6 F = J1 Extended SuperFrame with CRC6 (Japan)		
ISDNDuplicateQ931BuffMode	Activates / de-activates delivery of raw Q.931 messages.	0	-
ISDNGeneralCCBehavior	This is the bit-field used to determine several general ISDN behavior options.	0	See Descr.
ISDNIBehavior	Bit-field used to determine several behavior options, which influence how the Q.931 protocol behaves.	0	See Descr.
ISDNInCallsBehavior	This is the bit-field used to determine several behavior options that influence how the ISDN Stack INCOMING calls behave.	0	See Descr.
ISDNNFASInterfaceID	Defines the Interface ID. Functions with NS_EXPLICIT_INTERFACE_ID. Default = (unsigned char)-1.	See Descr.	0 to 255
ISDNOutCallsBehavior	This is the bit-field used to determine several behavior options that influence how the ISDN Stack OUTGOING calls behave.	0	See Descr.
IUAInterfaceID	Defines the IUA trunk interface ID value - unsigned integer - in RFC 3057 - SigTran. Default = 0xFFFFFFFF.	See Descr.	-
LineBuildOut.LOSS	Selects the line build out loss to be used for this trunk. 0 = 0 dB 1 = -7.5 dB 2 = -15 dB 3 = -22.5 dB	0	0 to 3
LineBuildOut.OVERWRITE	Overwrites the Framer's XPM registers values (these registers control the line pulse shape). 0 = No overwrite 1 = Overwrite	0	0 or 1
LineBuildOut.XPM0	Controls the Framer's XPM0 register value (line pulse shape control). Applicable only when TrunkConfig.LineBuildOut.Overwrite=1. Should be used only by expert users.	0	0 to 255
LineBuildOut.XPM1	Controls the Framer's XPM1 register value (line pulse shape control).	0	0 to 255

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Applicable only when TrunkConfig.LineBuildOut.Overwrite=1. Should be used only by expert Users.		
LineBuildOut.XPM2	Controls the Framer's XPM2 register value (line pulse shape control). Applicable only when TrunkConfig.LineBuildOut.Overwrite=1. Should be used only by expert Users.	0	0 to 255
LineCode	Selects line code. B8ZS or AMI for T1 spans and HDB3 or AMI for E1 spans. 0 = (default) HDB3 for E1, B8ZS for T1 1 = Use AMI line code (for T1 or E1 trunks) 2 = Use HDB3 line code (for E1 trunks only)	0	0 to 2
NFASGroupNumber	Relevant only to T1 ISDN NFAS trunks, indicates the group number of the NFAS group. Valid NFAS group numbers are only 1 to 4. 0 indicates that this trunk is not NFAS (in this case the parameters ISDN NFAS Interface ID and Dch Config are ignored).	0	0 to 4
ProtocolType	Used to set the PSTN protocol to be used for this trunk. Relevant only when TDMBusType=acFRAMERS (2). Either: ▪ NONE = 0 NONE – is none configuration trunk. This is the best choice for unused trunks. You can change the configuration later without board reset. ▪ E1_EURO_ISDN = 1 E1_EURO_ISDN – currently not supported. ▪ T1_CAS = 2 T1_CAS – with Megaco and MGCP controller only over 911 CAMA, Ground start and Loop start. ▪ T1_RAW_CAS = 3 T1_RAW_CAS – Not relevant for control protocols. Relevant for API	0	0 to 36

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	library users. No CAS state machine is relevant. Users build their state machine in his application and controls it via commands of Open channel, send CAS, and event detection of CAS changes and digits events. ▪ T1_TRANSPARENT = 4 T1_TRANSPARENT – provides bearer path termination (T1 system) without signaling-related functions. Channels 1-24 mapped to DSP channels. Used for provisioning SS7 trunk or PRI trunk of an NFAS group that does not host the D channel i.e. B-channel span only. ▪ E1_TRANSPARENT_31 = 5 E1_TRANSPARENT_31 – provides bearer path termination (E1 system) without signaling-related functions, with reclaiming timeslot 16. Channels 1-31 mapped to DSP channels. Used for provisioning SS7 trunk. Note: If using E1_TRANSPARENT_31, it is the only protocol type that can be used on that board (or logical GW). Note: There are 240 DSP resources per logical GW. The first 240 channels requesting a DSP resource have those resources allocated. Attempt to open bearer channels beyond that is denied. ▪ E1_TRANSPARENT_30 = 6 E1_TRANSPARENT_30 – provides bearer path termination (E1 system) without signaling-related functions. Channels 1-31, except 16 mapped to DSP channels. Used for provisioning SS7 trunk. Note: Attempts to establish a bearer path on timeslot 16 are rejected. ▪ E1_MFCR2 = 7 E1_MFCR2 – with Megaco controller only over Brazilian, Korean and Mexican R2 variants. ▪ E1_CAS_R2 = 8 E1_CAS_R2 – this protocol type was changed to E1_CAS. Megaco and MGCP do not use it. For API Library		

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	users, it is the same as E1_RAW_CAS. ▪ E1_RAW_CAS = 9 E1_RAW_CAS – Not relevant for control protocols. Relevant for API library users. No CAS state machine is relevant. Users build their state machine in his application and controls it via commands of Open channel, send CAS, and event detection of CAS changes and digits events. The following protocol type is currently not supported: ▪ T1_NI2_ISDN = 10 ▪ T1_4ESS_ISDN = 11 ▪ T1_5ESS_9_ISDN = 12 ▪ T1_5ESS_10_ISDN = 13 ▪ T1_DMS100_ISDN = 14 ▪ J1_TRANSPARENT = 15 ▪ T1_NTT_ISDN = 16 ▪ E1_AUSTEL_ISDN = 17 ▪ E1_HKT_ISDN = 18 ▪ E1_KOR_ISDN = 19 ▪ T1_HKT_ISDN = 20 ▪ E1_QSIG = 21 ▪ E1_TNZ_ISDN = 22 ▪ T1_QSIG = 23 ▪ V5_2_AN = 26 ▪ T1_IUA = 28 T1_IUA – relays ISDN signaling (T1 system) through SIGTRAN IUA and SCTP protocols. Used for provisioning PRI trunk or PRI trunk of an NFAS group that hosts the D channel. ▪ E1_IUA = 29 E1_IUA – relays ISDN signaling (E1 system) through SIGTRAN IUA and SCTP protocols. Used for provisioning PRI trunk.		

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Note: NFAS trunk is not supported on E1 ▪ T1_EURO_ISDN = 34 (Note: currently not supported) ▪ T1_DMS100_MERIDIAN_ISDN = 35 (Note : currently not supported) ▪ T1_NI1_ISDN = 36 (Note : currently not supported) ▪ E1_DUA = 37 E1_DUA – relays DPNSS signaling through SIGTRAN DUA and SCTP protocols. Used for provisioning DPNSS trunk. Note: In SN09, only 4 E1 DUA spans per TPM is supported.		
Q931RelayMode	Activates / de-activates the ISDN level 3 Q.931 Relay Mode. Choose 0 or ActivateLAPDmessaging or Q931_RELAY_TO_HOST or Layer3_IS_IUA.	0	See Descr.
TDMBusPSTNAutoClockEnable	Enables or disables the PSTN trunk auto-fallback clock feature. 0 = PSTN_Auto_Clock_Disable 1 = PSTN_Auto_Clock_Enable	0	0 or 1
TerminationSide	Selects the ISDN Termination to either User or Network. Termination = For ISDN only. User side = 0 Network side = 1	0	0 or 1
TraceLevel	Defines the Trace level: acNO_TRACE = 0 acFULL_ISDN_TRACE = 1 acLAYER3_ISDN_TRACE = 2 acONLY_ISDN_Q931_MSGS_TRACE = 3 acLAYER3_ISDN_TRACE_NO_DUPLICATION = 4 acFULL_ISDN_TRACE_WITH_DUPLICATION = 5 acISDN_Q931_RAW_DATA_TRACE =	0	0 to 15

Table 12-2: PSTN Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	6 acISDN_Q921_RAW_DATA_TRACE = 7 acISDN_Q931_Q921_RAW_DATA_TRACE = 8 acSS7_MTP2 = 10 acSS7_MTP2_AND_APPLI = 11 acSS7_MTP2_SL_L3_NO_MSU = 12 acSS7_AAL = 15		
TrunkAdministrativeState	Defines the administrative state of a trunk. Lock the trunk (0) = stop trunk traffic to configure the trunk protocol type Unlock the trunk (2) = enable trunk traffic	2	0 or 2

12.1.3 Infrastructure Parameters

The table below lists and describes the Infrastructure parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
BaseUDPPort	Defines the lower boundary of UDP ports to be used by the board. The upper boundary is calculated on the basis of BoardBaseUDPPort + 10 * (Number of Channels). This parameter value must be a multiple of 10.	4000	0 to 55000
BootPRetries	Defines the number of BootP retries that the board sends during start-up. The board stops issuing BootP requests when either an AA122BootP reply is received or the Number Of Retries is reached. This parameter takes effect only after the next board reset.	3	1 to 14
BootPSelectiveEnable	Configures the board so that it will only accept BootP replies, from the proprietary BootP-TFTP Software. 1 = Enable; 0 = Disable	0	0 or 1
BRONZEServiceClassDIFFSERV	Sets the DiffServ for the Bronze service class content.	10	0 to 56
DisableH100ClocksOnTrunkFailure	Disables the H.100 clock's output when the PSTN reference trunk fails. 0 = Disable 1 = NetRef 2 = A\B 3 = All	0	0 to 3
DisableNetRefOnTrunkFailure	0 = Enables the NetRef signal when the PSTN reference trunk fails. 1 = Disables the NetRef signal when PSTN reference trunk fails.	0	0 or 1
EnableDetectRemoteMACChange	Allows for the detection of an incoming RTP stream from a changed remote MAC address. Used for board redundancy purposes. 0 = Disable 1 = Enable (trigger by media)	3	0 to 3

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	2 = Enable (trigger by GARP) 3 = Enable (trigger by either media or GARP)		
EnableDiagnostics	Checks the correct functionality of the different hardware components on the board. On completion of the check, the board sends an EV_END_BIT value, which contains information on the test results of each hardware component. 0 = No diagnostics (default). 1 = Perform diagnostics (full test of DSPs, PCM, Switch, LAN, PHY and Flash). 2 = Perform diagnostics (full test of DSPs, PCM, Switch, LAN, PHY, but partial, test of Flash, a quicker mode).	0	0 to 2
EnableDNSasOAM	Sets the location of the DNS. If this parameter is set and the machine is functioning in multiple IPs mode, the DNS is located on the OAM network. If not, the DNS is on the control network.	1	0 or 1
EnableICMPUnreachableReport	Reports receipt of unreachable ICMP packets. 0 = Disabled; 1 = Enabled	1	0 or 1
EnableIPAddrTranslation	Specifies the type of compare operation performed on the first packet that is received on a newly opened channel for the Network Address Translation (NAT) feature. If set to 1, the board compares the first incoming packet's source IP address, to the remote IP address stated in the opening of the channel. If the two IP addresses do not match, the NAT operation takes place. Consequently, the remote IP address and the UDP port of the outgoing stream are replaced by the source IP address and UDP port of the first incoming packet. 0 = Disable; 1 = Enable	1	0 or 1
EnableLANWatchdog	Detects LAN failures on the board. A LAN failure can result from a	0	0 or 1

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	software or hardware malfunction. If a LAN failure is detected, the board performs a self reset (when not in PCI mode). 0 = Disable; 1 = Enable		
EnableMultipleIPs	Enables the multiple IPs feature. 0 = Disable; 1 = Enable	0	0 or 1
EnableNTPasOAM	Sets the location of the Network Time Protocol (NTP). If this parameter is set and the machine is functioning in multiple IPs mode, the NTP is located on the OAM network. If not, the NTP is located on the control network.	1	0 or 1
EnableSCTPasControl	Sets the location of the Stream Control Transmission Protocol (SCTP). If this parameter is set and the machine is functioning in multiple IPs mode, the SCTP is located on the control network. If not, the SCTP is located on the OAM network.	1	0 or 1
EnableUDPPortTranslation	Specifies the type of compare operation performed on the UDP ports. When set, the compare operation is performed on the UDP ports. If this parameter is set, EnableIpAddrTranslation must also be set. 0 = Disable; 1 = Enable	0	0 or 1
EthernetPhyConfiguration	Controls the Ethernet connection mode type. Auto-negotiate falls back to Half-Duplex mode (HD) when the opposite port is not in Auto-negotiate mode. The speed (10 Base-T or 100 Base-TX) in this mode is always configured correctly. 0 = 10 Base-T half-duplex 1 = 10 Base-T full-duplex 2 = 100 Base-TX half-duplex 3 = 100 Base-TX full-duplex 4 = Auto-negotiate	4	0 to 4
ExtBootPReqEnable	Enables extended information to be sent in the BootP request. The device uses the vendor specific information in the BootP request to	0	0 or 1

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	provide device-related, initial startup parameters such as board type, current IP address, software version, Geographical Address, etc. This is not available in DHCP.		
ForceExceptionDump	Forces an exception dump that is sent every time the board restarts. 0 = Disable; 1 = Enable	0	0 or 1
GOLDServiceClassDIFFSERV	Sets the DiffServ for the Gold service class content.	26	0 to 56
HeartbeatDestIP	Sets the destination UDP port to which the heartbeat packets are sent. Range = IP address in dotted notation xxx.xxx.xxx.xxx	0.0.0.0	See Descr.
HeartbeatDestPort	Sets the destination UDP port to which the heartbeat packets are sent.	0	0 to 64000
HeartbeatIntervalmsec	Sets the time delay in msec between consecutive heartbeat packets. Range = 0x0 to 0xFFFFFFFF Default = 0xFFFFFFFF	See Descr.	See Descr.
HeartbeatSecondaryDestIP	Sets the secondary destination IP address to which the heartbeat packets are sent. Range = IP address in dotted notation xxx.xxx.xxx.xxx	0.0.0.0	See Descr.
ICMPUnreachableReportInterval	Determines: (a) The time the board ignores incoming ICMP unreachable packets from the channel activation time (b) The time it takes from the last ICMP unreachable packet until the board reports ICMP Reachable. Range = unsigned long	5000	See Descr.
INIFileVersion	Contains the ini file version number that is reported in the acEV_BOARD_STARTED event. Range = Long integer value.	0	See Descr.
LocalControlDefaultGW	Defines the default gateway of the Control when operating in a multiple IP mode.	0.0.0.0	See Descr.

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Range: Legal IP		
LocalControlIPAddress	Defines the IP address of the Control when operating in a multiple IP mode. Range: Legal Subnet	0.0.0.0	See Descr.
LocalControlSubnetMask	Defines the Subnet Mask of the Control when operating in a multiple IP mode. Range: Legal Subnet	0.0.0.0	See Descr.
LocalMediaDefaultGW	Defines the default gateway for the media interface, when operating in a multiple IPs mode. Range: Legal IP address	0.0.0.0	See Descr.
LocalMediaIPAddress	Defines the IP address of the Media when operating in multiple IP mode. Range: Legal IP address	0.0.0.0	See Descr.
LocalMediaSubnetMask	Defines the Subnet Mask for the media interface when operating in a multiple IP mode. Range: Legal Subnet	0.0.0.0	See Descr.
LocalOAMDefaultGW	Sets the Default gateway for the OAM interface when operating in multiple IPs mode. Range: Legal IP address in subnet	0.0.0.0	See Descr.
LocalOAMIPAddress	Sets the IP address of the OAM (Operation, Administration & Management) when operating in multiple IPs mode. Range: Legal IP address	0.0.0.0	See Descr.
LocalOAMSubnetMask	Sets the Subnet Mask for the OAM interface, when operating in multiple IPs mode. Range: Legal Subnet	0.0.0.0	See Descr.
NetworkServiceClassDIFFSERV	This parameter is used to set the DiffServ for Network service class content.	48	0 to 56
PCMLawSelect	Selects the type of PCM companding law in input/output TDM bus (TDM bus is defined using the TDMBusType parameter). 1=A-law	3	1 to 3

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	3=μ-law		
PremiumServiceClassControlDIFFSERV	Sets the DiffServ for the Premium service class content and control traffic.	46	0 to 56
PremiumServiceClassMediaDIFFSERV	Sets the DiffServ for the Premium service class content and media traffic.	46	0 to 56
RoutingTableDestinationMasksColumn	Comprises the destination masks column of the static routing rules that users can add to. Range = Legal IP address.	NULL	See Descr.
RoutingTableDestinationsColumn	Comprises the Destination column of the static routing rules that users can add to. Range: Legal IP Address.	NULL	See Descr.
RoutingTableGatewaysColumn	Comprises the gateways column of the static routing rules that users can add. Range = Legal IP Address.	NULL	See Descr.
RoutingTableHopsCountColumn	Comprises the Hops count column of the static routing rules that users can add.	20	0 to 255
RoutingTableInterfacesColumn	Comprises the interfaces column of the static routing rules that users can add.	0	0 to 2
SubnetBroadcastAfterENetSOEnabled	Enables subnet broadcast after Ethernet switch over. 0 = Disable; 1 = Enable	0	0 or 1
TDMBITSClockReference	Configures the BITS clock reference when the board source clock is set to BITS and Fallback is set to manual or non-revertive. 1 = REF_1; 2 = REF_2	1	1 to 2
TDMBITSClockSource	Configures which clock is output to the BITS card and on which output signal. Range: 0 = No output (acTDMBusClockSource_Null) 4 = Network_A (acTDMBusClockSource_Network) 16 =	0	0, 4, 16 to 18

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Network_B(acTDMBusClockSource_Network_B) 17 = ATM_A(acTDMBusClockSource_ATM_OC3) 18 = ATM_B(acTDMBusClockSource_ATM_OC3_B)		
TDMBusClockSource	Selects the clock source on which the board synchronizes. 1 = Local oscillator 3 = MVIP 4 = PSTN Network 8 = H.110A 9 = H.110B 10 = NetRef1 11 = NetRef2 12 = SC2M 13 = SC4M 14 = SC8M Default = 1; TP-1610 = 3	See Descr.	1 to 14
TDMBusEnableFallback	Defines the auto fallback of the clock. Range: 0 = Manual 1 = Auto non-revertible 2= Auto revertible	0	See Descr.
TDMBusFallbackClock	Selects the fall-back clock source on which board synchronizes in the event of clock failure. 4 = PSTN Network 8 = H.110A 9 = H.110B 10 = NetRef1 11 = NetRef2	4	4 to 11
TDMBusLocalReference	When the clock source is set to Network, this parameter selects the Trunk ID to be used as the clock synchronization source of the board.	0	See Descr.

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	When using H.110/H.100 bus, this parameter also selects the trunk used as the clock source for the NetRef clock generation (in this case, the clock source must not be set to Network. Range = 0 to (MAX_TRUNK _NUM-1)		
TDMBusmasterSlaveSelection	Set SC/MVIP/H.100/H.110 to either: 0 = Slave mode (another board in the system must supply the clock to the TDM bus) or Master mode (the board is the clock source for the TDM bus) or Secondary Master mode (for H100/H110 Bus only). 1 = H.110A Master in Master mode 2 = H.110B Master	0	0 to 2
TDMBusNetrefOUTPUTMODE	Selects the NetRef output functionality. 0 = Do not output any NetRef 1 = Generation of NetRef 1 2 = Generation of NetRef 2 3 = Generation of both	0	0 to 3
TDMBusNetrefSpeed	Determines the NetRef frequency (for both generation and synchronization). 0 = 8 kHz 1 = 1.544 MHz 2 = 2.048 MHz	0	0 to 2
TDMBusOutputPort	Defines the SC/MVIP/H.100/H.110 output port to be used for the board's channel #0. All other channels then occupy the next timeslots sequentially. Range: 0 to 15 for SC/MVIP 0 to 31 for H.110	0	See Descr.
TDMBusOutputStartingChannel	Defines the outgoing TDM Timeslot for board's channel #0. The remaining channels are organized sequentially.	0	0 to 127

Table 12-3: Infrastructure Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
TDMBusSpeed	Selects the TDM bus speed according to the Bus Type as follows: SC = 0/2/3 H.110/H.100 = 3 MVIP = 0 Where: 0 = 2048 kbps 2 = 4096 kbps 3 = 8192 kbps 4 = 16384 kbps Default: TP-260 = 2; All other boards = 3	See Descr.	See Descr.
TDMBusType	Selects the TDM bus interface to be used (only one TDM bus interface can be enabled at one time although more than one can physically exist on the board). Range: 0 = acMVIP_BUS 1 = acSC_BUS 2 = acFRAMERS 4 = acH100_BUS 5 = EXT TDM 6 = Analog 8 = SW Pstn Default: TP-1610, TP-2810 and TP-6310 = 2; TPM-1100 = 5; TP-260 = 1	See Descr.	See Descr.

12.1.4 Media Processing Parameters

The table below lists and describes the Media Processing parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
AMDDetectionDirection	Determines the AMD (Answer Machine Detector) detection direction. 0 = Detection from the TDM side 1 = Detection from the Network side	0	0 or 1
ATMG711DefaultLawSelect	Determines the ATM G.711 Default Law Select. 0 = A-law; 1 = μ-law	0	0 or 1
BasicRTPPacketInterval	Selects the RTP packet rate for sample-based coders (such as G.711, G.726, G.727). Also applicable for G.729, G.729E & G.728. 0 = Default (set internally) 1 = 5 msec 2 = 10 msec 3 = 20 msec	0	0 to 3
BellModemTransportType	Use this parameter to set the Bell modem transport method. 0 = Transparent 2 = Bypass (enum ByPassEnable) 3 = Transparent with Events (enum EventsOnly)	0	0, 2, 3
BrokenConnectionEventActivationMode	Determines when to enable detection of broken connections. Default = 0 = Activate when the voice channel is opened for receiving 1 = Activate when the first RTP packet is received	0	0 or 1
BrokenConnectionEventTimeout	Determines for how long the RTP connection should be broken before the Broken Connection event is issued. In units of 100 msec. Range = 3 to 21474836 in units of 100 msec (300 to 0x80000000 msec) Default = 3 (= 300 msec)	See Descr.	See Descr.
CallerIDTransportType	Defines the Caller ID transport type. Disable Caller ID (0): Caller ID detectors are not activated. The Caller ID signal flows in the regular	3	0 to 3

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	RTP audio stream. Relay Caller ID (1): Presently the same as Mute. Mute Caller ID (2): CallerID signals detected and reported but muted from the RTP voice stream.		
CallerIDType	Defines the supported Caller ID type. 0 = Bellcore 1 = ETSI 2 = NTT 4 = British 16 = ETSI_ETS 17 = Denmark 18 = Indian 19 = Brazilian	0	0 to 19
CallProgressDetectorEnable	Enables or disables detection of Call Progress Tones. 0 = Disable; 1 = Enable	1	0 or 1
CASTransportType	Controls the ABCD signaling transport type over IP. 0 = No Relay over the network 1 = Enable CAS relay according to RFC 2833	0	0 or 1
CNGDetectorMode	Determines the CNG Detector mode. 0 = Disable 1 = Relay 2 = Event Only	0	0 to 2
ConnectionEstablishmentNotificationMode	Determines the notification mode for the RTP connection establishment event acEV_CONNECTION_ESTABLISHED. 0 = Notify only after a broken connection event 1 = Also notify when the first RTP packet is received	0	0 or 1
DisableNAT	Enables or disables the NAT feature. 0 = Don't disable NAT; 1 = Disable NAT	1	0 or 1

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
DisableRTCPRandomize	Controls whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter defining RTCP Mean Tx Interval (in milliseconds). 0 = Randomize; 1 = Don't Randomize	0	0 or 1
DJBufMinDelay	Defines the Dynamic Jitter Buffer Minimum Delay (in msec).	150	0 to 150
DJBufOptFactor	Defines the Dynamic Jitter Buffer frame error/delay optimization.	7	0 to 12
DSPVersionTemplateNumber	Selects the DSP load number. Each load has a different coder list, a different channel capacity and different features supported.	0	0 to 255
DTMFDetectorEnable	Enables or disables detection of DTMF. 0 = detection disabled; 1 = detection enabled.	1	0 or 1
DTMFTransportType	Defines the type of DTMF transport. 0 (DTMF Mute) = Erase DTMFs from voice transport, not relayed to remote 2 (Transparent DTMF) = DTMFs remain in the voice stream 3 (RFC2833 Relay DTMF) = DTMFs are muted from the voice stream and relayed according to RFC 2833 Notes: For Nortel H.248 GW applications, the supported value for DTMFTransportType is '2' (Transparent DTMF). - DTMFTransportType set to 'Transparent DTMF' enables the MG 3200 to negotiate for RFC2833 dynamically (via parsing of the SDP data provided by the Media Gateway Controller embedded within the H248 messaging). If the two sides *do not* agree, the unit will leave the DTMF digits within the bearer path and it will be passed to the distant RTP device within the codec that was established for the bearer path. If the SDP information *is negotiated*, then the	3	0 to 3

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	DTMF detected digits will be removed from the bearer path and relayed to the remote RTP device by use of RFC2833 DTMF relay. - DTMFTransportType set to 'RFC2833 Relay DTMF' enables the MG 3200 to always relay DTMF digits using RFC2833 (no negotiation).		
DTMFVolume	Defines and controls the DTMF generation volume [-dBm].	-11	-31 to 0
ECHybridLoss	Sets the worst case ratio between the signal level transmitted to the hybrid and the echo level returning from hybrid. Set this per worst hybrid in the system in terms of echo return loss. Refer to the enumeration acTECHybridLoss. 0 = 6 dBm 1 = 9 dBm 2 = 0 dBm 3 = 3 dBm	0	0 to 3
EnableContinuityTones	Enables or disables Continuity Test tone detection and generation according to the ITU-T Q.724 recommendation. 0 = Disable; 1 = Enable	0	0 or 1
EnableDSPIPMDetectors	Enables or disables DSP IP Media Detectors if allowed in the Feature Key. Enabling this parameter might reduce the board channel capacity. 0 = Disable; 1 = Enable	0	0 or 1
EnableEchoCanceller	Enables or disables the Echo Canceler. 0 = Disable; 1 = Enable	1	0 or 1
EnableFaxModemInbandNetworkDetection	Enables or disables inband network detection related to fax/modem.	0	0 to 1
EnablePatternDetector	Enables or disables activation of the PD (Pattern Detector). 0 = Disable; 1 = Enable	0	0 or 1
EnableRFC2658Interleaving	When enabled, RTP packets include an interleaving byte for VBR coders. 0 = Disable; 1 = Enable	0	0 or 1

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
EnableSilenceCompression	Enables or disables Silence Suppression Mode. 0 = Disable = SILENCE_COMPRESION_DISABLE 1 = Enable = SILENCE_COMPRESION_ENABLE 2 = Enable without adaptation = SILENCE_COMPRESION_ENABLE_NOISE_ADAPTATION_DISABLE	0	0 to 2
EnableStandardSIDPayloadType	When set to 1 (Enable), SID packets are sent with the RTP SID type (RFC 3389). 0 = Disable; 1 = Enable	0	0 or 1
EnableSTUModemDetection	Enables or disables detection of two tones required for an STU modem. 0 = Disable; 1 = Enable	0	0 or 1
EnableTrunkTestingTones	Enables or disables trunk testing tones. 0 = Disables trunk testing tones 1 = Enables trunk testing tones	0	0 or 1
EVRCRate	This parameter is used to configure the EVRC coder bit rate. 0 = Variable Rate 1 = 1 kbps 2 = 4 kbps 3 = 8 kbps	0	0 to 3
FaxBypassPayloadType	Modifies the Fax Bypass Mode RTP packet's payload type. If congestion (if the selected payload type is already used for other coders/modes), then a TP_SETUP_PARAMETER_INVALID_ERROR is issued and the payload type is set to the default value (102). It is the user's responsibility to avoid congestion with other payload types.	102	0 to 127
FaxModemBypasDJBufMinDelay	Determines the Jitter Buffer constant delay (in milliseconds) during a Fax & Modem Bypass session. (The minimum Jitter Buffer Size).	40	0 to 150
FaxModemBypassBasicRTPPa	Sets the basic Fax / Modem Bypass	0	0 to 3

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
cketInterval	RTP packet rate. 0 = Default (set internally) (PACKET_INTERVAL_DEFAULT) 1 = 5 msec (PACKET_INTERVAL_5_MSEC) 2 = 10 msec (PACKET_INTERVAL_10_MSEC) 3 = 20 msec (PACKET_INTERVAL_20_MSEC)		
FaxModemBypassCoderType	Sets the fax/modem bypass coder (according to acTCoders). 0 = G.711 A-law	0	0 to 64
FaxModemBypassM	Defines the number of basic frames to generate one RTP fax/modem bypass packet.	1	1 or 2
FaxModemRelayVolume	Determines the fax gain control. The range -18 to -3 relates to -18.5 dBm to -3.5 dBm in steps of 1 dBm.	-12	-18 to -3
FaxRelayECMEnable	Enables or disables the using of ECM mode during Fax Relay. 0 = Disable; 1 = Enable	1	0 or 1
FaxRelayEnhancedRedundancyDepth	Number of repetitions to be applied to control packets when using the T.38 standard. 4 = Maximum redundancy	4	0 to 4
FaxRelayMaxRate	Limits the maximum rate at which fax messages are transmitted. 0 = 2400 bps 1 = 4800 bps 2 = 7200 bps 3 = 9600 bps 4 = 12000 bps 5 = 14400 bps	5	0 to 5
FaxRelayRedundancyDepth	Determines the depth of redundancy for fax packets. This parameter is applicable only to non-V.21 packets. 0 = No redundancy 1 = Include payload of previous packet 2 = Include payload of previous 2	0	0 to 2

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	packets		
FaxTransportMode	Sets the Fax over IP transport method. 0 = Transparent 1 = Relay 2 = Bypass 3 = Transparent with Events	1	0 to 3
IBSDetectionRedirection	Determines the IBS (In-Band Signaling) Detection Direction. 0 = PCM; 1 = Network	0	0 or 1
IdleABCDPattern	Defines the ABCD (CAS) pattern to be applied on the signaling bus before it is changed by the user or the PSTN protocol. This is only relevant when using PSTN interface with CAS protocols. Range = 0x0 to 0xF	-	See Descr.
IdlePCMPattern	Defines the PCM pattern applied to the E1/T1 timeslot (B-channel) when the channel is idle. Default: 0xFF if PCMLawSelect is μ-law 0xD5 if PCMLawSelect is A-law Range = 0x00 to 0xFF	See Descr.	See Descr.
InputGain	Defines the PCM input gain. The range is -32 dB to +31 dB in 1 dB steps. Default = No Gain	0	-32 to +31
LowDSPResourcesEventHyst	Determines the space between the low and hi watermarks of the DSP resource notifications. Range = 0 to the maximum number of DSP channels	0	See Descr.
LowDSPResourcesEventThreshold	Determines when a notification indicating a 'low number of DSP resources' is issued. Range = Between 0 and the maximum number of DSP channels	0	See Descr.
MaxDTMFDigitsInCIDString	Determines the maximum number of DTMF digits in a DTMF-based Caller ID string.	26	0 to 26

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
MFSS5DetectorEnable	Enables or disables detection of MF SS5 line signaling. 0 = Disable; 1 = Enable	0	0 or 1
MFTransportType	Defines the type of MF transport. 0 = Erase MFs from voice transport not relayed to remote 2 = MFs not erased are not relayed to remote 3 = MFs are muted from the voice stream and relayed according to RFC 2833	3	0 to 3
MinDTMFDigitsInCIDString	Determines the miniumum number of DTMF digits in a DTMF-based Caller ID string.	0	0 to 26
ModemBypassPayloadType	Modifies the Modem Bypass Mode RTP packet's payload type. If congestion (if the selected payload type is already used for other coders/modes), then a TP_SETUP_PARAMETER_INVALID_ERROR is issued and the payload type is set to the default value (103). It is the user's responsibility to avoid congestion with other payload types.	103	0 to 127
NSEMode	Enables or disables Cisco's NSE fax / modem automatic pass-through mode. 0 = Disable; 1 = Enable	0	0 or 1
NSEPayloadType	Users can use this parameter to modify the NSE packet's payload type.	105	96 to 127
PDPattern	Defines the patterns that can be detected by the Pattern Detector.	-	0 to 0xFF
PDThreshold	Defines the number of consecutive patterns to trigger the pattern detection event.	5	0 to 31
PrerecordedTonesFileName	Defines the name (and path) of the file containing the Prerecorded Tones. Range = String of ASCII characters	-	See Descr.
QCELP13Rate	This parameter is used to configure the QCELP13 coder bit rate.	0	0 to 4

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	0 = Variable Rate 1 = 1 kbps 2 = 3 kbps 3 = 7 kbps 4 = 13 kbps		
QCELP8Rate	This parameter is used to configure the QCELP8 coder bit rate. 0 = Variable Rate 1 = 1 kbps 2 = 2 kbps 3 = 4 kbps 4 = 8 kbps	0	0 to 4
RFC2198PayloadType	This parameter sets the RFC 2198 (RTP Redundancy) packet's parameter 'RTP Payload Type'.	104	96 to 127
RFC2833RxPayloadType	Controls the RFC 2833 Rx Relay RTP Payload type.	96	96 to 127
RFC2833TxPayloadType	Controls the RFC 2833 Tx Relay RTP Payload type.	96	96 to 127
RTPRedundancyDepth	Enables or disables generation of RFC 2198 redundancy packets. 0 = Disable; 1 = Enable	0	0 or 1
SITDetectorEnable	Enables or disables SIT (Special Information Tone) detection according to the ITU-T recommendation E.180/Q.35. 0 = Disable; 1 = Enable	0	0 or 1
TestMode	Defines the type of testing mode applied: 0 = Coder Loopback performs an encoder/decoder loopback inside the DSP device 1 = PCM Loopback loops back an incoming PCM to the outgoing PCM. 2 = ToneInjection generates a 1000 Hz tone to the outgoing PCM 3 = NoLoopback sets the channel to work in normal mode	3	0 to 3
UserDefinedToneDetectorEnabl	Enables or disables detection of User	0	0 or 1

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
e	Defined Tones signaling. 0 = Disable; 1 = Enable		
V22ModemTransportType	Sets the V.22 modem transport method. 0 = Transparent 2 = Bypass 3 = Transparent with Events	2	0 to 3
V23ModemTransportType	Sets the V.23 modem transport method. 0 = Transparent 2 = Bypass 3 = Transparent with Events	2	0 to 3
V32ModemTransportType	Sets the V.32 modem transport method. 0 = Transparent 2 = Bypass 3 = Transparent with Events	2	0 to 3
V34ModemTransportType	Sets the V.34 modem transport method. 0 = Transparent 2 = Bypass 3 = Transparent with Events	2	0 to 3
VoicePayloadFormat	Sets the voice payload format. Choose either 0 = RTP or 1 = ATM (which enables working with vendors that use G.726 ATM Payload Format over RTP. Uses the enum acTVoicePayloadFormat. 0 = VoicePayloadFormatRTP 1 = VoicePayloadFormatATM 2 = VoicePayloadFormatIllegal	0	0 to 2
VoicePromptsFileName	Defines the name (and path) of the file containing the Voice Prompts. Range = String of ASCII characters	-	See Descr.
VoiceVolume	Defines the voice output gain control. Range: -32 dB to +31 dB in 1 dB steps -32 = mute	0	-32 to +31

Table 12-4: Media Processing Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Default = 0 = No Gain		

12.1.5 SS7 Parameters

The table below lists and describes the SS7 parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-5: SS7 Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
SS7_MTP2_Param_AERM_TIE	Defines the SS7 alignment emergency error rate threshold.	1	0 to 10
SS7_MTP2_Param_AERM_TIN	Defines the SS7 alignment normal error rate threshold.	4	0 to 20
SS7_MTP2_Param_Error_Correction_Method	Defines the SLI error correction method. 0 = no error correction B = Basic P = PCR (Preventive Cyclic Retransmission)	B	0, B or P
SS7_MTP2_Param_IAC_CP	Defines the number of aborted proving attempts before sending an out-of-service to MTP-3.	5	0 to 10
SS7_MTP2_Param_Link_Rate	Defines the SS7 SLI Link Rate. Choose either: 0 = link not active A = 64 kbps D = 56 kbps	A	0, A or D
SS7_MTP2_Param_LSSU_Length	Defines the SS7 MTP2 LSSU length as 1 or 2 (bytes).	1	1 to 2
SS7_MTP2_Param_Octet_Counting	Defines the SS7 MTP2 Octet received while the octet is in counting mode (# of Octets received - N Octets - while in Octet counting mode).	16	0 to 256
SS7_MTP2_Param_PCR_N2	Defines the Preventive Cyclic Retransmission - the number of message signal unit octets available for retransmission (ITU-T Q703 6.4 -	200	0 to 512

Table 12-5: SS7 Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Forced retransmission).		
SS7_MTP2_Param_SUERM_SU_D	Defines the SS7 Signal Unit error rate monitor D threshold.	256	0 to 256
SS7_MTP2_Param_SUERM_T	Defines the SS7 SUERM (Signal Unit Error Rate Monitor) T threshold.	64	0 to 256
SS7_MTP2_Param_Timer_T1	Defines the SS7 MTP2 T1 alignment ready timer (in msecs).	50000	0 to 100000
SS7_MTP2_Param_Timer_T2	Defines the SS7 MTP2 T2 unaligned timer (in msecs).	150000	0 to 200000
SS7_MTP2_Param_Timer_T3	Defines the SS7 MTP2 T3 timer aligned.	2000	0 to 20000
SS7_MTP2_Param_Timer_T4E	Defines the SS7 MTP2 T4e Emergency proving period timer (msec).	500	0 to 5000
SS7_MTP2_Param_Timer_T4N	Defines the SS7 MTP2 T4n Nominal proving period timer.	8200	0 to 15000
SS7_MTP2_Param_Timer_T5	Defines the SS7 MTP2 Sending SIB timer.	120	0 to 2400
SS7_MTP2_Param_Timer_T6	Defines the SS7 MTP2 Remote Congestion timer (in msec).	6000	0 to 10000
SS7_MTP2_Param_Timer_T7	Defines the SS7 MTP2 excessive delay of the ack timer (in msec).	2000	0 to 5000

12.1.6 Parameters Common to All Control Protocols

The table below lists and describes the parameters, contained in the *ini* file, that are common to all call control protocols. Use this table as a reference when modifying *ini* file parameter values.

Table 12-6: Common Control Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
AdminState	Determines the media gateway's initial administrative state. 0 = Locked; 2 = Unlocked	2	0 or 2
AdminStateLockControl	Defines the time remaining (in seconds) for the shutdown to complete. 0 = immediate shutdown	-1	-1, 0, > 0

Table 12-6: Common Control Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	-1 = waits until all calls drop (infinite) Positive number = the number of seconds to wait		
CallAgentDomainName	Defines a domain name to be used to connect with the Call Agent. The parameter takes precedence over the Call Agent IP and the provisioned Call Agent parameters. Range = String[63]	NULL	See Descr.
CallWaitingToneDuration	Changes the call waiting tones family duration, in msec.	12000	300 to 30000
ControlDiffServ	Defines the value of the field 'DiffServ' in the IP header for control traffic.	0	0 to 63
CPTransportType	Defines the transport type for the control protocol: 0 = UDP; 1 = TCP	0	0 or 1
CPTrunkIdOffset	Sets the trunk numbering offset. CPTRUNKIDOFFSET_2 causes the first trunk number to be 2.	0	0, >0
DefaultPacketizationPeriod	Defines the default packetization period (Frame Size). Default = 20 msec (for G.723 30)	20	5 to 80
DialToneDuration	Defines the timeout (in seconds) for the dial tone signal.	16	1 to 65535
DigitMapTimeoutTimer	Defines the timeout value (T symbol) in a digit map, in increments of 10. For H.248, it's the start timer. For the rest, it's the end timer.	16	1 to 65535
DTMFDigitLength	Defines the time to play DTMF, in msec.	100	0 to 65535
DTMFInterDigitInterval	Defines the time between DTMFs played, in msec.	100	0 to 65535
EnableCallerIDTypeTwo	Enables or disables Caller ID Type 2. If Off (0), Caller ID Type Two is not played (if playing is requested from the Call Agent). 0 = Off; 1 = On	1	0 or 1
EndpointName	H.248: Prefix of the endpoint part of the termination name Range: String[19] Default:	See Descr.	See Descr.

Table 12-6: Common Control Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	H.248: 'line' for analog board and '/c' for trunking boards		
GatewayName	Defines the media gateway's identification name. H.248: Prefix of the gateway part of the termination name. Range: String[63] Default: H.248: NULL for analog boards and 'tgw' for trunking boards	See Descr.	See Descr.
IPDiffServ	Defines the value of the 'DiffServ' field in the IP header for media (RTP) traffic.	0	0 to 63
IPPrecedence	Sets the value of the IP precedence field in the IP header for all packets generated from the channel.	0	0 to 7
IPTOS	Sets the value of the parameter defining IP Type Of Service (TOS) in the IP header for all packets generated from this channel.	0	0 to 15
KeepAliveEnabled	This parameter can be used to enable a KeepAlive message (NOP ServiceChange). 0 = disable; >0 = enable	0	0 or >0
KeepAliveInterval	This parameter is used to define the interval in seconds of a KeepAlive message.	12	1 to 300
MGControlProtocolType	Defines the control protocol type. Choose either: 0 = None 1 = MGCP 2 = H.248 4 = H.323 8 = SIP	1	0 to 8
MGCPCommunicationLayerTimeout	This parameter defines the maximal time to wait for a response before declaring a disconnection (in seconds).	30	>0
MGCPCompatibilityProfile	Controls H.248 functioning for vendor-specific compatibility. Refer to the product's User's Manual.	1	See Descr.

Table 12-6: Common Control Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Range: Integer > 0 Refer to the product's User's Manual or the enumerator mgTMGCPProfile for possible values.		
MGCPDefaultCoder	This parameter can be used to set a default coder for channel opening. For the legal coder names, refer to the product's User Manual. Default = cpDPT_G711µ-law_Coder	G.711	See Descr.
MGCPDefaultPacketizationPeriod	Defines the default packetization period (Frame Size).	20	5 to 120
MGCPDTMFDetectionPoint	Defines if the detection of DTMF events is notified at the start or end of DTMF. 0 = at start of DTMF 1 = at the end of DTMF	1	0 or 1
MGCPRetransmissionTimeout	Controls protocols retransmission timeout. Sets the initial time (in msec) for the first retransmission. The retransmission intervals thereafter increase exponentially.	200	0 to 10000
MGCPRetransmitionTimeout	Sets the initial time for the first retransmission. The Retransmission intervals thereafter increase exponentially.	200	0 to 65535
ProvisionedCallAgents	Use this parameter to define a list of up to 10 (MGCP) or 5 (H.248) legal IP addresses separated by ',' or ';' for the ServiceChange command. The gateway starts connecting with the first and in case of failure, attempts the others. Range: Legal IP Address	NULL	See Descr.
ProvisionedCallAgentsPorts	Use this parameter to define a list of up to 10 (MGCP) or 5 (H.248) Call Agent UDP ports separated by , or ; for each Call Agent defined by the parameter used to specify the Allowed Call Agent Address.	2944	0 to 65535
RandomizeTransactionID	Defines if the transactions produced by the board start with a fixed or random number. 1 = Randomize On Refer also to the parameters defining	1	0 or 1

Table 12-6: Common Control Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Transaction Id Range and Transaction ID Base.		
RTCPInterval	Defines the time interval between the adjacent RTCP reports, in msec.	5000	0 to 65535
SingleSIDPacketWithSCEG729	When using a G.729 coder connection and SCE (Silence Suppression Enable) is On, a single SID packet is sent. If set to 1 and the channel was opened or modified to operate with the G.729 coder with Silence Suppression when Silence is detected, only a single SID packet is sent. If set to 0, SID packets are sent frequently, according to energy changes that require a SID packet for each change.	0	0 or 1
TransactionIDBase	Defines the minimum number for the transaction ID.	2000	> 0
TransactionIDRange	Defines the range for the transaction ID. Default = 999999999	See Descr.	> 0
TransparentCoderPayloadType	Alternative payload type to use as transparent coder.	116	0 to 127
TrunkName	(H.248) Prefix of the trunk part of the termination name. Range: String[19] Default: H.248 = ' ' for analog boards and 's' for trunking boards	See Descr.	See Descr.
USETransparentCoderWithHBR	If this parameter is set to 1 and the connection uses HBR (High Bit Rate) coders, the DTMF transport type is set to Transparent. Coders list: G711A-law_64, G711 µ-law, G726_16, G726_24, G726_32, G726_40, G727_16, G727_24_16, G727_24, G727_32_16, G727_32_24, G727_32, G727_40_16, G727_40_24, G727_40_32. 0 = Do not use; 1 = Use	0	0 or 1

12.1.7 SNMP Parameters

The table below lists and describes the SNMP parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-7: SNMP Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
DisableSNMP	Enables or disables SNMP. 0 = Enable; 1 = Disable		0 or 1
PM_EnableThresholdAlarms	Sends SNMP traps and Syslog messages when performance of the device is degraded (according to the configured thresholds).	0	0 or 1
SetCommunityString	User-determined community string with access limited to ini file entered values only. This parameter is the singular version of the readWriteCommunityStrings, and corresponds to readWriteCommunityStrings_0. Range = String[19]	NULL	See Descr.
SNMPManagerIP	Defines the IP address of the default SNMP manager, in dotted notation format: xxx.xxx.xxx.xxx. SNMP traps are sent to this manager. Range = string[15]	NULL	See Descr.
SNMPManagerIsUsed	Enables a row in the SNMP Managers table. 0 = row is disabled; 1 = row is enabled.	0	0 or 1
SNMPManagerTableIP	Used to define the SNMP manager server IP address. This is the tabular version of the parameter defining SNMP Manager IP. Range = String[15]	0	See Descr.
SNMPManagerTrapPort	Sets the trap ports to be used by the different managers. This parameter is the tabular version of the parameter defining SNMP Trap Port.	162	100 to 3999
SNMPManagerTrapSendingEnable	Enables the SNMP Manager's IP address for traps to be sent to it. When set to 1, traps are sent to this	1	0 or 1

Table 12-7: SNMP Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	manager's IP address;. when set to 0, traps are not sent to it.		
SNMPPort	This parameter specifies the port number for SNMP requests and responses. Generally, it isn't specified and the default is used.	161	100 to 3999
SNMPReadOnlyCommunityString	Used to define a read-only community string. Default = DEFAULT_READONLY_COMMUNITY_STRING Range = String[19]	See Descr.	See Descr.
SNMPReadWriteCommunityString	Used to define a read-write community string. Default = DEFAULT_READWRITE_COMMUNITY_STRING Range = String[19]	See Descr.	See Descr.
SNMPTRAPCOMMUNITYSTRING	Defines the community string used in traps. Default = DEFAULT_TRAP_COMMUNITY_STRING Range = String[19]	See Descr.	See Descr.
SNMPTrapManagerHostName	Defines the Host Name of the SNMP Trap Manager. Example: 'mngr.corp.mycompany.com'. String. 99 characters maximum.	NULL	
SNMPTrustedMGR	Defines the IP address of a trusted SNMP manager. Range = String[15]	0.0.0.0	See Descr.

12.1.8 H.248-Specific Parameters

The table below lists and describes the H.248-specific parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-8: H.248 Specific Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
ATM_BIT_FIELD_SIZE	(For binary H.248) Defines the bit field size for each ATM termination name level.	0	0 to 30
ATM_Num	Defines the starting number for each ATM termination level name. Range: Any positive number.	0	See Descr.
DigitMapName	Name of the provisioned digit map. Range = String[10]	NULL	See Descr.
DIGITMAPPING	The digit map patterns separated by a vertical bar (|), as defined in the H.248 RFC. Range = String[151]	NULL	See Descr.
EP_BIT_Field_Size	(For binary H.248) Defines the bit field size for each name level (level 0 is the left one, i.e. the Trunk number). The total binary name is 32 bits long.	0	0 to 30
EP_Num	Defines the starting number for each name level (level 0 is the left one when looking at the parameter defining Phys Term Name Pattern. Thus, to start trunk numbering from 1, set EP_NUM_0 to 1. Range: Any positive number.	0	See Descr.
LogicalATMTermPattern	Defines the name pattern of an ATM termination. Range: String [30]	NULL	See Descr.
LogicalRTPTermPattern	Defines the name pattern of an RTP termination. For example: 'gw/rtp/*'. The '*' sign stands for the actual number of the RTP termination. Range: String [30]	NULL	See Descr.
MEGACO_MID	Defines the media gateway's MID (Message ID) towards the H.248 Call Agent. If empty or illegal, the MID holds the IP address of the board. Range: String[64]	NULL	See Descr.
MEGACOASN1Profile	Used to profile the binary ASN.1 encoding. Range: Integer >0 Refer to the product's User's Manual for possible values.	1	See Descr.

Table 12-8: H.248 Specific Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
MEGACOCheckLegalityOfMGC	This parameter controls whether H.248 rejects commands from a Media Gateway Controller not in the provisioned list. 0 = Accept 1 = Reject	0	0 or 1
MEGACOContextIDOffset	Offset for the context ID generated by the gateway. e.g., offset = 100 causes the first context to be 101. Range = 0 to 4294967295	0	See Descr.
MEGACOEncoding	Sets the H.248 coding method. 1 = Support H.248 protocol's binary ASN.1 format 0 = Text mode	0	0 or 1
MEGACOTerminationIDOffset	Offset for the ephemeral terminations IDs in the gateway. e.g., offset = 100 causes the first ephemeral termination ID to be 101. Note: This parameter was replaced by the parameter 'RTP_Num'. Range = 0 to 4294967295	0	See Descr.
MEGACOTrunkIDOffset	Sets the offset to the trunk numbering. e.g., Offset = 2 causes the first trunk number to be 2. Note: This parameter was replaced by the parameter 'EP_NUM'. Range: 0 to 4294967295	0	See Descr.
MGCExecutionTime	Defines the estimated execution time of the MGC (in msec).	100	0 to 2000
MGCProvisionalResponseTime	Defines the provisional response timer for the MGC (in msec).	100	0 to 20000
MGExecutionTime	Defines the estimated execution time of the media gateway (in msec).	100	0 to 2000
MGProvisionalResponseTime	Defines the provisional response timer for the media gateway (in msec).	100	0 to 20000
PhysTermNamePattern	Defines the name pattern of a physical termination. Example: 'tgw/t*/c*'. The '*' sign stands for the actual numbers of the trunk and Bchannel. Range: String [30]	NULL	See Descr.

Table 12-8: H.248 Specific Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
RTP_BIT_Field_Size	(For binary H.248) Defines the bit field size for each RTP termination name.	0	0 to 30
RTP_Num	Defines the starting number for each name's RTP termination level (level 0 is the left one, i.e. the Trunk number). Range: Any positive number	0	See Descr.

12.1.9 Web Interface Parameters

The table below lists and describes the Web Interface parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-9: Web Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
BKGImageFileName	Changes a default Web background image to the user background image, by loading a GIF/JPEG file. Range = String[47] Notes: 1. Background height should be 85 pixels. 2. Background image is duplicated alongside to fit the screen width.	NULL	See Descr.
HTTPPort	Determines the local HTTP port of the device. Range = 1 to 65535 (other restrictions may apply in this range)	80	See Descr.
HTTPSCertFileName	Defines the name of the HTTPS server certificate file to be downloaded via TFTP. The file must be in base64-encoded PEM format. Range = String[47]	NULL	See Descr.
HTTPSCipherString	Defines the Cipher string for HTTPS (in OpenSSL cipher list format). Refer to URL http://www.openssl.org/docs/apps/ciphers.html Range = EXP, RC4	0	See Descr.
HTTPSOnly	Use this parameter to allow only HTTPS connections to the internal Web server. When set to 1, unencrypted HTTP is blocked; when set to 0, unencrypted HTTP is allowed.	0	0 or 1
HTTPSPORT	Determine the local Secure HTTPS port of the device. Range = 1 to 65535 (other restrictions may apply in this range)	443	See Descr.
HTTPSRequireClientCertificate	Requires client certificates for HTTPS connection. The client certificate must be preloaded on the	0	0 or 1

Table 12-9: Web Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	gateway, and its matching private key must be installed on the managing computer. Time and date must be correctly set on the gateway, for the client certificate to be verified. When set to 0, client certificates are not required; when set to 1, client certificates are required.		
HTTPSRootFileName	Defines the name of the HTTPS trusted root certificate file to be downloaded via TFTP. The file must be in base64-encoded PEM format. Range = String[47]	NULL	See Descr.
LogoFileName	GIF/JPEG image file name to replace the default Web logo image appearing in the upper left hand corner of the device web interface pages. (Note: Image height should be 85 pixels.) Range = String[47]	NULL	See Descr.
LogoWidth	Defines the logo image (upper left hand corner of web interface pages) width in pixel units. Range = Up to 9999 pixels	441	See Descr.
UseProductName	Activates the userProductName parameter. 1 = On = Enables the userProductName string to override any defaults. 0 = Off = userProductName string has no effect on the product name.	0	0 or 1
UserProductName	A string of characters to replace the default product name appearing in the upper right hand corner of the device web interface pages. Range = String[29]	NULL	See Descr.
UseWeblogo	Enables the webLogoText string to override any loaded logo image file. 1 = Enables the webLogoText string to override any loaded logo image file (and the default logo image). 0 = The webLogoText string will have no effect on the logo image.	0	0 or 1
WebAccessList	Allows IP addesses to connect to the	0.0.0.0	See

Table 12-9: Web Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	Web interface. Set to zeroes to allow all IP addresses. Range = Valid IP address		Descr.
WebLogoText	Replaces the default logo image, appearing in the upper left hand corner of the device web interface pages, with a text string. Range = String[15] Note: This string also replaces the default name in the title bar.	NULL	See Descr.

12.1.10 SCTP Parameters

The table below lists and describes the SCTP parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 12-10: SCTP Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
SCTPAssociationsNum	Defines the maximum number of Stream Control Transmission Protocol (SCTP) associations that can be opened.	3	1 to 8
SCTPChecksumMethod	Stream Control Transmission Protocol (SCTP) uses a checksum mechanism in order to authenticate packets on both sides (the receiving side and the transmitting side). Two checksum mechanisms exist: adler32 checksum mechanism, activated when this parameter is set to 0 crc32c checksum mechanism, which is the improved mechanism, activated when this parameter is set to 1.	0	0 or 1
SCTPDNetNum	Defines the maximum number of association transport addresses that can be active.	3	1 to 3
SCTPHBInterval	Defines the SCTP heartbeat interval.	30	1 to 3600
SCTPHOSTNAME	When set to any value other than an	NULL	See

Table 12-10: SCTP Parameters

ini File Field Name	Description	Host/Manual Default Value	Valid Range
	empty string, SCTP (Stream Control Transmission Protocol) uses the value as the value of the FQDN (Fully Qualified Domain Name) parameter attached to the INIT chunk. In this case, the FQDN parameter replaces any IP address parameters in the INIT chunk. This overcomes NAT problems where the original IP addresses belonging to the endpoint supports are converted into pseudo addresses. When this parameter is not set (default), the INIT chunk is sent without any FQDN parameter. Range = String[42]		Descr.
SCTPISTRMNum	Defines the maximum number of incoming streams.	10	1 to 200
SCTPMaxAssocInitAttempts	Defines the maximum number of SCTP association initialization attempts.	5000	5 to 10000
SCTPMaxAssocRet	Defines the maximum number of SCTP association retransmission attempts.	10	5 to 20
SCTPMaxDataChunkSize	Defines the maximum length of SCTP data chunks.	500	50 to 1504
SCTPOSTRMNum	Defines the maximum number of outgoing streams.	10	1 to 200
SCTPOutChunksNum	Defines the maximum number of outgoing chunks.	630	50 to 630
SCTPPortsNum	Defines the maximum number of SCTP endpoints that can be opened.	5	1 to 5
SCTPT4SAckTimer	Defines the SCTP T4 SACK timer interval.	3	1 to 5

Reader's Notes

13 Appendix - Table Parameters

13.1 ini File Table-Parameters

The following *ini* file Table-Parameters are provided:

SS7 *ini* File Table Parameters

Table 13-1: SS7 Signaling Nodes Table Parameters

***ini* File Field Name**	**Default Value**	**Valid Range**	**Description**
SS7_SN_INDEX	0	0 - (MAX_SN_PER_CARD-1)	Index Field for line
SS7_SN_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST - acPARAMSET_ROWSTATUS_DESTROY	RowStatus Field for line
SS7_SN_ACTION	acSS7SN_PS_ACTION_NONE	acSS7SN_PS_ACTION_NONE - acSS7SN_PS_ACTION_START	Management Field for Actions 0 = acSS7SN_PS_ACTION_NONE 1 = acSS7SN_PS_ACTION_STOP 2 = acSS7SN_PS_ACTION_START

Table 13-1: SS7 Signaling Nodes Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SN_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Result
SS7_SN_NAME	"SN"		String name for SN Params
SS7_SN_TRACE_LEVEL	0	0 or 1	Trace level of signaling node (level 3)
SS7_SN_OPERATIONAL_STATE	L3_OFFLINE	L3_OFFLINE - L3_INSERVICE	Operational state of signaling node 0 = L3_OFFLINE 1 = L3_BUSY 2 = L3_INSERVICE
SS7_SN_MTC_BUSY_STATUS	0	0 or 1	Manual busy status of signaling node
SS7_SN_ADMINISTRATIVE_STATE	L3_OFFLINE	L3_OFFLINE or L3_INSERVICE	Administrative state of signaling node 0 = L3_OFFLINE 2 = L3_INSERVICE
SS7_SN_VARIANT	NET_VARIANT_ITU	NET_VARIANT_ITU - NET_VARIANT_CHINA	Variant of signaling node 1 = NET_VARIANT_ITU 2 = NET_VARIANT_ANSI 3 = NET_VARIANT_CHINA
SS7_SN_NI	NET_INDICATOR_INTERNATIONAL	NET_INDICATOR_INTERNATIONAL - NET_INDICATOR_NATIONAL_SPARE	Network Indicator of signaling node 0 = INTERNATIONAL 1 = INTERNATIONAL_SPARE 2 = NATIONAL 3 = NATIONAL_SPARE
SS7_SN_SP_STP	SN_FUNCTION_IS_SP	SN_FUNCTION_IS_SP - SN_FUNCTION_IS_STP	Routing function of signaling node 0 = SP 1 = STP
SS7_SN_TFC	0	0 or 1	Currently not supported
SS7_SN_OPC	0	0 to 0xFFFFFFFF	Origination (local) point-code of signaling node

Table 13-1: SS7 Signaling Nodes Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SN_ROUTESET_CONGESTION_WINSIZE	8	0 to 255	RouteSet Congestion Size (messages) of signaling node
SS7_SN_TIMERS_INDEX	0	0 - (MTP3_SN_TIMER_SETS-1)	Index of SNTimers tables used for this signaling node
SS7_SN_ISUP_APP	MTP3_NIL_APP	MTP3_NIL_APP, MTP3_UAL_APP	Level 4 application that handles ISUP traffic for this signaling node 0 = NIL 4 = UAL
SS7_SN_SCCP_APP	MTP3_NIL_APP	MTP3_NIL_APP, MTP3_UAL_APP	Level 4 application that handles SCCP traffic for this signaling node 0 = NIL 4 = UAL
SS7_SN_BISUP_APP	MTP3_NIL_APP	MTP3_NIL_APP, MTP3_UAL_APP	Level 4 application that handles BISUP traffic for this signaling node 0 = NIL 4 = UAL
SS7_SN_ALCAP_APP	MTP3_NIL_APP	MTP3_NIL_APP, MTP3_UAL_APP, MTP3_ALCAP_APP	Level 4 application that handles ALCAP traffic for this signaling node 0 = NIL 4 = UAL 5 = ALCAP

Table 13-2: SS7 Signaling Node Timers Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SNTIMERS_INDEX	0	0 - (MTP3_SN_TIMER_SETS-1)	Index Field for line
SS7_SNTIMERS_ACTION	acSS7SNTIMERS_PS_ACTION_NONE	acSS7SNTIMERS_PS_ACTION_NONE - acSS7SNTIMERS_PS_ACTION_NONE	Management Field for Actions

Table 13-2: SS7 Signaling Node Timers Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SNTIMERS_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Results
SS7_SNTIMERS_NAME	"SN_Timers"		String name for SN timer-set
SS7_SNTIMERS_T6	1200	500 to 0xFFFFFFFF	Delay to avoid message mis-sequencing on controlled rerouting
SS7_SNTIMERS_T8	1200	500 to 0xFFFFFFFF	Transfer prohibited inhibition timer (transient solution)
SS7_SNTIMERS_T10	60000	500 to 0xFFFFFFFF	Waiting to repeat signaling route set test message
SS7_SNTIMERS_T11	90000	500 to 0xFFFFFFFF	Transfer restricted timer
SS7_SNTIMERS_T15	3000	500 to 0xFFFFFFFF	Waiting to start signaling route set congestion test
SS7_SNTIMERS_T16	2000	500 to 0xFFFFFFFF	Waiting for route set congestion status update
SS7_SNTIMERS_T18_ITU	20000	500 to 0xFFFFFFFF	Timer within a signaling point whose MTP restarts for supervising link and link set activation as well as the receipt of routing information
SS7_SNTIMERS_T19_ITU	67000	500 to 0xFFFFFFFF	Supervision timer during MTP restart to avoid possible ping-pong of TFP, TFR and TRA messages
SS7_SNTIMERS_T20_ITU	60000	500 to 0xFFFFFFFF	Overall MTP restart timer at the signaling point whose MTP restarts
SS7_SNTIMERS_T21_ITU	65000	500 to 0xFFFFFFFF	Overall MTP restart timer at a signaling point adjacent to one whose MTP restarts
SS7_SNTIMERS_T24_ITU	500	500 to 0xFFFFFFFF	Stabilizing timer after removal of local processor outage, used in LPO latching to RPO (national option)
SS7_SNTIMERS_T22_ANSI	180000	500 to 0xFFFFFFFF	Timer at restarting SP waiting for signaling links to become available

Table 13-2: SS7 Signaling Node Timers Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SNTIMERS_T23_ANSI	180000	500 to 0xFFFFFFFF	Timer at restarting SP, started after T22, waiting to receive all traffic restart allowed messages
SS7_SNTIMERS_T24_ANSI	5000	500 to 0xFFFFFFFF	Timer at restarting SP with transfer function, started after T23, waiting to broadcast all traffic restart allowed messages
SS7_SNTIMERS_T25_ANSI	30000	500 to 0xFFFFFFFF	Timer at SP adjacent to restarting SP waiting for traffic restart allowed message
SS7_SNTIMERS_T26_ANSI	12000	500 to 0xFFFFFFFF	Timer at restarting SP waiting to repeat traffic restart waiting message
SS7_SNTIMERS_T28_ANSI	3000	500 to 0xFFFFFFFF	Timer at SP adjacent to restarting SP waiting for traffic restart waiting message
SS7_SNTIMERS_T29_ANSI	60000	500 to 0xFFFFFFFF	Timer started when TRA sent in response to unexpected TRA or TRW
SS7_SNTIMERS_T30_ANSI	30000	500 to 0xFFFFFFFF	Timer to limit sending of TFPs and TFRs in response to unexpected TRA or TRW

13.1.1.1 SS7 Signaling LinkSet Timers Table Parameters

Table 13-3: SS7 Signaling LinkSet Timers Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LKSETTIMERS_INDEX	0	0 - (MTP3_LKSET_TIMER_SETS-1)	Index Field for line
SS7_LKSETTIMERS_ACTION	acSS7LKSETTIMERS_PS_ACTION_NONE	acSS7LKSETTIMERS_PS_ACTION_NONE - acSS7LKSETTIMERS_PS_ACTION_NONE	Management Field for Actions

Table 13-3: SS7 Signaling LinkSet Timers Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LKSETTIMERS_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Results
SS7_LKSETTIMERS_NAME	"SN_Timers"		String name for SN timer-set
SS7_LKSETTIMERS_T2SLT	30000	500 to 0xFFFFFFFF	Interval timer for sending signaling link test messages
SS7_LKSETTIMERS_T1	1000	500 to 0xFFFFFFFF	Delay to avoid message mis-sequencing on changeover
SS7_LKSETTIMERS_T2	2000	500 to 0xFFFFFFFF	Waiting for changeover acknowledgement
SS7_LKSETTIMERS_T3	1200	500 to 0xFFFFFFFF	Time controlled diversion-delay to avoid mis-sequencing on changeback
SS7_LKSETTIMERS_T4	1200	500 to 0xFFFFFFFF	Waiting for changeback acknowledgement (first attempt)
SS7_LKSETTIMERS_T5	1200	500 to 0xFFFFFFFF	Waiting for changeback acknowledgement (second attempt)
SS7_LKSETTIMERS_T7	2000	500 to 0xFFFFFFFF	Waiting for signaling data link connection acknowledgement
SS7_LKSETTIMERS_T12	1200	500 to 0xFFFFFFFF	Waiting for uninhibit acknowledgement
SS7_LKSETTIMERS_T13	1300	500 to 0xFFFFFFFF	Waiting for force uninhibit
SS7_LKSETTIMERS_T14	3000	500 to 0xFFFFFFFF	Waiting for inhibition acknowledgement
SS7_LKSETTIMERS_T17	1500	500 to 0xFFFFFFFF	Delay to avoid oscillation of initial alignment failure and link restart
SS7_LKSETTIMERS_T22_ITU	180000	500 to 0xFFFFFFFF	Local inhibit ITU test timer
SS7_LKSETTIMERS_T23_ITU	180000	500 to 0xFFFFFFFF	Remote inhibit ITU test timer

Table 13-3: SS7 Signaling LinkSet Timers Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LKSETTIMERS_T20_ANSI	90000	500 to 0xFFFFFFFF	Local inhibit ANSI test timer
SS7_LKSETTIMERS_T21_ANSI	90000	500 to 0xFFFFFFFF	Remote inhibit ANSI test timer

13.1.1.2 SS7 Signaling Link Table Parameters

Table 13-4: SS7 Signaling Link Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINK_INDEX	0	0 - (MAX_SIGNALING_LINKS_PER_CARD-1)	Index Field for line
SS7_LINK_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST - acPARAMSET_ROWSTATUS_DESTROY	RowStatus Field for line
SS7_LINK_ACTION	acSS7LINK_PS_ACTION_NONE	acSS7LINK_PS_ACTION_NONE - acSS7LINK_PS_ACTION_LPR	Management Field for Actions 0 = acSS7LINK_PS_ACTION_NONE 1 = acSS7LINK_PS_ACTION_OFFLINE 2 = acSS7LINK_PS_ACTION_INSERVICE 3 = acSS7LINK_PS_ACTION_ACTIVATE 4 = acSS7LINK_PS_ACTION_DEACTIVATE 5 = acSS7LINK_PS_ACTION_INHIBIT, 6 = acSS7LINK_PS_ACTION_UNINHIBIT

Table 13-4: SS7 Signaling Link Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINK_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Result
SS7_LINK_NAME	"LINK"		String name for Link Params
SS7_LINK_OPERATIONAL_STATE	L3_OFFLINE	L3_OFFLINE - L3_INSERVICE	Operational state of signaling link 0 = L3_OFFLINE 1 = L3_BUSY, 2 = L3_INSERVICE
SS7_LINK_ADMINISTRATIVE_STATE	L3_OFFLINE	L3_OFFLINE or L3_INSERVICE	Administrative state of signaling link 0 = L3_OFFLINE 2 = L3_INSERVICE
SS7_LINK_TRACE_LEVEL	0	0 or 1	Trace level of signaling link (level 2)
SS7_LINK_L2_TYPE	SS7_SUBLINK_L2_TYPE_NONE	SS7_SUBLINK_L2_TYPE_NONE - SS7_SUBLINK_L2_TYPE_SAAL	Link layer type - defines level 2 media of signaling link 1 = SS7_SUBLINK_L2_TYPE_MTP2 2 = SS7_SUBLINK_L2_TYPE_M2UA_MGC 3 = SS7_SUBLINK_L2_TYPE_SAAL
SS7_LINK_L3_TYPE	SS7_SUBLINK_L3_TYPE_NONE	SS7_SUBLINK_L3_TYPE_NONE - SS7_SUBLINK_L3_TYPE_MTP2_TUNNELING	Link high layer type - defines level 3 or L2 high layer of signaling link 1 = SS7_SUBLINK_L3_TYPE_M2UA_SG 2 = SS7_SUBLINK_L3_TYPE_MTP3 3 = SS7_SUBLINK_L3_TYPE_MTP2_TUNNELING

Table 13-4: SS7 Signaling Link Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINK_TRUNK_NUMBER	0	0 - MAX_TRUNK_CAPACITY - 1	Trunk number of signaling link (TDM)
SS7_LINK_TIMESLOT_NUMBER	16	0 to 31	Time-Slot number of signaling link (TDM)
SS7_LINK_MTC_BUSY	0	0 or 1	Link local busy indicator - if set, indicates link is busy due to local mtc action
SS7_LINK_INHIBITION	L3_LINK_UNINHIBITED	0 or 1	Link inhibit indicator - if set, indicates link is inhibited
SS7_LINK_LAYER2_VARIANT	NET_VARIANT_ITU	NET_VARIANT_OTHER - NET_VARIANT_CHINA	Variant (layer 2) of signaling link (TDM) 1 = NET_VARIANT_ITU 2 = NET_VARIANT_ANSI 3 = NET_VARIANT_CHINA
SS7_LINK_MTP2_ATTRIBUTES	3	0 - MAX_C7_MTP2_PARAMS_INDEX	MTP2 attributes of signaling link (TDM)
SS7_CONGESTION_LOW_MARK	5	0 to 255	Link congestion low mark of signaling link (TDM)
SS7_CONGESTION_HIGH_MARK	20	0 to 255	Link congestion high mark of signaling link (TDM)
SS7_LINK_M2UA_IF_ID	0	0 to 0xFFFFFFFF	Interface ID (M2UA) of signaling link
ATM_SAAL_LINK_PROFILE_NUM	0	0 - MAX_SAAL_PROFILES-1	ATM SAAL Link profile number
ATM_SAAL_LINK_TYPE	ATM_VCC_TYPE_PVC	ATM_VCC_TYPE_PVC - ATM_VCC_TYPE_SVC	ATM SAAL link Type PVC/SVC 0 = ATM_UNI_LINK_TYPE 1 = ATM_NNI_LINK_TYPE
ATM_SAAL_LINK_PORT_NUM	0	0 - ATMDB_ATM_MAX_INTERFACES_RANGE	ATM SAAL link port num
ATM_SAAL_LINK_VPI	0	0 to 255	ATM SAAL link VPI
ATM_SAAL_LINK_VCI	0	0 to 0xFFFF	ATM SAAL link VCI

Table 13-4: SS7 Signaling Link Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINK_TNL_MGC_LINK_NUMBER	0	0 - MAX_SIGNALING_LINKS_PER_CARD -1	MTP2 Tunneling: MGC link number (MTP2 \other side\ of signaling link
SS7_LINK_TNL_ALIGNMENT_MODE	M3B_ALIGNMENT_EMERGENCY	0 to 255	MTP2 Tunneling: Alignment mode of signaling links in tunnel 0 = M3B_ALIGNMENT_NORMAL 1 = M3B_ALIGNMENT_EMERGENCY
SS7_LINK_TNL_CONGESTION_MODE	M3B_CONGESTION_ACCEPT	0 to 255	MTP2 Tunneling: Congestion mode of signaling links in tunnel 0 = M3B_CONGESTION_ACCEPT 1 = M3B_CONGESTION_DISCARD
SS7_LINK_TNL_WAIT_START_COMPLETE_TIMER	30000	500 to 0xFFFFFFFF	MTP2 Tunneling Timer: wait start complete
SS7_LINK_TNL_OOS_START_DELAY_TIMER	5000	500 to 0xFFFFFFFF	MTP2 Tunneling Timer: OOS start delay
SS7_LINK_TNL_WAIT_OTHER_SIDE_INSV_TIMER	30000	500 to 0xFFFFFFFF	MTP2 Tunneling Timer: wait other side inservice
SS7_LINKSET_SN_INDEX	0	0 - (MAX_SN_PER_CARD-1)	First Index Field for line
SS7_LINKSET_LINKSET_INDEX	0	0 - (MAX_LINKSETS_PER_SN-1)	Second Index Field for line
SS7_LINKSET_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST - acPARAMSET_ROWSTATUS_DESTROY	RowStatusField for line
SS7_LINKSET_ACTION	acSS7LINKSET_PS_ACTION_NONE	acSS7LINKSET_PS_ACTION_NONE - acSS7LINKSET_PS_ACTION_DEACTIVATE	Management Field for Actions 0 = acSS7LINKSET_PS_ACTION_NONE 1 = acSS7LINKSET_PS_ACTION_

Table 13-4: SS7 Signaling Link Table Parameters

ini File Field Name	Default Value	Valid Range	Description
			OFFLINE 2 = acSS7LINKSET_PS_ACTION_INSERVICE 3 = acSS7LINKSET_PS_ACTION_ACTIVATE 4 = acSS7LINKSET_PS_ACTION_DEACTIVATE
SS7_SN_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Result

13.1.1.3 SS7 Signaling LinkSets Table Parameters

Table 13-5: SS7 Signaling LinkSets Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINKSET_NAME	"LINKSET"		String name for LinkSet Params
SS7_LINKSET_OPERATIONAL_STATE	L3_OFFLINE	L3_OFFLINE - L3_INSERVICE	Operational state of signaling LinkSet 0 = L3_OFFLINE 1 = L3_BUSY, 2 = L3_INSERVICE
SS7_LINKSET_MTC_BUSY_STATUS	0	0 or 1	Manual busy status of signaling LinkSet
SS7_LINKSET_ADMINISTRATIVE_STATE	L3_OFFLINE	L3_OFFLINE or L3_INSERVICE	Administrative state of signaling LinkSet 0 = L3_OFFLINE 2 = L3_INSERVICE
SS7_LINKSET_DPC	0		Destination Point-Code of signaling LinkSet
SS7_LINKSET_MASK	15	0 - 255	Mask for links within signaling LinkSet

Table 13-5: SS7 Signaling LinkSets Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINKSET_ALTERNATE_MASK	240	0 - 255	Alternate mask for links within signaling LinkSet
SS7_LINKSET_TIMERS_INDEX	0	0 - (MTP3_LINKSET_TIMER_SETS-1)	Timers Index of signaling LinkSet

13.1.1.4 SS7 Signaling LinkSet-Links Table Parameters

Table 13-6: SS7 Signaling LinkSet-Links Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINKSETLINK_SN_INDEX	0	0 - (MAX_SN_PER_CARD-1)	First Index Field for line: Signaling Node Number
SS7_LINKSETLINK_LINKSET_INDEX	0	0 - (MAX_LINKSETS_PER_SN-1)	Second Index Field for line: Signaling LinkSet Number
SS7_LINKSETLINK_INNER_LINK_INDEX	0	0 - (MAX_LINKS_PER_LINKSET-1)	Third Index Field for line: Inner Link Index in Signaling LinkSet
SS7_LINKSETLINK_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST - acPARAMSET_ROWSTATUS_DESTROY	RowStatus Field for line
SS7_LINKSETLINK_ACTION	acSS7LINKSETLINK_PS_ACTION_NONE	acSS7LINKSETLINK_PS_ACTION_NONE - acSS7LINKSETLINK_PS_ACTION_NONE	Management Field for Actions
SS7_LINKSETLINK_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Results
SS7_LINKSETLINK_LINK_NUMBER	MTP3_LINK_NIL	0 - MAX_SIGNALING_LINKS_PER_CARD-1	Physical number of signaling link which is part of the LinkSet

Table 13-6: SS7 Signaling LinkSet-Links Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_LINKSETLINK_LINK_SLC	0	0 - MTP3_MAX_SLC	Physical number of signaling link which is part of the LinkSet

13.1.1.5 SS7 RouteSets Table Parameters

Table 13-7: SS7 RouteSets Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_ROUTESET_SN_INDEX	0	0 - (MAX_SN_PER_CARD-1)	First Index Field for line: Signaling Node Number
SS7_ROUTESET_INDEX	0	0 - (MAX_ROUTESETS_PER_SN-1)	Second Index Field for line: Signaling RouteSet Number
SS7_ROUTESET_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST - acPARAMSET_ROWSTATUS_DESTROY	RowStatus Field for line
SS7_ROUTESET_ACTION	acSS7ROUTESET_PS_ACTION_NONE	acSS7ROUTESET_PS_ACTION_NONE - acSS7ROUTESET_PS_INSERVICE	Management Field for Actions 0 = acSS7ROUTESET_PS_ACTION_NONE 1 = acSS7ROUTESET_PS_OFFLINE 2 = acSS7ROUTESET_PS_INSERVICE
SS7_ROUTESET_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Result
SS7_ROUTESET_NAME	"ROUTESET"		String name for RouteSet Params
SS7_ROUTESET_OPERATIONAL_STATE	L3_OFFLINE	L3_OFFLINE - L3_INSERVICE	Operational state of signaling RouteSet 0 = L3_OFFLINE

Table 13-7: SS7 RouteSets Table Parameters

ini File Field Name	Default Value	Valid Range	Description
			1 = L3_BUSY, 2 = L3_INSERVICE
SS7_ROUTESET_ADMINISTRATIVE_STATE	L3_OFFLINE	L3_OFFLINE or L3_INSERVICE	Administrative state of signaling RouteSet 0 = L3_OFFLINE 2 = L3_INSERVICE
SS7_ROUTESET_DPC	0		Destination Point-Code of signaling RouteSet
SS7_ROUTESET_MASK	15	0 - 255	Mask for routes within signaling RouteSet

13.1.1.6 SS7 RouteSet-Routes Table Parameters

Table 13-8: SS7 RouteSet-Routes Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_ROUTESETROUTE_SN_INDEX	0	0 - (MAX_SN_PER_CARD-1)	First Index Field for line: Signaling Node Number
SS7_ROUTESETROUTE_ROUTESET_INDEX	0	0 - (MAX_ROUTESETS_PER_SN-1)	Second Index Field for line: Signaling RouteSet Number
SS7_ROUTESETROUTE_INNER_ROUTE_INDEX	0	0 - (MAX_LINKSETS_PER_ROUTESET-1)	Third Index Field for line: Inner Route Index in Signaling RouteSet
SS7_ROUTESETROUTE_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST - acPARAMSET_ROWSTATUS_DESTROY	RowStatus Field for line
SS7_ROUTESETROUTE_ACTION	acSS7ROUTESETROUTE_PS_ACTION_NONE	acSS7ROUTESETROUTE_PS_ACTION_NONE - acSS7ROUTESETROUTE_PS_ACTION_NONE	Management Field for Actions

Table 13-8: SS7 RouteSet-Routes Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_ROUTESETROUTE_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED - acPARAMSET_ACTION_RESULT_FAILED	Management Field for Actions Result
SS7_ROUTESETROUTE_LINKSET_NUMBER	MTP3_LINKSET_NIL	0 - MAX_LINKSETS_PER_SN-1	Number of signaling LinkSet which is part of the RouteSet
SS7_ROUTESETROUTE_PRIORITY	0	0 to 0xFF	Priority of route within RouteSet

Table 13-9: SigTran Interface Groups Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SIG_IF_GR_INDEX	0	0 to 7	Index Field for line
SS7_SIG_IF_GR_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST, acPARAMSET_ROWSTATUS_DESTROY	ROWSTATUS Field for line
SS7_SIG_IF_GR_ACTION	acSS7SigIfGroup_PS_ACTION_NONE	acSS7SigIfGroup_PS_ACTION_NONE	Management Field for ACTIONS
SS7_SIG_IF_GR_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED, acPARAMSET_ACTION_RESULT_FAILED	Management Field for ACTIONS RESULT
SS7_IF_GR_ID	0xFFFE	0 to 0xFFFF	SigTran group id
SS7_SIG_SG_MGC	83	77(MGC), 83(SG)	UAL group function
SS7_SIG_LAYER	0	0 to 5	SigTran group layer (No layer,IUA/M2UA)
SS7_SIG_TRAF_MODE	1	1 to 3	SigTran group traffic mode.
SS7_SIG_T_REC	2000	0 to 10000000	SigTran group T recovery
SS7_SIG_T_ACK	2000	0 to 10000000	SigTran group T Acknowledge

Table 13-9: SigTran Interface Groups Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SIG_T_HB	2000	0 to 10000000	SigTran group T Heartbeat
SS7_SIG_MIN_ASP	1	1 to 10	SigTran group minimal ASP number
SS7_SIG_BEHAVIOUR	0	0 to 0xFFFFFFFE	SigTran group Behavior bit field
SS7_SCTP_INSTANCE	0xFFFE	0 to 0xFFFE	SigTran group SCTP instance
SS7_LOCAL_SCTP_PORT	0xFFFE	0 to 0xFFFE	SigTran group local SCTP port
SS7_SIG_NETWORK	1	1 to 3	SigTran group Network (ITU,ANSI,CHINA)
SS7_DEST_SCTP_PORT	0xFFFE	0 to 0xFFFE	SigTran group destination SCTP port
SS7_DEST_IP	0	0 to 0xFFFFFFFE	SigTran group destination IP Address
SS7_MGC_MX_IN_STREAM	2	2 to 0xFFFE	SigIfGr_MAX_INBOUND_STREAM
SS7_MGC_NUM_OUT_STREAM	2	2 to 0xFFFE	

Table 13-10: SigTran Interface IDs Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SIG_IF_ID_INDEX	0	0 to 15	Index Field for line
SS7_SIG_IF_ID_ROWSTATUS	acPARAMSET_ROWSTATUS_DOESNOTEXIST	acPARAMSET_ROWSTATUS_DOESNOTEXIST, acPARAMSET_ROWSTATUS_DESTROY	ROWSTATUS Field for line
SS7_SIG_IF_ID_ACTION	acSS7SigIntId_PS_ACTION_NONE	acSS7SigIntId_PS_ACTION_NONE	Management Field for ACTIONS
SS7_SIG_IF_ID_ACTION_RESULT	acPARAMSET_ACTION_RESULT_SUCCEEDED	acPARAMSET_ACTION_RESULT_SUCCEEDED, acPARAMSET_ACTION_RESULT_FAILED	Management Field for ACTIONS RESULT

Table 13-10: SigTran Interface IDs Table Parameters

ini File Field Name	Default Value	Valid Range	Description
SS7_SIG_IF_ID_VALUE	0	0 to 0xFFFFFFFE	SigTran interface Id value field
SS7_SIG_IF_ID_NAME	"INT_ID"	--	SigTran interface Id string name
SS7_SIG_IF_ID_OWNER_GROUP	0	0 to 0xFFFE	SigTran interface Id owner group field
SS7_SIG_IF_ID_LAYER	0	0 to 5	SigTran interface Id layer (NO_LAYER,IUA/M2UA/M3UM2TN)
SS7_SIG_IF_ID_NAI	0xFFFE	0 to 0xFFFE	SigTran interface Id NAI field

Reader's Notes

14 Appendix - RTP/RTCP Payload Types

Latest RTP Payload Types are defined in RFC 3551. For coders that should have dynamic Payload types, proprietary default values out of the dynamic Payload type range have been defined. These defaults are appropriate when working with MG 3200 only. However, it is recommended to set a dynamic Payload type for them, which is usually done by higher applications during call setup. Be sure not to overload dynamic Payload types.

Note: Refer to the Release Notes for the supported coders.

14.1 Payload Types Defined in RFC 3551

Table 14-1: Payload Types Defined in RFC 3551

Payload Type	Description	Basic Packet Rate [msec]
0	G.711 µ-Law	20
2	G.726-32	20
4	G.723 (6.3/5.3 kbps)	30
8	G.711 A-Law	20
15	G.728	20
18	G.729	20
35	G.726-16	20
36	G.726-24	20
38	G.726-40	20
62	QCELP (13.3 kbps)	20
63	G729E	20
200	RTCP Sender Report	Randomly, approximately every 5 sec (when packets are sent by channel)
201	RTCP Receiver Report	Randomly, approximately every 5 sec (when channel is only receiving)
202	RTCP SDES packet	
203	RTCP BYE packet	
204	RTCP APP packet	

Note: QCELP-13 default value (63) is not equal to the RFC 3551 value (12) due to backward compatible problem.

14.2 Payload Types

14.3 Payload Types Not Defined in RFC 3551

Table 14-2: Payload Types Not Defined in RFC 3551

Payload Type	Description	Basic Packet Rate [msec]
39	G.727 16 kbps	20
40	G.727 24-16 kbps	20
41	G.727 24 kbps	20
42	G.727 32-16 kbps	20
43	G.727 32-24 kbps	20
44	G.727-32 kbps	20
45	G.727 40-16 kbps	20
46	G.727 40-24 kbps	20
47	G.727 40-32 kbps	20
51	NetCoder 6.4 kbps	20
52	NetCoder 7.2 kbps	20
53	NetCoder 8.0 kbps	20
54	NetCoder 8.8 kbps	20
55	NetCoder 9.6 kbps	20
56	Transparent PCM	20
60	EVRC	20
61	QCELP (8 Kbps)	20
64	AMR 4.75 Kbps	20
65	AMR 5.15 Kbps	20
66	AMR 5.9 Kbps	20
67	AMR 6.7 Kbps	20
68	AMR 7.4 Kbps	20
69	AMR 7.95 Kbps	20

Table 14-2: Payload Types Not Defined in RFC 3551

Payload Type	Description	Basic Packet Rate [msec]
70	AMR 10.2 Kbps	20
71	AMR 12.2 Kbps	20
72	Vox ADPCM	20
90	Linear PCM	20

14.4 Default Dynamic Payload Types Which are Not Voice Coders

Table 14-3: Payload Types Not Defined in RFC 3551

Payload Type	Description
96	RFC 2833
102	Fax Bypass
103	Modem Bypass
104	RFC 2198
105	NSE

14.5 Default RTP/RTCP/T.38 Port Allocation

The following table shows the default RTP/RTCP/T.38 port allocation.

Table 14-4: Default RTP/RTCP/T.38 Port Allocation

Channel Number	RTP Port	RTCP Port	T.38 Port
1	4000	4001	4002
2	4010	4011	4012
3	4020	4021	4022
4	4030	4031	4032
5	4040	4041	4042
6	4050	4051	4052
7	4060	4061	4062
8	4070	4071	4072
:	:	:	:
n	**4000 + 10(n-1)**	**4001 + 10(n-1)**	**4002 + 10(n-1)**
:	:	:	:
120	5190	5191	5192
:	:	:	:
192	5910	5911	5912
:	:	:	:
384	7830	7831	7832
:	:	:	:
480	8790	8791	8792

Note the changed port allocation from earlier releases, for channel #5 and above.

15 Appendix - DTMF, Fax and Modem Transport Modes

15.1 DTMF/MF Relay Settings

Users can control the way DTMF/MF digits are transported to the remote Endpoint, using the DTMFTransport/MFTransport configuration parameters. The following four modes are supported:

- **DTMF/MFTransportType= 0 (MuteDTMF/MF)** In this mode, DTMF/MF digits are erased from the audio stream and are not relayed to the remote side. Instead, silence is sent in the RTP stream.
- **DTMF/MFTransportType= 2 (TransparentDTMF/MF)** In this mode, DTMF/MF digits are left in the audio stream and the DTMF/MF relay is disabled.
- **DTMF/MFTransportType= 3 (acRelayDTMFOverRTP/ acRFC2833RelayMF)** In this mode, DTMF/MF digits are relayed to the remote side using the RFC 2833 Relay syntax.
- **DTMFTransportType = 7 (acRFC2833RelayDecoderMute)** In this mode, DTMF digits are relayed to the remote side using the RFC 2833 Relay syntax. RFC 2833 digit packets that are received from the remote side are muted on the audio stream.

15.2 Fax/Modem Settings

Users may choose from one of the following transport methods for Fax and for each modem type (V.22/V.23/Bell/V.32/V.34):

- **fax relay -** demodulation / remodulation
- **bypass -** using a high bit rate coder to pass the signal
- **transparent -** passing the signal in the current voice coder
- **transparent with events -** transparent + issues fax/modem events

When the fax relay mode is enabled, distinction between fax and modem is not immediately possible at the beginning of a session. Therefore, the channel is in **Answer Tone** mode until a distinction is determined. The packets being sent to the network at this stage are Fax relay T.38 packets.

15.3 Configuring Fax Relay Mode

When FaxTransportType= 1 (relay mode), upon detection of fax, the channel automatically switches from the current voice coder to answer tone mode, and then to Fax T.38 relay mode.

When Fax transmission has ended, the reverse switching from fax relay to voice is performed. This switching automatically mode occurs at both the local and remote Endpoints.

The fax rate can be limited by using the FaxRelayMaxRate parameter and the ECM Fax Mode can be enabled/disabled using the FaxRelayECMEnable parameter settings.

The (proprietary) redundancy mode that was specially designed to improve protection against packet loss through the EnhancedFaxRelayRedundancyDepth parameter. Although this is a proprietary redundancy scheme, it is compatible with other T.38 decoders. The depth of the redundancy (that is, the number of repetitions) is defined by the FaxRelayRedundancyDeoth configuration parameter.

Note: T.38 mode currently supports only the T.38 UP syntax.

15.4 Configuring Fax/Modem ByPass Mode

When VxxTransportType= 2 (FaxModemBypass, Vxx can be one of the following: V32/V22/V21/Bell/V34/Fax), then on detection of Fax/Modem, the channel automatically switches from the current voice coder to a high bit-rate coder, as defined by the user in the FaxModemBypassCoderType configuration parameter.

If relay is enabled for one of the modes (Fax/Modem), the Answer Tone mode packets are relayed as Fax relay packets.

When the EnableFaxModemInbandNetworkDetection parameter is enabled under the conditions discussed above, a detection of an Answer Tone from the network triggers a switch to bypass mode in addition to the local Fax/Modem tone detections. However, only a high bit-rate coder voice session effectively detects the Answer Tone sent by a remote Endpoint

During the bypass period, the coder uses the packing factor (by which a number of basic coder frames are combined together in the outgoing WAN packet) set by the user in the FaxModemBypassM configuration parameter. The user can also configure the basic frame size by through the FaxModemBypassBasicRTPPacketInterval configuration parameter. The network packets generated and received during the bypass period are regular RTP voice packets (as per the selected bypass coder) but with a different RTP Payload type.

When Fax/Modem transmission ends, the reverse switching, from bypass coder to regular voice coder, is performed.

Note: When Fax relay is enabled, V21TransportType must be set to disable (Transparent) mode.

15.5 Configuring Fax/Modem Bypass NSE mode

Setting the NSEMode to **1** configures the answering Fax/Modem channel to send NSE packets to the calling Fax/Modem channel to switch to Bypass. Using the NSEPayloadType parameter, the user can control the NSE RTP packet's Payload type (default = 105). Note that the value of this parameter should be within the RTP Dynamic Payload Type range (96 to 127).

15.6 Supporting V.34 Faxes

Unlike the T.30 fax machines, the V.34 fax machines have no relay standard to transmit the data over IP to the remote side. Therefore the following operation modes for transporting the V.34 fax data over the IP are provided.

Note: For all the setups described below, the CNG tone detector is disabled.

15.6.1 Using Bypass Mechanism for V.34 Fax Transmission

Configuration:

- **Fax transport mode -** Relay/Bypass
- **Vxx modem mode -** Bypass

Expected events for V.34 Fax to V.34 Fax - Bypass Mode are shown in the table below.

Table 15-1: V.34 Fax to V.34 Fax - Bypass Mode

Calling	Answering
	EV_DETECT_MODEM (2100 AM + Reversal)
EV_DETECT_MODEM	
	EV_DETECT_FAX
EV_DETECT_FAX (Refer to Note 1 below)	
EV_END_FAX	EV_END_FAX

Note: The board changes its status to bypass mode upon receiving fax bypass packet from the remote side.

Note that if the fax transport type is set to relay, the fax relay benefits for the T.30 fax machines and, in parallel, are a variable when using a V.34 fax with its full rate. Therefore, this setup is recommended. Also note that if CNG relay is used, in some cases, such as for manual answering machine, the fax may revert to T.30 fax with a speed of 14400 bps.

15.6.2 Using Events Only Mechanism for V.34 Fax Transmission

Use events only mode to transmit V.34 fax with its maximum capabilities:

Configuration:

- **Fax transport mode -** Events only mode
- **Vxx modem mode -** Events only mode

Expected events for V.34 Fax **to** V.34 Fax - Events Only Mode are shown in the table below.

Table 15-2: V.34 Fax to V.34 Fax - Events Only Mode

Calling	Answering
	EV_DETECT_ANSWER_TONE
	EV_DETECT_FAX

15.6.3 Using Relay Mode for Various Fax Machines (T.30 and V.34)

The user can force the V.34 fax machines to revert to T.30 and work at relay mode.

Configuration:

- **Fax transport mode -** Relay
- **Vxx modem mode -** Disable
- **CNG detectors mode -** Disable

In this mode, the fax events are identical to the regular T.30 fax session over T.38 protocol.

Expected events for V.34 Fax to V.34 Fax - Relay Mode are shown in the table below.

Table 15-3: V.34 Fax to V.34 Fax - Relay Mode

Calling	Answering
	EV_DETECT_ANSWER_TONE
	EV_DETECT_FAX
EV_DETECT_FAX	
EV_END_FAX	EV_END_FAX

16 Appendix - CAS Protocol Table

16.1 Constructing a CAS Protocol Table

Constructing or Modifying a CAS Protocol Table for CAS-Terminated Protocols

The protocol table file is a text file containing the protocol's state machine that defines the entire protocol process. It is constructed of States, pre-defined Actions/Events, and pre-defined functions. With this file, the user has full control of the CAS protocol and can define or modify any CAS protocol by writing the protocol state machine in a text file according to the defined rules.

➢ To generate the protocol file, take these 5 steps:

1. Learn the protocol text file rules (rules detailed in this manual and their syntax are based on C pre-processor commands).
2. Get the provided example.
3. Build the specific protocol/script text (*xxx.txt*) file and its related numerical value h file (*xxx.h*).
4. Compile the *xxx.txt* with the "TrunkPack Downloadable conversion utility" to produce the *xxx.dat* file. Refer to Section D on page 189 ("API Demonstration Utilities") for a detailed description of the utility usage.
5. Download the *User_protocol.dat* file to the board via acOpenBoard() command at initialization phase.

16.2 Table Elements

CASSetup.h - File includes all the pre-defined tools needed to build a new protocol text file or modifying an existing one. The protocol table file is composed of the following bricks:

16.2.1 INIT variables

INIT variables - Numeric values in *UserProt_defines_xxx.h*, defined by the user. For example, INIT_RC_IDLE_CAS defines the ABCD bits expected to be received in the IDLE state, INIT_DTMF_DIAL defines the On-time and Off-time for the DTMF digits generated towards the PSTN. See the detailed list in *CASSetup.h* and in the sample protocol text file. Refer to the following ST_INIT detailed explanation.

16.2.2 Actions

Actions (i.e., protocol table events) - Actions are protocol table events activated either by the DSP (e.g., EV_CAS_01) or by the user (e.g., EV_PLACE_CALL, EV_TIMER_EXPIRED1). The full list of the possible pre-defined events can be found in the *CASSetup.h* file.

16.2.3 Functions

Functions - Define a certain procedure that can be activated in any state or in the transition from one state to another. The available functions include, for example, SET_TIMER (timer number, timeout in ms.) SEND_CAS (AB value, CD value). A full list of the possible pre-defined functions can be found in the *CASSetup.h* file.

16.2.4 States

States - Each Protocol table consists of several states that it switches between during the call setup and tear-down process. Every state definition begins with the prefix ST_ followed by the state name and colons. The body of the state is composed of up to 4 unconditional performed functions and list of actions that may trigger this state.

As an example, the table below was taken from an E&M wink start table protocol file:

Table 16-1: ST_DIAL: Table Elements

Action	Function		Parameter		Next State
		#1	#2	#3	
FUNCTION0	SET_TIMER	2	Extra Delay Before Dial	None	DO
EV_TIMER_ EXPIRED2	SEND_DES T_NUM	None	None	None	NO_STATE
EV_DIAL_ ENDED	SET_TIMER	4	No Answer Time	None	ST_DIAL_ENDED

When the state machine reaches the dial state, it sets timer number 2 and then waits for one of the two possible actions to be triggered: either timer 2 expiration or end of dial event. When timer 2 expires, the protocol table executes SEND_DEST_NUM function and remains in the same state (NEXT_STATE=NO_STATE). When the dial event ends, the protocol table sets timer 4 and moves to ST_DIAL_ENDED written in the NEXT_STATE field.

Although users can define their own states, there are two states defined in the *CASSetup.h* file and must appear in every protocol table created.

The two states are ST_INIT and ST_IDLE.

- **ST_INIT** - When channels initialization is selected, the table enters the Init state. This state contains functions that initialize the following global parameters:
  - **RC_IDLE_CAS** - Defines the ABCD bits expected to be received in the IDLE state in the specific protocol.
  - **TX_IDLE_CAS** - Defines the ABCD bits transmitted on IDLE state in the specific protocol.
  - **DIAL_PLAN** - A change regarding the issue of an incoming call dialed number is implemented in revision 3.21 as opposed to revision 3.2 and earlier. In revision 3.2 and earlier, users were required to pre-define the expected number of digit to receive an incoming call. If a lower number of digits than expected were received, the call setup would have failed.

Revisions 3.21 and later, process the incoming call detection event by declaring end of digit reception in the following ways (both for ADDRESS/destination number and ANI/source number):

- Receiving '#' digit (in MF or DTMF)
- The number of digits collected reaches its maximum value as defined in the DIAL_PLAN Parameter #1 and #2 for destination and ANI numbers respectively
- A pre-defined time-out value defined in the DIAL_PLAN Parameter #3 elapses

Note: This method is not used when working with MFC/R2 protocols. MFC/R2 uses expected number of digits defined in *ProtUser_defines_xxx.h*.

- **DTMF_DIAL** - Defines the On-time and Off-time for the DTMF digits generated towards the PSTN.
- **COMMA_PAUSE_TIME** - Defines the delay between each digit when a "," sign is used as part of the dialed number string. (See acPSTNPlaceCall for further explanation).
- **DTMF_DETECTION** - Defines the minimum/maximum On-time for DTMF digit dialing detection.
- **PULSE_DIAL_TIME** - Not supported by current stack version. Defines the Break and Make time for pulse dialing.
- **PULSE_DIAL** - Not supported by the current stack version. Defines the Break and Make ABCD bits for pulse dialing.
- **DEBOUNCE** - Defines the interval time of CAS to be considered as a hit.
- **COLLECT_ANI** - Enables or Disables reception of ANI in a specific protocol.
- **DIGIT_TYPE** - Defines the dialing method used (DTMF, MF). On MFC/R2 protocols this parameter is not applicable (digits are assumed to be R2 digits).
- **NUM_OF_EVENT_IN_STATE** - Inserted for detection on TOTAL_NUMBER_OF_EVENTS_IN_STATE (*CASSetup.h*).
- **INIT_GLOBAL_TIMERS** - Initiates specific timers, is used with Parameter#1 for metering pulse timer duration.
- **INIT_VERSION** - Defines the version number. The version number is related to the release version number.
- **INIT_SIZE_OF_TABLE_PARAM** - Users must insert the definition of TOTAL_NUMBER_OF_EVENTS_IN_STATE from the *CASSetup.h*.

- ST_IDLE - When no active call is established or in the process of being established, the table resides in Idle state, allowing it to start the process of incoming or outgoing calls. When the call is cleared, the state machine table returns to its idle state.

16.3 Reserved Words

For reserved words, such as DO, NO_STATE, etc. Refer to the detailed list in *CASSetup.h*.

16.4 State's Line Structure

Each text line in the body of each state is composed of 6 columns:

1. action/event
2. function
3. parameter #1
4. parameter #2
5. parameter #3
6. next state

16.5 Action/Event

Action/event is the name of the table's events that are the possible triggers for the entire protocol state machine. Those can be selected from the list of events in the *CASSetup.h* file (e.g., EV_DISCONNECT_INCOMING).

At the beginning of the state, there can be up to 4 special unconditional action/events called FUNCTION. They events are functions that are unconditionally performed when the table reaches the state. These actions are labeled FUNCTION0 to FUNCTION3.

The following is the list of available protocols table actions (events to the state machine):

1. **User Command Oriented:**
   - **EV_PLACE_CALL** - When using acPSTNPlaceCall().
   - **EV_ANSWER** - When using acPSTNAnswerCall().
   - **EV_DISCONNECT_OUTGOING** - When using the function acPSTNDisconnectCall() and the call is outgoing.
   - **EV_DISCONNECT_INCOMING** - When using the function acPSTNDisconnectCall() and the call is incoming.
   - **EV_RELEASE_CALL** - When using acPSTNReleaseCall()
   - **EV_USER_BLOCK_COMND** - When using acCASBlockChannel(), this event handled for blocking or unblocking the channel.
   - **EV_MAKE_METERING_PULSE** - When using acCASMeteringPulse it triggers the start of the metering pulse while using the SET_PULSE_TIMER function to start the timer to get the Off event (refer to the EV_METERING_TIMER_PULSE_OFF below.).
   - **EV_METERING_TIMER_PULSE_OFF** - event after timer (SET_PULSE_TIMER function) expires. (Refer to EV_MAKE_METERING_PULSE above.)
   - **EV_MAKE_FLASH_HOOK** - When using acCASFlashHook, a flash hook is triggered.
2. **CAS Change Oriented:**
   - **EV_CAS_1_1** - a new CAS A,B bits are received (A=1, B=1, was stable for the bouncing period).
   - **EV_CAS_1_0** - a new CAS A,B bits are received (A=1, B=0, was stable for the bouncing period).

- **EV_CAS_0_1** - a new CAS A,B bits are received (A=0, B=1, was stable for the bouncing period).
- **EV_CAS_0_0** - a new CAS A,B bits are received (A=0, B=0, was stable for the bouncing period).

3. **Timer Oriented:**
   - **EV_TIMER_EXPIRED1** - timer 1 that was previously set by table has expired.
   - **EV_TIMER_EXPIRED2** - timer 2 that was previously set by table has expired.
   - **EV_TIMER_EXPIRED3** - timer 3 that was previously set by table has expired.
   - **EV_TIMER_EXPIRED4** - timer 4 that was previously set by table has expired.
   - **EV_TIMER_EXPIRED5** - timer 5 that was previously set by table has expired.
   - **EV_TIMER_EXPIRED6** - timer 6 that was previously set by table has expired.
   - **EV_TIMER_EXPIRED7** - timer 7 that was previously set by table has expired.
   - **EV_TIMER_EXPIRED8** - timer 8 that was previously set by table has expired.
4. **Counter Oriented:**
   - **EV_COUNTER1_EXPIRED** - counter 1 value has reached 0.
   - **EV_COUNTER2_EXPIRED** - counter 2 value has reached 0.
5. **IBS oriented:**
   - **EV_RB_TONE_STARTED** - Ring back tone as defined in the call progress *ini* file (type and index) is detected.
   - **EV_RB_TONE_STOPPED** - Ring back tone as defined in the call progress *ini* file (type and index) is stopped after it has been previously detected.
   - **EV_DIAL_TONE_DETECTED** - Dial tone as defined in the call progress *ini* file (type and index) is detected.
   - **EV_DIAL_TONE_STOPPED** - Dial tone as defined in the call progress *ini* file (type and index) was stopped after it has been previously detected.
6. **MF Oriented (MFCR2 protocol related):**
   - **EV_MFRn_1** - MF digit 1 is detected.
   - **EV_MFRn_2** - MF digit 2 is detected.
   - **EV_MFRn_3** - MF digit 3 is detected.
   - **EV_MFRn_4** - MF digit 4 is detected.
   - **EV_MFRn_5** - MF digit 5 is detected.
   - **EV_MFRn_6** - MF digit 6 is detected.
   - **EV_MFRn_7** - MF digit 7 is detected.
   - **EV_MFRn_8** - MF digit 8 is detected.
   - **EV_MFRn_9** - MF digit 9 is detected.
   - **EV_MFRn_10** - MF digit 10 is detected.
   - **EV_MFRn_11** - MF digit 11 is detected.
   - **EV_MFRn_12** - MF digit 12 is detected.
   - **EV_MFRn_13** - MF digit 13 is detected.

- **EV_MFRn_14** - MF digit 14 is detected.
- **EV_MFRn_15** - MF digit 15 is detected.
- **EV_MFRn_1_STOPPED** - MF digit 1 previously detected, is now stopped.
- **EV_MFRn_2_ STOPPED** - MF digit 2 previously detected, is now stopped.
- **EV_MFRn_3_ STOPPED** - MF digit 3 previously detected, is now stopped.
- **EV_MFRn_4_ STOPPED** - MF digit 4 previously detected, is now stopped.
- **EV_MFRn_5_ STOPPED** - MF digit 5 previously detected, is now stopped.
- **EV_MFRn_6_ STOPPED** - MF digit 6 previously detected, is now stopped.
- **EV_MFRn_7_ STOPPED** - MF digit 7 previously detected, is now stopped.
- **EV_MFRn_8_ STOPPED** - MF digit 8 previously detected, is now stopped.
- **EV_MFRn_9_ STOPPED** - MF digit 9 previously detected, is now stopped.
- **EV_MFRn_10_ STOPPED** - MF digit 10 previously detected, is now stopped.
- **EV_MFRn_11_ STOPPED** - MF digit 11 previously detected, is now stopped.
- **EV_MFRn_12_ STOPPED** - MF digit 12 previously detected, is now stopped.
- **EV_MFRn_13_ STOPPED** - MF digit 13 previously detected, is now stopped.
- **EV_MFRn_14_ STOPPED** - MF digit 14 previously detected, is now stopped.
- **EV_MFRn_15_ STOPPED** - MF digit 15 previously detected, is now stopped.
- **EV_END_OF_MF_DIGIT** - When using DialMF() and no more dialed number digits are available. (They already have been sent. For example, the far side requests the next ANI digit, but all digits already have been sent). This event usually appears in MFR2 tables.
- **EV_NO_ANI** - When using DialMF() and no ANI was specified by the outgoing user in the acPSTNPlaceCall() function. (MFCR2 protocols specifications should define what to do when no ANI digits are available. Usually I-12 is sent).

Note: MF digit is MF R1 or R2-FWD or R2-BWD according to the context, protocol type and call direction.

- **EV_ACCEPT** - When using acCASAcceptCall (used only in MFC/R2) with CALLED_IDLE as its reason parameter.
- **EV_REJECT_BUSY** - When using acCASAcceptCall with CALLED_BUSY as its reason parameter.
- **EV_REJECT_CONGESTION** - When using acCASAcceptCall with CALLED_CONGESTION as its reason parameter.
- **EV_REJECT_UNALLOCATED** - When using acCASAcceptCall with CALLED_UNALLOCATED as its reason parameter.
- **EV_REJECT_RESERVE1** - When using acCASAcceptCall with CALLED_RESERVE1 as its reason parameter.
- **EV_REJECT_RESERVE2** - When using acCASAcceptCall with CALLED_RESERVE2 as its reason parameter.

7. Miscellaneous:

- **EV_DIALED_NUM_DETECTED** - (Incoming call) dialed destination number is collected after START_COLLECT was previously activated and the condition for incoming_call_detected event is satisfied (see ST_INIT for conditions details).
- **EV_DIAL_ENDED** - Dialing initiated by table SEND_DEST_NUM is completed (last digit has been sent).
- **EV_ANI_NUM_DETECTED** - This action is used to inform the script file of a successful reception of the ANI digits string, or when timeout of digit waiting occurs. This is reported at the incoming call detected event, when the ANI flag is YES.
- **EV_FIRST_DIGIT** - Reception of first digit out of the incoming digit string. Used in the FXO protocols, where informing the script of receiving of the first digit, enables the script to use the SEND_PROG_TON function to stop the dial tone.

16.6 Function

The function column holds the name of the function to be activated when the action specified in the action/events field occurs. Select the functions from the list of eight functions defined in *CasSetup.h*. (e.g., START_COLLECT). When NONE is specified in this column, no function is executed.

16.7 Parameters

Table 16-2: CAS Parameters

Parameter #1	These columns are used as the function's parameters. The list of global parameters can be found in *CasSetup.h*. If a parameter is not essential, the parameter is marked **None**.
Parameter #2	
Parameter #3	

List of available user-functions and their parameters:

- **SET_TIMER (timer number, timeout) -** Set timers that are managed per B-channel, and their expiration triggers the state machine table. Each protocol table/state machine can use up to 8 timers per B-channel/call, (timeout in msec).
- **SEND_CAS (AB value, CD value) -** ABCD bits are sent as line signaling for the specific channel when the call is setup.
- **SEND_EVENT (event type, cause) -** The specific event type is sent to the host/user and retrieved by applying acGetEvent().
- **SEND_DEST_NUM -** Enbloc dialing: Enbloc dialing: refers to the digits string located in the acPSTNPlaceCall function. Three types are available: (1) DestPhoneNum (2) InterExchangePrefixNum (3) SourcePhoneNum.
- **DEL_TIMER (timer number) -** Delete specific or all timers (0 for all) for the B-channel.
- **START_COLLECT -** Initiates the collection of address information i.e. the dialed (destination) number for incoming calls where appropriate according to the protocol. At the time between START_COLLECT and STOP_COLLECT, no digit is reported to the user (EV_DIGIT is blocked) and the destination number is reported in the EV_INCOMING_CALL_DETECTED event.

- **STOP_COLLECT -** See START_COLLECT.
- **SET_COUNTER (counter number, counter value or NONE) -** Set counters that are managed per B-channel and their expiration triggers the state machine. The counter initialization value should be a non-negative number. To delete all timers, perform this function with 0 in the counter number field.
- **DEC_COUNTER (counter number) -** Decreases counter value by 1. When the counter value reaches 0, EV_COUNTERx_EXPIRES is sent to the table (The x represent the counter number).
- **SEND_MF (MF type, MF digit or index or NONE, MF sending time) -** This function is used only with MFC/R2 protocols.

The Channel Parameter structure contains three parameters regarding sending digits.

1. **AddressVector and ANIDigitVector** - These parameters are initialized when using a PlaceCall function. When the code reaches the dialing section, it sends MF digit according to the MF type specified in the MF type cell (the types are defined in *CASSetup.h* file):
   - **ADDRESS** - Sends the digit from the address vector (destination number) according to the index requested. (Refer to the Index definition).
   - **ANI** - Sends the digit from the ANI vector (source number) according to the index requested.
   - **SPECIFIC** - Sends the MF digit specified in the Parameter #2 rubric.
   - **SOURCE_CATEGORY** - Sends the pre-defined source category MF digit. The source category digit is set as the SourceNumberingType parameter when using a PlaceCall function. The second and third parameters have no use when using this type.
   - **TRANSFER_CAPABILITY** - Send the pre-defined line category MF digit. The line category digit is set as the TransferCapability parameter when using a PlaceCall function. The second and third parameters have no use when using this type.
2. **Index -** Specifies the Offset of the next digit to be sent from the vector (ADDRESS or ANI types described above):
   - **Index 1** - Used to send the next digit in the vector.
   - **Index -n** - Used to send the last **n** digit. Underflow can occur if n is greater than the number of digits sent so far.
   - **Index 0** - Used to send the last sent digit.
   - **Index SEND_FIRST_DIGIT** - Used to start sending the digits vector from the beginning.
   - (Refer to *CASSetup.h*.)
3. **MF Send Time** - This send time parameter specifies the maximum transmission time of the MF.
   - **STOP_SEND_MF** - Stops sending the current MF.
   - **SEND_PROG_TON** - Operation, Tone or NONE.

   - Two operations are available.
     - Sends the Call Progress Tone specified in the Parameter #2 rubric (The second parameter can be taken from *CASsetup.h*).
     - Stops sending the last parameter.

- **CHANGE_COLLECT_TYPE** (Collect Type) - Used only in MFCR2 protocol by the incoming user to indicate his waiting for the reception of the MF digit of the requested type. The type can be one of the following:
- **ADDRESS** - The user is waiting for the reception of address digits.
- **ANI** - The user is waiting for the reception of ANI digits.
- **SOURCE_CATEGORY** - The user is waiting for the reception of the source category.
- **TRANSFER_CAPABILITY** - The user is waiting for the reception of the source transfer capability (line category).

16.8 Next State

The Next State column contains the next state the table moves to after executing the function for that action/event line. When the user selects to stay in the same state, insert NO_STATE or use the current state.

Note the difference between NO_STATE and the current state name in this field. If the user selects to stay in the same current state, the unconditional actions (FUNCTION0) at the beginning of the state are performed. In contrast, NO_STATE skips these functions and waits for another action to come.

Reserved word "DO" must be written in the next state field if the unconditional actions (FUNCTION0) at the beginning of the state are used.

16.9 Changing the Script File

16.9.1 General

- CAS bouncing is filtered globally for each received CAS for each channel. The User defines the time for the filtering criteria in the protocol table file (see INIT_DEBOUNCE), and this is above the bouncing in the DSP detection of 30 msec.
- ANI/CLI is enabled using ST_INIT ANI parameter with 'YES'. ANI/CLI is supported using EV_ANI_NUM_DETECTED as the table action for collecting the ANI number in an incoming call. For outgoing calls, the table's function SEND_DEST_NUM with ANI parameter I initiates ANI dialing. The ANI number is provided by the User in the Source phone number parameter of acPSTNPlaceCall().

16.9.2 MFC R2 protocol

- Use the SEND_MF script function to generate the outgoing call destination number. In this case, the first parameter should be ADDRESS (or ANI for source phone number) and the second parameter -3 to 1 (+1), indicating which digit is sent out of the number that the string conveyed by the User in the acPSTNPlaceCall().
- (+1) implies sending of next digit, 0 implies repeat of last digit, and -1 implies last but one digit. This parameter actually changes the pointer to the phone number string of digits. Thus, a one-to-one mapping with the MF backward signals of the R2 protocol exists.
- Using the parameter SEND_FIRST_DIGIT initiates resending the string from the beginning, (change the pointer back to first digit and then proceed as above). This parameter is defined in CASSetup.h.

- When MFC/R2 protocol is used, the two detectors (opened by default) are the Call Progress Tones and MFC/R2 Forward MF. When the User invokes outgoing call via acPSTNPlaceCall(), MFC/R2 Forward MF detector is replaced with MFC/R2 Backward MF detector, since only two detectors per DSP channel are permitted to operate simultaneously.
- The correct MF is automatically generated according to the call direction - Forward for outgoing calls and Backward for incoming calls.
- MFC/R2 protocol fault could cause a channel block. In this case, the script file provided by Nortel releases the call to enable the User to free the call resources and be notified about being in blocking state.
- START_COLLECT and STOP_COLLECT must be used in the script file for MF collecting both in outgoing and incoming calls. Warning: If this script function isn't used, the script gets stuck and forward\backward MF are not detected.
- The Ringback Call Progress Tone is translated to a unique event acEV_PSTN_ALERTING, since the Ringback tone is actually used in all Nortel protocols' state machines. All other Call Progress Tones are conveyed via the acEV_TONE_DETECTED, and retrieved by the User according to their type and index (note that the Ringback tone should be defined in the Call Progress Tones table with the relevant type in order to get this event).
- When the tone detection event is received, Users can perform any action. For example, if the event is received with BUSY tone indication, Users can invoke acPSTNDisconnectCall() to end the call.
- The MFR2 destination number is collected using: EXPECTED_NUM_OF_DIGITS_MINUS_1 parameter for SET_COUNTER that the User defines at UserProt_defines_R2_MF.h. The counter function is used to trigger the script file for the last-but-one received, after receiving the last digit, the script file (acting as the outgoing register) initiates the A6/A3 FWD MF. Normally variant supports end of digit information (MF15) or silence at the end of the dialing (when MF15 is not used), a short pulse of MF3 (A3) is sent to indicate that the entire string of digits (according to Q442, 476) is received.
- Sending Group B digit by an incoming register requires invoking acCASAcceptCall() with a certain reason parameter. Six reason parameters are available:
- **CALLED_IDLE** - Subscribers line is free. Continue the call sequence. Usually should be followed by accept or reject.

1. **CALLED_BUSY** - Subscriber line is busy. Perform disconnect procedures.
2. **CALLED_CONGESTION** - Congestion encountered. Perform disconnect procedures.
3. **CALLED_UNALLOCATED** - Dial number was not allocated. Perform disconnect procedures.
4. **CALLED_RESERVE1** - Reserved for additional group B (user additional requirements).
5. **CALLED_RESERVE2** - Reserved for additional group B (user additional requirements).

Each reason generates a specific action, defined by the User, who modifies the script file. The action is then used to generate/respond with a group B MF (free, busy, etc.).

- Transfer Capability - This parameter of acPSTNPlaceCAll() function is used by the outgoing register to generate the service nature of the originating equipment. In most variants (countries) this is the same as the Calling Subscriber Categories but in some countries it is different, such as in R2 china protocol, it is referred to as the KD (Group II) digit.

Note: This parameter only receives the MF values from the acTISDNTransferCapability enumerator. Choose the MF digit according to the service type that should be sent.

- Source Category - This parameter of acPSTNPlaceCall() function determines the calling subscriber category. For example: subscriber with priority, subscriber without priority etc. This parameter is usually sent as part of the Group II forward digits (except for R2 china where it is sent as the KA digit using Group I forward digits).

Note: Applicable only to MFC-R2 protocol type.

Reader's Notes

17 Appendix - Security

This appendix describes the MG 3200's implementation of security protocols.

The following list specifies the available security protocols and their purposes:

- **IPSec**
- **IKE**

The IPSec and IKE protocols are part of the IETF standards for security issues. IPSec and IKE are used together on the media gateway to provide security for control and management protocols. The IPSec protocol is responsible for securing the data streams. The IKE protocol (Internet Key Exchange) is responsible for obtaining the IPSec encryption keys and encryption profile (known as IPSec Security Association). IPSec is used by MG 3200 to assure confidentiality, authentication and integrity for the following media types:

- Control traffic, such as H.248
- Management traffic, such as SNMP and HTTP

Note: Some Security features are optional and can be ordered or upgraded at a future time.

Note: The RTP and RTCP streams cannot be secured by IPSec.

Important

Using IPSec reduces the channel capacity of the MG 3200.

- **SSL/TLS** - Secures Web access (HTTPS) and Telnet access.
- **RADIUS** - Is utilized by the Embedded Web Server and Telnet server for authentication.
- **Media Security** - Allows encryption of voice traffic on the IP network.

This section also contains network port usage information (useful for firewall administrators) and recommended practices for keeping your network secure.

17.1 IPSec and IKE

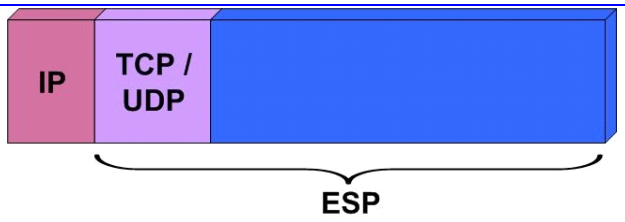
IPSec 'FOOTNOTE-IPSec and IKE'[1] and IKE protocols are part of the IETF standards for establishing a secured IP connection between two applications (also referred to as peers). Providing security services at the IP layer, IPSec and IKE are transparent to IP applications.

[1] FOOTNOTE@IPSec and IKE - ALL NOT MP / M1KUsing IPSec reduces the channel capacity of the MG 3200 by 24 channels.

IPSec and IKE are used in conjunction to provide security for control and management (e.g., SNMP and Web) protocols but not for media (i.e., RTP, RTCP and T.38).

IPSec is responsible for securing the IP traffic. This is accomplished by using the Encapsulation Security Payload (ESP) protocol to encrypt the IP payload (illustrated in the figure below). The IKE protocol is responsible for obtaining the IPSec encryption keys and encryption profile (known as IPSec Security Association (SA)).

Figure 17-1: IPSec Encryption



17.1.1 IKE

IKE is used to obtain the Security Associations (SA) between peers (the gateway and the application it's trying to contact). The SA contains the encryption keys and profile used by the IPSec to encrypt the IP stream. The IKE table lists the IKE peers with which the gateway performs the IKE negotiation (up to 20 peers are available).

The IKE negotiation is separated into two phases: main mode and quick mode. The main mode employs the Diffie-Hellman (DH) protocol to obtain an encryption key (without any prior keys), and uses a pre-shared key to authenticate the peers. The created channel secures the messages of the following phase (quick mode) in which the IPSec SA properties are negotiated.

The IKE negotiation is as follows:

- Main mode (the main mode creates a secured channel for the quick mode)
  - SA negotiation – The peers negotiate their capabilities using four proposals. Each proposal includes three parameters: Encryption method, Authentication protocol and the length of the key created by the DH protocol. The key's lifetime is also negotiated in this stage. For detailed information on configuring the four-main mode proposals, refer to 'IKE Configuration' on page 321.
  - Key exchange (DH) – The DH protocol is used to create a phase-1 key.
  - Authentication – The two peers authenticate one another using the pre-shared key (configured by the parameter 'IKEPolicySharedKey').
- Quick mode (quick mode negotiation is secured by the phase-1 SA)
  - SA negotiation – The peers negotiate their capabilities using four proposals. Each proposal includes two parameters: Encryption method and Authentication protocol. The lifetime is also negotiated in this stage. For detailed information on configuring the four-quick mode proposals, refer to the SPD table under 'IPSec Configuration' on page 321.
  - Key exchange – a symmetrical key is created using the negotiated SA.

IKE Specifications:

- Authentication mode - pre-shared key only
- Main mode is supported for IKE Phase 1
- Supported IKE SA encryption algorithms - DES and 3DES
- Hash types for IKE SA - SHA1 and MD5

17.1.2 IPSec

IPSec is responsible for encrypting and decrypting the IP streams.

The IPSec Security Policy Database (SPD) table defines up to 20 IP peers to which the IPSec security is applied. IPSec can be applied to all packets designated to a specific IP address or to a specific IP address, port (source or destination) and protocol type.

Each outgoing packet is analyzed and compared to the SPD table. The packet's destination IP address (and optionally, destination port, source port and protocol type) are compared to each entry in the table. If a match is found, the gateway checks if an SA already exists for this entry. If it doesn't, the IKE protocol is invoked (refer to Section 1.1.1 above) and an IPSec SA is established. The packet is encrypted and transmitted. If a match isn't found, the packet is transmitted un-encrypted.

Note: An incoming packet whose parameters match one of the entries of the SPD table but is received un-encrypted, is dropped.

IPSec Specifications:

- Transport mode only
- Encapsulation Security Payload (ESP) only
- Support for Cipher Block Chaining (CBC)
- Supported IPSec SA encryption algorithms - DES and 3DES
- Hash types for IPSec SA are SHA1 and MD5

17.1.3 Configuring the IPSec and IKE

To enable IPSec and IKE on the MG 3200 set the *ini* file parameter 'EnableIPSec' to 1. Note that when this parameter is defined, even if no table entries exist, the MG 3200 channel capacity is reduced (by 24 channels).

17.1.3.1 IKE Configuration

The parameters described in the table below are used to configure the first phase (main mode) of the IKE negotiation for a specific peer. A different set of parameters can be configured for each of the 20 available peers.

17.1.3.2 IPSec Configuration

The parameters described in the table below are used to configure the SPD table. A different set of parameters can be configured for each of the 20 available IP destinations.

17.1.3.3 IPSec and IKE Configuration Table's Confidentiality

Since the pre-shared key parameter of the IKE table must remain undisclosed, measures are taken by the MG 3200 *ini* file, Embedded Web Server and SNMP agent to maintain this parameter's confidentiality. On the Embedded Web Server a list of asterisks is displayed instead of the pre-shared key. On SNMP, the pre-shared key parameter is a write-only parameter and cannot be read. In the *ini* file, the following measures to assure the secrecy of the IPSec and IKE tables are taken:

- **Hidden IPSec and IKE tables -** When uploading the *ini* file from the gateway the IPSec and IKE tables are not available. Instead, the notifications (shown in the example below) are displayed. The following is an example of an *ini* File Notification of Missing Tables.

```
;
;  *** TABLE IPSEC_IKEDB_TABLE ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts
;

;
;  *** TABLE IPSEC_SPD_TABLE ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts
;
```

- **Preserving the values of the parameters in the IPSec and IKE tables from one ini file loading to the next** – The values configured for the parameters in the IPSec tables in the *ini* file are preserved from one loading to another. If a newly loaded *ini* file doesn't define IPSec tables, the previously loaded tables remain valid. To invalidate a previously loaded *ini* file's IPSec tables, load a new *ini* file with an empty IPSec table.

17.2 SSL/TLS

SSL (the Secure Socket Layer), also known as TLS (Transport Layer Security), is the method used to secure the MG 3200's Embedded Web Server and Telnet server. The SSL protocol provides confidentiality, integrity and authenticity of the Web server.

Specifications for the SSL/TLS implementation:

- Supported transports: SSL 2.0, SSL 3.0, TLS 1.0
- Supported ciphers: DES, RC4 compatible
- Authentication: X.509 certificates; CRLs are not supported

17.2.1 Web Server Configuration

For additional security, you can configure the Web server to accept only secure (HTTPS) connections. This is done by changing the *ini* file parameter, HTTPS Only or via the Embedded Web Server, Network Settings screen (refer to "Network Settings" on page 154). You can also change the port number used for the secure Web server (by default 443) by changing the *ini* file parameter, HTTPSPort.

17.2.2 Using the Secure Web Server

➢ To use the secure Web server, take these 3 Steps:

1. Navigate your browser to the following URL:

https://[*hostname[or [ip address]*

Depending on the browser's configuration, a security warning dialog may be displayed. The reason for the warning is that the MG 3200's initial certificate is not trusted by your PC. The browser may allow you to install the certificate, thus skipping the warning dialog the next time you connect to the MG 3200

2. If you are using Internet Explorer, click **View Certificate** and then **Install Certificate**.

3. The browser also warns you if the host name used in the URL is not identical to the one listed in the certificate. To overcome this, add the IP address and host name (ACL_nnnnnn where nnnnnn is the serial number of the MG 3200) to your hosts file, located at /etc/hosts on UNIX or C:\WINDOWS\SYSTEM32\DRIVERS\ETC\hosts on Windows; then use the host name in the URL, e.g., https://ACL_280152 .Below is an example of a host file:

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# Location: C:\WINDOWS\SYSTEM32\DRIVERS\ETC\hosts
#
127.0.0.1    localhost
10.31.4.47   ACL 280152
```

17.2.3 Secure Telnet

The MG 3200 has an embedded Telnet server allowing easy command-line access to the device configuration and management interface. The Telnet server is disabled by default. To enable it, set the parameter, TELNETServerEnable to 1 (standard mode) or 2 (SSL mode).

No information is transmitted in the clear when using SSL mode.

If the Telnet server is set to SSL mode, a special Telnet client is required on your PC to connect to the Telnet interface over a secure connection; examples include C-Kermit for UNIX, Kermit-95 for Windows, and the acSSLTelnet utility for Windows (which requires prior installation of the free OpenSSL toolkit).

17.2.4 Server Certificate Replacement

The MG 3200 is shipped with a working SSL configuration consisting of a unique self-signed server certificate. When a MG 3200 is upgraded to firmware version 4.6, a unique self-signed server certificate is created. If an organizational PKI (public key infrastructure) is in place, you may wish to replace this certificate with one provided by your security administrator.

➢ To replace this certificate, take these 9 steps:

1. Your network administrator should allocate a unique DNS name for the MG 3200 (e.g., dns_name.corp.customer.com). This name is used to access the device, and should therefore be listed in the server certificate.
2. Navigate your browser to the following URL (case-sensitive):

'https://dns_name.corp.customer.com/SSLCertificateSR'
https://dns_name.corp.customer.com/sslcertificatesr

Note that you should use the DNS name provided by your network administrator. The Certificate Signing Request Web page is displayed.

3. Enter the DNS name as the certificate subject (in the input box), and click **Generate CSR**. The Web page displays a textual certificate signing request, which contains the SSL device identifier
4. Copy this text and send it to your security provider.

The security provider (also known as Certification Authority or CA) signs this request and send you a server certificate for the device.

5. Save the certificate in a file (e.g., cert.txt) and make sure it is a plain-text file with the "BEGIN CERTIFICATE" header. Below is an example of a Base64-Encoded X.509 Certificate.

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJG
UjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBTZXJ2
ZXVyMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMC
RlIxEzARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2Vy
dmV1cjCCASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkCggEAPqd4MziR4spWldGR
x8bQrhZkonWnNm+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qI
JcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lR
efiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwv
REXfFcUW+w==
-----END CERTIFICATE-----
```

6. Before continuing, set the parameter, HTTPSOnly = 0 to make sure you have a method of accessing the device in case the new certificate is not working. Restore the previous setting after testing the configuration.
7. In the SSLCertificateSR Web page, locate the server certificate upload section.
8. Click **Browse** and locate the *cert.txt* file, then click **Send File**.
9. When the operation is complete, save the configuration and restart the device. The Web server now uses the provided certificate.

Note 1: The certificate replacement process may be repeated as necessary, e.g., when the new certificate expires.

Note 2: It is possible to set the subject name to the IP address of the device (e.g., "10.3.3.1") instead of a qualified DNS name. This practice is not recommended, since the IP address is subject to changes and may not uniquely identify the device.

17.2.5 Client Certificates

By default, Web servers using SSL provide one-way authentication. The client is certain that the information provided by the Web server is authentic. When an organizational PKI is in place, two-way authentication may be desired: both client and server should be authenticated using X.509 certificates. This is achieved by installing a client certificate on the management PC, and uploading the same certificate (in base64-encoded X.509 format) to the MG 3200's Trusted Root Certificate Store. The Trusted Root Certificate file should contain both the certificate of the authorized user, and the certificate of the CA.

Since X.509 certificates have an expiration date and time, the MG 3200 must be configured to use NTP (Network Time Protocol) to obtain the current date and time. Without a correct date and time, client certificates cannot work.

➢ To install a client certificate, take these 5 steps:

1. Before continuing, set HTTPSONLY=0 to make sure you have a method of accessing the device in case the client certificate is not working. Restore the previous setting after testing the configuration.
2. To upload the Trusted Root Certificate file, go to the SSLCertificateSR Web page as above and locate the trusted root certificate upload section.
3. Click **Browse** and locate the file, then click **Send File**.
4. When the operation is complete, set the *ini* file parameter, HTTPSRequireClientCertificates = 1.
5. Save the configuration and restart the device.

   When a user connects to the secure Web server:

   - If the user has a client certificate from a CA listed in the Trusted Root Certificate file, the connection is accepted and the user is prompted for the system password.
   - If both the CA certificate and the client certificate appear in the Trusted Root Certificate file, the user is not prompted for a password (thus providing a single-sign-on experience - the authentication is performed using the X.509 digital signature).
   - If the user does not have a client certificate from a listed CA, or does not have a client certificate at all, the connection is rejected.

Note : The process of installing a client certificate on your PC is beyond the scope of this document. For more information, refer to your Web browser or operating system documentation, and/or consult your security administrator.

17.3 RADIUS Support

To connect to the Embedded Web Server or Telnet server, the user must provide a valid name and password. While the device supports only a single system password, it is possible to enhance login security using a RADIUS server. RADIUS (RFC 2865) is a standard protocol for authentication, which defines a method for contacting a predefined server and verifying a given name and password pair against a remote database, in a secure manner.

17.3.1 Setting Up a RADIUS Server

A free RADIUS server implementation can be downloaded from' http://www.freeradius.org' http://www.freeradius.org. Follow the directions on that site for information on installing and configuring the server. If you use a RADIUS server from a different vendor, refer to the appropriate documentation.

➢ To set up a RADIUS server, take these 4 steps:

1. Define the MG 3200 as an authorized client of the RADIUS server, with a predefined "shared secret" - a password used to secure communication. Below is an example of a clients.conf file (FreeRADIUS client configuration).

```
#
# clients.conf - client configuration directives
#
client 10.31.4.47 {
        secret          = FutureRADIUS
        shortname       = TP-1610 name
}
```

2. Define the users authorized to use the MG 3200 on the server, using one of the password authentication methods supported by the server implementation. The following example shows a user configuration file for FreeRADIUS using a plain-text password.

```
# users - local user configuration database

john    Auth-Type := Local, User-Password == "qwerty"
        Service-Type = Login-User

larry   Auth-Type := Local, User-Password == "123456"
        Service-Type = Login-User
```

3. Make sure you have the IP address and port number used by the RADIUS server, and the configured "shared secret".
4. Go to "Configuring RADIUS Support" on page 327.

17.3.2 Configuring RADIUS Support

➢ To configure RADIUS support on the MG 3200 via the Embedded Web Server, take these 7 steps:

1. In the Embedded Web Server, from the Advanced Configuration screen, select the **Network Settings** from the sub-menu bar on the top (Refer to "Network Settings" on page 154).
2. Locate the **RADIUS settings** section.
3. Fill in the RADIUS server IP address, port number and shared secret.
4. Set **Enable RADIUS access control** to **Enable**.
5. Set **Use RADIUS for Web/Telnet login** to **Enable**.
6. Set **Require secure Web connection (HTTPS)** to **Enable (HTTPS Only)**.

   It is important that you use HTTPS (secure Web server) if connecting to the device over an open network, since the password must be transmitted in clear text over the network. Similarly, if using Telnet, make sure you use SSL mode (TELNETSERVERENABLE=2).
7. Save the configuration and restart the device. When you connect to the Web server or Telnet interface, use the name and password configured in the RADIUS database. The old system password is still active, and may be used if the RADIUS server is down.

➢ To configure RADIUS support on the MG 3200 using the ini file, take these 3 steps:

1. Open the *ini* file in any text editor.
2. Add the following lines to the *ini* file:
   - ENABLERADIUS = 1
   - WEBRADIUSLOGIN = 1
   - RADIUSAuthServerIP = *IP address of RADIUS server*
   - RADIUSAuthPort = *port number of RADIUS server, usually 1812*
   - SHAREDSECRET = *'your shared secret'*
   - HTTPSONLY = 1
3. Save the configuration and restart the device. When you connect to the Telnet interface, use the name and password configured in the RADIUS database. The old system password is still active, and may be used if the RADIUS server is down.

17.4 Network Port Usage

The following table lists the default TCP/UDP network port numbers used by the MG 3200. Where relevant, the table lists the *ini* file parameters that control the port usage and provide source IP address filtering capabilities.

Table 17-1: Default TCP/UDP Network Port Numbers

Port number	Peer port	Application	Notes
2	2	Debugging interface	Always ignored
4	4	EtherDiscover	Open only on unconfigured devices
23	-	Telnet	Disabled by default (TELNETSERVERENABLE). Configurable (TELNETSERVERPORT), access controlled by TELNETSERVERAUTHORIZEDADDRESS
68	67	DHCP	Active only if DHCPENABLE=1
80	-	Web server (HTTP)	Configurable (HTTPPORT), may be disabled (DISABLEWEBTASK or HTTPSONLY). Access controlled by WEBACCESSLIST
161	-	SNMP GET/SET	Configurable (SNMPPORT), may be disabled (DISABLESNMP). Access controlled by SNMPTRUSTEDMGR
443	-	Web server (HTTPS)	Configurable (HTTPSPORT), may be disabled (DISABLEWEBTASK). Access controlled by WEBACCESSLIST
500	-	IPSec IKE	May be disabled (ENABLEIPSEC)
2422	2422	TPM LinkLayer	Used for internal synchronization between the two TPMs on a board
2423-2424	2423 and up	TPNCP	Proprietary control protocol. N/A
2427	2427	MGCP / H.248	Configurable (GATEWAYMGCPPORT), Access controlled by PROVISIONEDCALLAGENTS and MEGACOCHECKLEGALITYOFMGC
4000, 4010 and up	-	RTP traffic	Base port number configurable (BASEUDPPORT), fixed increments of 10. The number of ports used depends on the channel capacity of the device.
4001, 4011 and up	-	RTCP traffic	Always adjacent to the RTP port number
4002, 4012 and up	-	T.38 traffic	Always adjacent to the RTCP port number
32767	-	SCTP	If SCTP/IUA is available on the device

Table 17-1: Default TCP/UDP Network Port Numbers

Port number	Peer port	Application	Notes
(random) > 32767	514	Syslog	May be disabled (ENABLESYSLOG).
(random) > 32767	-	Syslog ICMP	May be disabled (ENABLESYSLOG).
(random) > 32767	-	ARP listener	
(random) > 32767	162	SNMP Traps	May be disabled (DISABLESNMP)
(random) > 32767	-	DNS client	

17.5 Media Security

The MG 3200 supports media encryption via TGCP (PacketCable extensions to the MGCP protocol). With media security, IP voice traffic for some or all channels is encrypted using predefined session keys. No key negotiation is performed for media security. Instead, the MG 3200 assumes higher-level protocols handle key management.

Encryption specifications:

- AES (Rijndael) cipher algorithm, in CBC mode
- Key strength - 128 bit

Note: Using media security reduces the channel capacity of the device.

17.6 Recommended Practices

To improve network security, the following guidelines are recommended when configuring the MG 3200:

- Set the management password to a unique, hard-to-guess string. Do not use the same password for several devices, as a compromise of one may lead to the compromise of others. Keep this password safe at all times, and change it frequently.
- If possible, use a RADIUS server for authentication. RADIUS allows you to set different passwords for different users of the MG 3200, with centralized management of the password database. Both Web and Telnet interfaces support RADIUS authentication.
- Use IPSec to secure traffic to all management and control hosts. Since IPSec encrypts all traffic, hackers cannot capture sensitive data transmitted on the network, and malicious intrusions are severely limited.
- Use HTTPS when accessing the Web interface. Set HTTPSONLY=1 to allow only HTTPS traffic (and block port 80). If you don't need the Web interface, disable the Web server.
- If you use Telnet, do not use the default port (23). Use SSL mode to protect Telnet traffic from network sniffing.

- If you use SNMP, do not leave the community strings at their default values, as they can be easily discovered by hackers. See the SNMP configuration chapter for further details.
- Use a firewall to protect your VoIP network from external attacks. Robustness of the network may be compromised if the network is exposed to "denial of service" (DoS) attacks; such attacks are mitigated by stateful firewalls. Do not allow unauthorized traffic to reach the MG 3200.

17.7 Legal Notice

By default, the MG 3200 supports export-grade (40-bit and 56-bit) encryption, due to U.S. government restrictions on the export of security technologies. To enable 128-bit and 256-bit encryption on your device, contact your Nortel representative.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. ('http://www.openssl.org/' http://www.openssl.org/)

This product includes cryptographic software written by Eric Young' (eay@cryptsoft.com mail to: eay@cryptsoft.com).

18 Appendix - ISDN Signaling Gateway Functionality

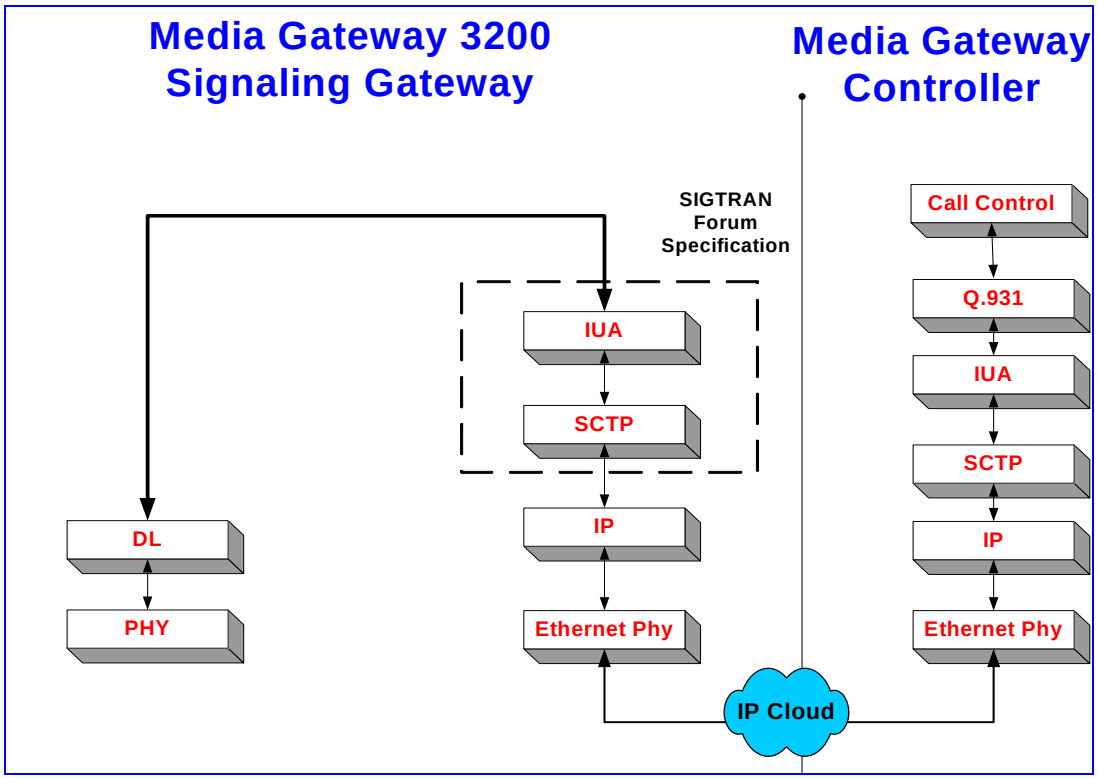
The Media Gateway 3200 supports the relay of ISDN signaling messages using SIGTRAN IUA and SCTP protocols (refer to Figure 18-1).

18.1 IUA (ISDN User Adaptation)

A signaling message entering the device from the ISDN connection goes through the Data Link Layer. The Q.931 PDU is then relayed to the Media Gateway Controller using IUA over SCTP over IP. The Media Gateway Controller (MGC) supports SCTP and IUA layers and then completes the upper signaling layers of Figure 18-1.

18.1.1 IUA Signaling Messages

Figure 18-1: ISDN Signaling Messages



18.1.2 Configuring SIGTRAN IUA

Use *ini* file parameter values to configure an IUA connection.

Table 18-1: SIGTRAN IUA Configuration Parameters

ini File Field Name (X is the Trunk)	Valid Range	Description
IUAINTERFACEID_X	Unsigned Integer	IUA Interface ID
ProtocolType_X	acPROTOCOL_TYPE_T1_IUA = 28 or: acPROTOCOL_TYPE_E1_IUA = 29	IUA PSTN protocol type causes the IUA layer to be above the DL layer.

18.1.3 Support for IUA behind NAT

To be able to support IUA signaling gateway functionality behind a NAT, the signaling gateway must initiate SCTP (by sending an SCTP init to the MGC side). After an SCTP association is established, the Signaling Gateway waits for ASP commands from the MGC. This is performed via a new configuration of the following line in the SS7_SIG_IF_GROUP table. To configure the connection of an IUA behind an NAT, refer to the following example.

Please add the following lines to your INI file: Change the IP in red to your MGC IP address.

[SS7_SIG_IF_GROUP_TABLE]

FORMAT SS7_SIG_IF_GR_INDEX = SS7_IF_GR_ID,SS7_SIG_SG_MGC, SS7_SIG_LAYER, SS7_SIG_TRAF_MODE, SS7_SIG_T_REC, SS7_SIG_T_ACK, SS7_SIG_T_HB, SS7_SIG_MIN_ASP, SS7_SIG_BEHAVIOUR, SS7_LOCAL_SCTP_PORT, SS7_SIG_NETWORK, SS7_DEST_SCTP_PORT, SS7_DEST_IP, SS7_MGC_MX_IN_STREAM, SS7_MGC_NUM_OUT_STREAM;

SS7_SIG_IF_GROUP_TABLE 1 = 1,1, 1, 1, 2000, 2000, 30000, 1, 0, 9900, 1,9900,10.3.2.45,3,3;

Note: The two values 3,3 at the end of the entry of the SS7_SIG_IF_GROUP_TABLE parameter controls the number of in and out SCTP streams to open. This MUST be the number of E1/T1 ports + 1 at a minimum. The reason is because in RFC3057, Stream 0 is reserved for ASP/MGMT messages, and each E1/T1 uses a different stream.

Example: For an 8-port MG3200 communicating via NAPT, the values would be 9,9

[\SS7_SIG_IF_GROUP_TABLE]

SCTPHOSTNAME = ‘MG3200’

MEGACO_MID = 'MG3200'

Note: The SCTPHOSTNAME parameter must match the MEGACO_MID parameter which must match the gateway name provisioned on the CS2000 Management Tools and must only be used in NAPT configurations. The hostname is used to identify the gateway to the CS2000 since IP address cannot be used.

The value ‘MG3200’ in the example above is the provisioned gateway name on the CS2000 Management Tools.

18.2 DUA (DPNSS User Adaptation)

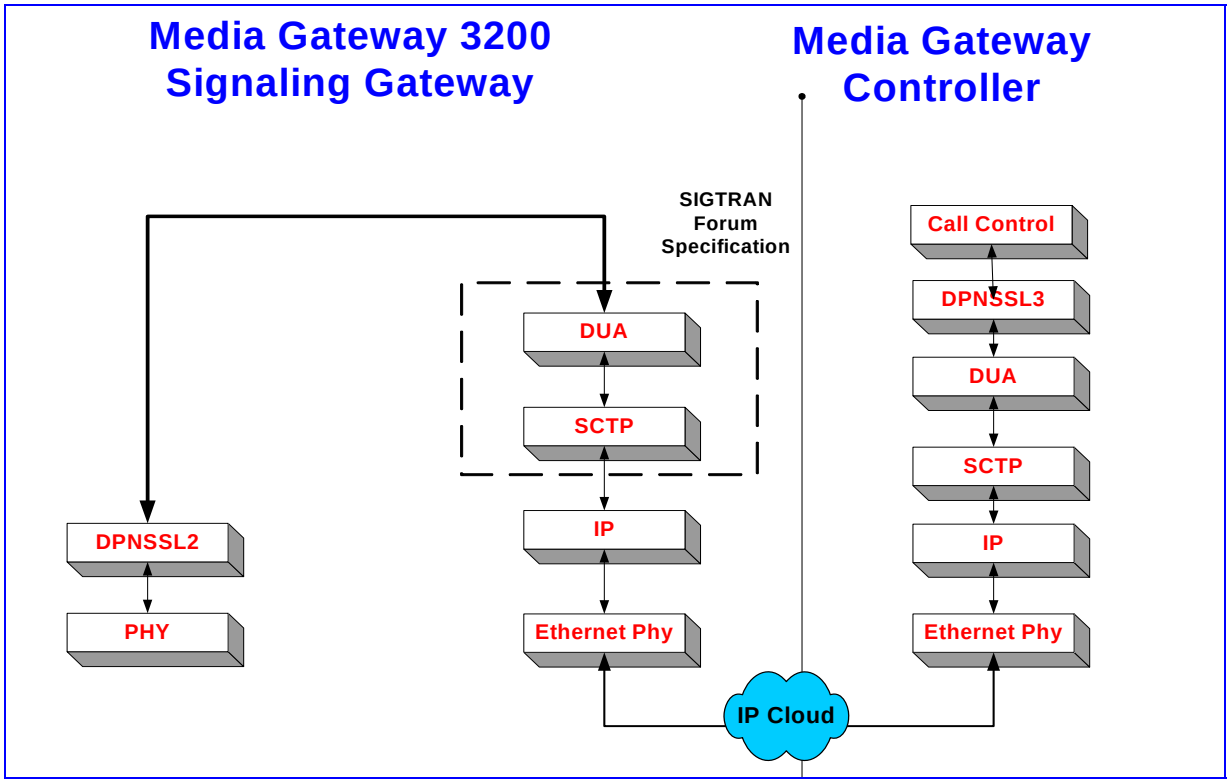
DUA is based on the draft-ietf-sigtran-dua-08 published by the IETF. Refer to https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=7506. It is implemented with BTNR 188 DPNSS Layer 2 (an early ISDN protocol in the U.K.; British Telecom Network Requirements). A signaling message entering the device from the DPNSSL2 connection goes through the Data Link Layer. A DPNSSL2 PDU is then relayed to the Media Gateway Controller using DUA over SCTP over IP. The Media Gateway Controller supports SCTP and DUA layers and then completes the upper signaling layers of Figure 18-2.

18.2.1 DPNSSL2 Protocol

1. The link layer can use 30 real channels; an additional 30 virtual channels can be used for services.
2. The link layer uses compelled signaling with Layer 2 on the far end.

18.2.2 DUA Signaling Messages

Figure 18-2: DPNSS Signaling Messages



18.2.3 Configuring SIGTRAN DUA

18.2.3.1 Configuring via the INI file

Use the *ini* file parameter values below to configure a DUA connection.

Table 18-2: SIGTRAN DUA Configuration Parameters

ini File Field Name (X is the Trunk)	Valid Range	Description
IUAINTERFACEID_X	Unsigned Integer	Used for the DUA Interface ID. (Note: Must be unique and match the value provisioned for the corresponding carrier on the Call Server Element Manager).
ProtocolType_X	acPROTOCOL_TYPE_E1_DUA = 37	DUA PSTN protocol type causes the DUA layer to be above the DPNSSL2 layer.
DPNSSBehaviour	Ulong	DPNSS behavior bit field for options implementation.

ini File Field Name (X is the Trunk)	Valid Range	Description
DPNSSNumRealChannels	Char - Valid range 1-30	Number of real B-channels used for voice. Default = 30.
DPNSSNumVirtualChannels	Char - Valid range 0-30	Number of virtual B-channels used for services. Default = 30.

18.2.3.1.1 DPNSSBehavior Bits Values

DPNSS_BEHAV_STOP_SABMR_AFTER_NL_AND_NT1 bit: (bit #0, bitmask 0x0001

when 1: DPNSS stops repeating SABMR after NL and NT1 limits are exceeded

when 0: DPNSS continues repeating SABMR after NL and NT1 limits are exceeded

Default is 0 (continue repeating SABMR).

DPNSS_BEHAV_FULL_STARTUP_SUCCESS bit: (bit #1, bitmask 0x0002)

when 1: the startup procedure is considered a SUCCESS only when ALL DLCs succeed to reset

when 0: the startup procedure is considered a SUCCESS as soon as 1 DLC succeed to reset

Default is 0: (only partial reset is considered a success).

DPNSS_BEHAV_DLC_OOS_AFTER_NL_AND_NT1 bit: (bit #2, bitmask 0x0004)

(Note: The current implementation is 'the DLC is declared OOS to the MGC after NL and NT1 limits are exceeded' regardless of bit setting).

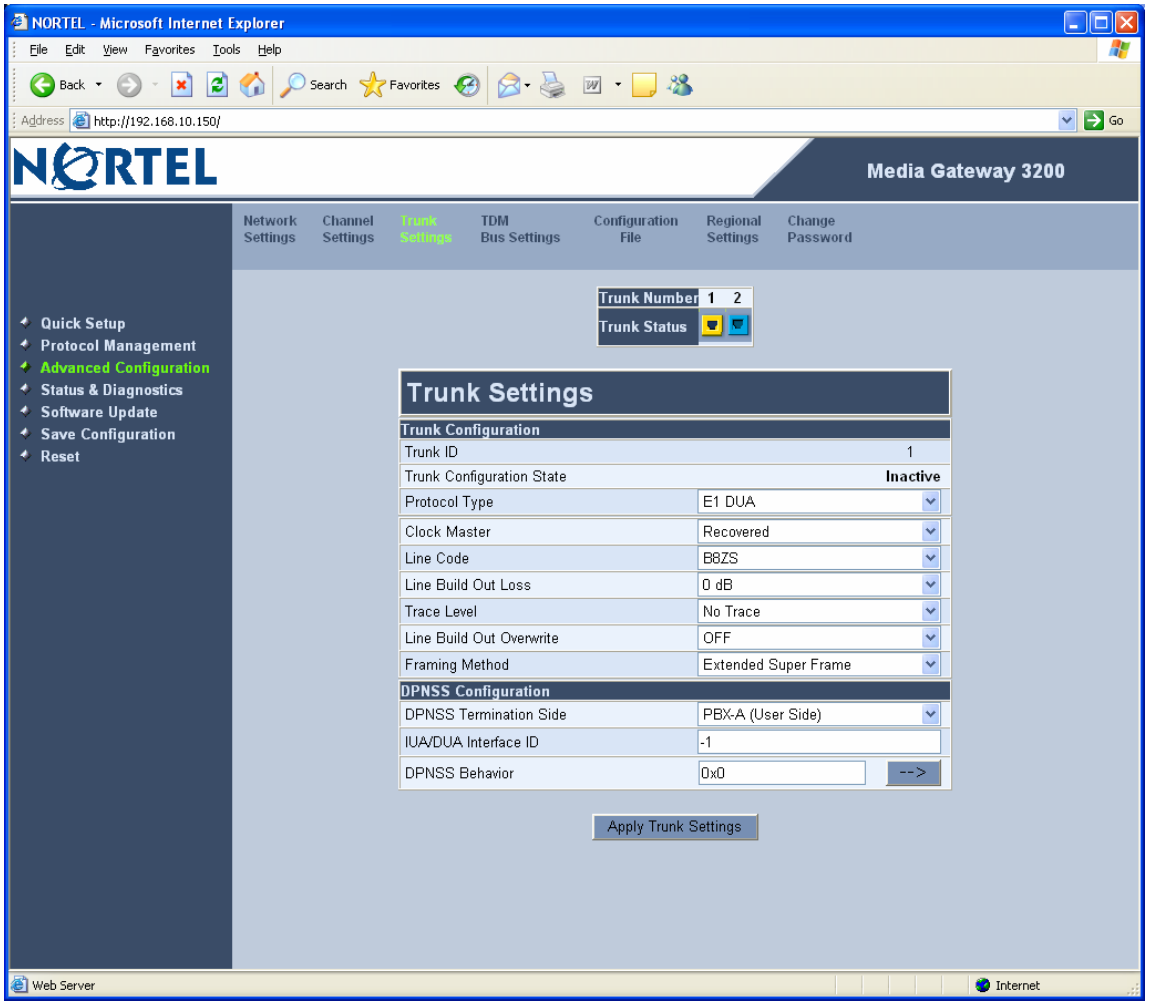
DPNSS_BEHAV_DLC_OOS_WHEN_L3_Q_FULL bit: (bit #3, bitmask 0x0008)

(Note: The current implementation is 'the DLC is declared OOS to the MGC when the L3 queue limit is exceeded' regardless of bit setting).

18.2.3.2 Configuring via the Web Interface

Login to the MG 3200 web server and select "Advanced Configuration" in the left hand pane. Then select "Trunk Settings" from the top menu. Select the trunk to be configured by clicking on the appropriate trunk status icon. Select "E1 DUA" as the protocol type and fill in the remaining fields according to the desired characteristics. See Figure 18-3 Trunk Settings Configuration Page

Figure 18-3 Trunk Settings Configuration Page



Refer to LTRT-72904 MG 3200 Configuration Guide Ver SN09 for guidelines of provisioning DUA configuration.

18.3 DUA Behind NAT Support

DUA uses the same IUA configuration. To configure a DUA behind NAT connection, refer to the example in Support for IUA behind NAT on page 332

19 Appendix - SS7 Configuration Guide

Several SS7 network elements are available. This section provides a brief description of each network element, and corresponding configuration description.

Part of the various network elements described below includes the use of SigTran (M2UA), as implemented in products such as MG 3200.

Note: please refer to the description of SS7 configuration parameters in Table of Parameter Value Constructs and in the Appendix, 'Table Parameters' on page 281.

19.1 SS7 Network Elements

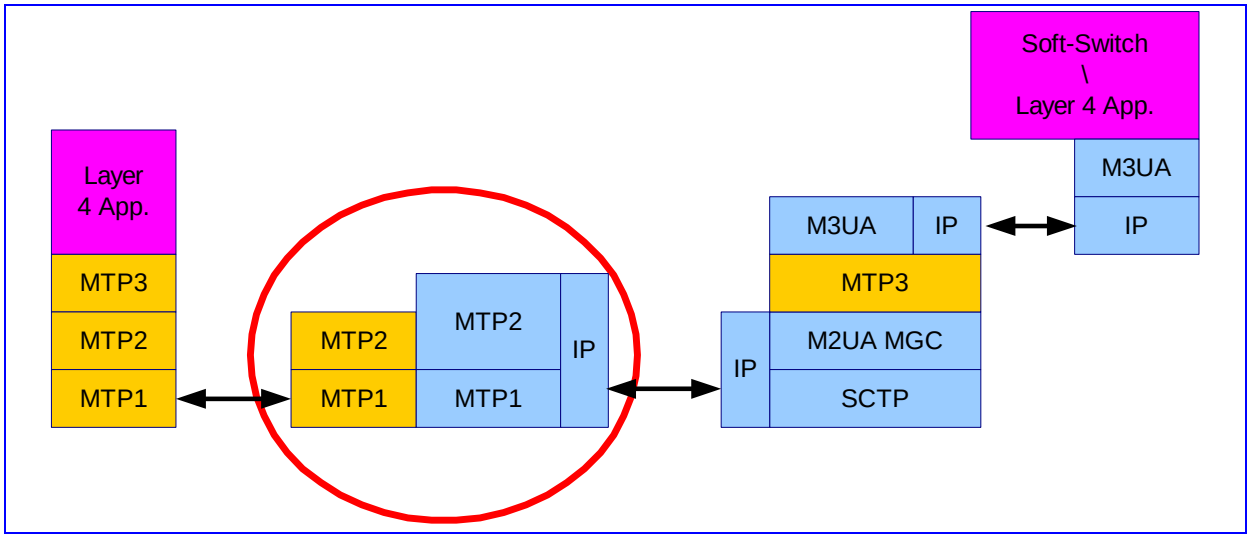
The SS7 network elements include 4 basic configurations:

- SS7 M2UA - SG Side
- SS7 M2UA – Media Gateway Controller Side
- SS7 MTP2 Tunneling

19.1.1 SS7 M2UA - SG Side

For the SS7 M2UA - SG side network element, the MTP2 link from the SS7 network side is sent via SCTP (IP) to Media-Gateway side.

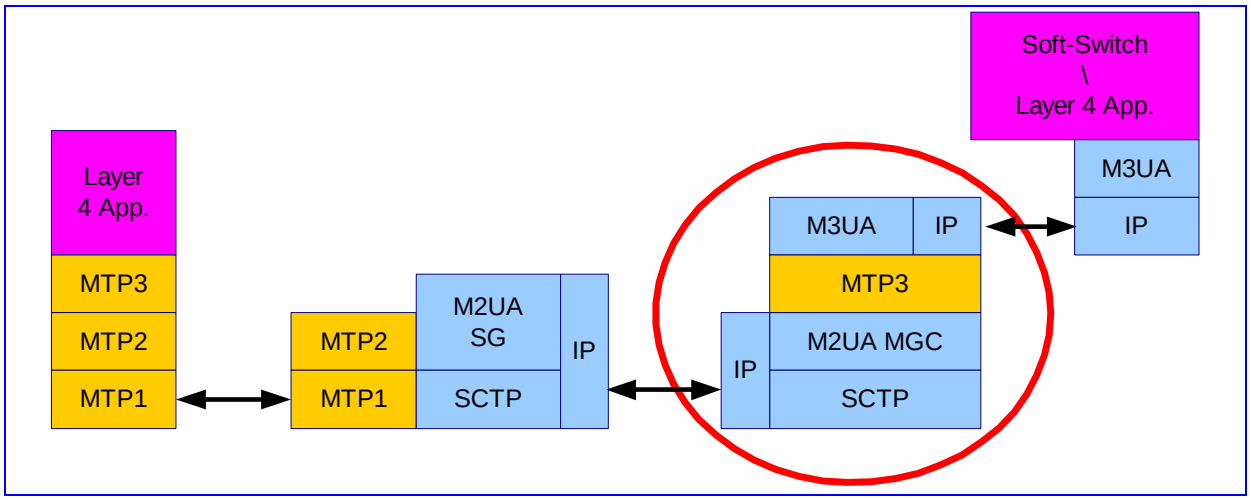
Figure 19-1: SS7 M2UA - SG Side



19.1.2 SS7 M2UA – Media Gateway Controller Side

For the SS7 M2UA – Media Gateway Controller side network element, the M2UA Media Gateway Controller link is from the IP side. MTP3 is supported in the board's software. The MTP3 payload is sent via M3UA to the Soft-Switch. (MTP3 can also route MSUs to other SS7 network elements via other links).

Figure 19-2: SS7 M2UA - MGC Side

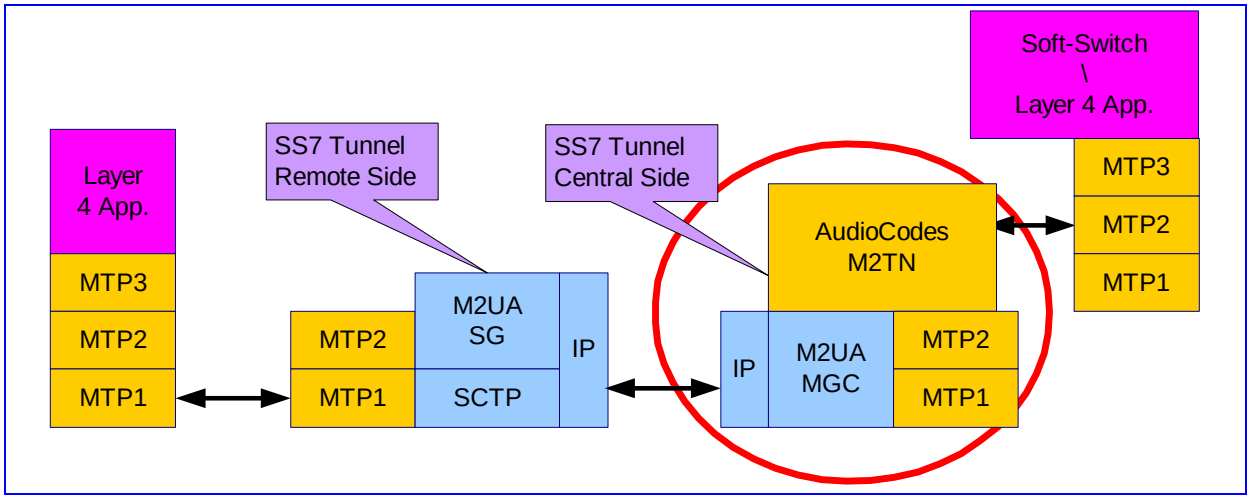


19.1.3 SS7 MTP2 Tunneling

For the SS7 MTP2 Tunneling configuration, the MTP2 SS7 link payload is sent across long distances (over the IP network). Both of its termination ends have SS7 MTP2 interfaces, which are unaware of the MTP2 Tunneling between them.

MTP2 Tunneling is a proprietary solution, based on SS7 and SigTran standards.

Figure 19-3: SS7 MTP2 Tunneling



19.1.4 Configuration Extensions:

In addition to the basic SS7 configurations described above, the extensions below provide more options:

1. 2 SS7 Nodes (SP/STP) can be configured per TPM
2. MTP3 supports mixed SS7 link types, i.e. one MTP3 signaling node can have few MTP2 links and a few M2UA links
3. Nodes can be configured as SP or STP
4. Supported SS7 variants: ITU-T, ANSI, CHINA
5. SS7 signaling links can be configured on any available timeslot of any trunk, so that several SS7 signaling links can be configured on one E1/T1
6. F-links are supported: any mixture of voice and signaling links can be configured on any trunk (providing that the trunk type supports SS7 signaling links - refer to the examples provided below).

19.1.5 Other dependencies in ini File:

Trunk Protocol Types

Trunks that carry SS7 Link(s) must be configured with protocol type: T1_TRANSPARENT=4, E1_TRANSPARENT31=5 or E1_TRANSPARENT30=6

19.2 Examples of SS7 ini Files

This section provides examples of *ini* files for each of the SS7 network elements described previously. Each example can be modified to fit the user's field configuration is accompanied by loading instructions for a testing/Lab mini-network environment.

19.2.1 SS7 M2UA - SG Side ini File Example

For the SS7 M2UA - SG Side ini file example, take into account the following notes:

- There are 4 SS7 links of type: MTP2->M2UA SG.
- There is 1 interface group (only 1 remote Media Gateway Controller).
- There are 4 interface IDs defined: 1 per link.
- This file is intended for ITU link variant (E1 trunks).

➢ To load the SS7 M2UA - SG Side ini file example, take these 2 steps:

1. This *ini* file is to be loaded on an MTP2 SG board. An MTP2 Media Gateway Controller board should be connected (over IP) to the MTP2 SG board.
2. Change the value of the SyslogServerIP parameter accordingly.

The following is an example of SS7 M2UA - SG Side *ini* File

```
[TDM BUS configuration]
```

```
; 1=aLaw  3=ulaw
PCMLawSelect=    1

; EXT BUS=5   H110=4   QSLAC=3   FRAMERS=2   SC BUS=1   MVIP BUS=0
TDMBusType=        2

; 0=2048kbps, 2=4096kbps, 3=8192kbps
TDMBusSpeed=   3

;1 - internal, 3 - mvip, 4 - Network, 8 - h110a, 9 - h110b, 10 -
Netref
TDMBUSCLOCKSOURCE= 1

[Trunk Configuration]

;e1 euro isdn=1 t1 isdn=2 ;e1 cas r2=8 (8 for fcd); e1 trans 62=5
ProtocolType = 5

TraceLevel   = 0

; acCLOCK MASTER ON =1
CLOCKMASTER= 1

;acUSER TERMINATION SIDE = 0
TerminationSide = 1

;acEXTENDED SUPER FRAME=0
FramingMethod = 0

;acB8ZS = 0   2 for E1 CAS - FCD
LineCode = 0

Q931RELAYMODE = 0

; 0=Internal Clock, 1=rx signal derived clk
PHYCLKSOURCE=0

[syslog]
SYSLOGSERVERIP = 168.100.0.1
ENABLESYSLOG = 1

WATCHDOGSTATUS = 0

[ SS7 LINK TABLE ]
FORMAT SS7 LINK INDEX = SS7 LINK NAME, SS7 LINK TRACE LEVEL,
SS7_LINK_ADMINISTRATIVE_STATE,SS7_LINK_L2_TYPE, SS7_LINK_L3_TYPE,
SS7 LINK TRUNK NUMBER,SS7 LINK TIMESLOT NUMBER,SS7 LINK M2UA IF ID,
SS 7 LINK GROUP ID;

SS7 LINK TABLE 0 = new link 0, 0, 2, 1, 1, 1, 15, 50, 4;
SS7 LINK TABLE 1 = new link 1, 0, 2, 1, 1, 2, 12, 12, 4;
SS7_LINK_TABLE 2 = new_link_2, 0, 2, 1, 1, 4,  7, 18, 4;
SS7 LINK TABLE 3 = new link 3, 0, 2, 1, 1, 5,  3,  1, 4;

[\SS7_LINK_TABLE]


[ SS7_SIG_IF_GROUP_TABLE ]
FORMAT SS7 SIG IF GR INDEX = SS7 IF GR ID,SS7 SIG SG MGC,
SS7 SIG LAYER, SS7 SIG TRAF MODE, SS7 SIG T REC, SS7 SIG T ACK,
SS7 SIG T HB, SS7 SIG MIN ASP, SS7 SIG BEHAVIOUR,
SS7 LOCAL SCTP PORT, SS7 SIG NETWORK;
SS7 SIG IF GROUP TABLE 4 =  4,83, 2, 1, 2000, 2000, 30000, 1, 0,
2904, 1;
[ \SS7 SIG IF GROUP TABLE ]
```

```
 [ SS7 SIG INT ID TABLE ]
FORMAT SS7 SIG IF ID INDEX = SS7 SIG IF ID VALUE,
SS7_SIG_IF_ID_NAME, SS7_SIG_IF_ID_OWNER_GROUP, SS7_SIG_IF_ID_LAYER,
SS7 SIG IF ID NAI, SS7 SIG M3UA SPC;
SS7 SIG INT ID TABLE 7 = 50, BELFAST12, 4, 2, 0, 0;
SS7_SIG_INT_ID_TABLE 8 = 12, AMSTERDAM, 4, 2, 1, 0;
SS7 SIG INT ID TABLE 9 = 18, ROTERDAM , 4, 2, 2, 0;
SS7 SIG INT ID TABLE 10 = 1, GAUDA    , 4, 2, 3, 0;
[ \SS7_SIG_INT_ID_TABLE ]
```

19.2.2 SS7 M2UA - Media Gateway Controller Side ini File Example

For the SS7 M2UA - Media Gateway Controller Side *ini* file example, take into account the following notes:

- This ini file acts as the M2UA Media Gateway Controller (toward the remote MTP2 side) and M3UA SG (toward the layer 4 application, e.g., Soft-Switch).
- There are 4 SS7 links of type: MTP2 Media Gateway Controller->MTP3.
- There is 1 SN (Signaling Node). Modify its point-code according to your network.
- There is 1 LinkSet with 4 links.
- There is 1 RouteSet.
- The DPC of the RouteSet and LinkSet is the point-code of the remote end (to which the MTP2 link on the MTP2 SG side is connected). Modify it on both LinkSet and RouteSet tables.
- There are 2 interface groups: 1 interface group is used for the M2UA SG <=> M2UA Media Gateway Controller connection, and the other one is used for the M3UA SG <=> M3UA Media Gateway Controller connection.
- There are 4 interface IDs defined: 1 per link (M2UA Media Gateway Controller side) and one more interface Id for M3UA SG. The connection between the interface ID and the Interface group is determined by the SS7_SIG_IF_ID_OWNER_GROUP parameter.
- This file is intended for ITU link variant (E1 trunks).

➢ To load the SS7 M2UA - Media Gateway Controller Side *ini* file example, take these 4 steps:

1. Load this *ini* file on an MTP2 Media Gateway Controller board. An MTP2 SG board should be connected (over IP) to the MTP2Media Gateway Controller board.
2. Change the value of the **SyslogServerIP** parameter accordingly.
3. Change the **SS7_DEST_IP** parameter according to the actual IP address of the M2UA SG board.
4. Change the **SS7_SIG_M3UA_SPC** parameter of line 0 (M3UA related interface ID line) according to the local SN point code.

The following is an example of SS7 M2UA - Media Gateway Controller Side *ini* File

```
[TDM BUS configuration]

; 1=aLaw  3=ulaw
PCMLawSelect=    1
```

```
; EXT BUS=5   H110=4   QSLAC=3   FRAMERS=2   SC BUS=1   MVIP BUS=0
TDMBusType=         2

; 0=2048kbps, 2=4096kbps, 3=8192kbps
TDMBusSpeed=    3

;1 - internal, 3 - mvip, 4 - Network, 8 - h110a, 9 - h110b, 10 -
Netref
TDMBUSCLOCKSOURCE= 1

[Trunk Configuration]

;e1 euro isdn=1 t1 isdn=2 ;e1 cas r2=8 (8 for fcd); e1 trans 62=5
ProtocolType = 5

TraceLevel    = 1

; acCLOCK MASTER ON =1
CLOCKMASTER= 1

;acUSER TERMINATION SIDE = 0
TerminationSide = 1

;acEXTENDED SUPER FRAME=0
FramingMethod = 0

;acB8ZS = 0    2 for E1 CAS - FCD
LineCode = 0

Q931RELAYMODE = 0

[SS7]

SS7_MTP2_PARAM_TIMER_T7_0=2000

; 0=Internal Clock, 1=rx signal derived clk
PHYCLKSOURCE=0

[syslog]
SYSLOGSERVERIP = 168.100.0.1
ENABLESYSLOG = 1

WATCHDOGSTATUS = 0

; ***************************************
; SS7 TIMERS - ITU
; ***************************************

[SS7_SN_TIMERS_TABLE]
FORMAT SS7 SNTIMERS INDEX = SS7 SNTIMERS NAME, SS7 SNTIMERS T6,
SS7 SNTIMERS T8, SS7 SNTIMERS T10, SS7 SNTIMERS T11,
SS7_SNTIMERS_T15, SS7_SNTIMERS_T16, SS7_SNTIMERS_T18_ITU,
SS7 SNTIMERS T19 ITU, SS7 SNTIMERS T20 ITU, SS7 SNTIMERS T21 ITU,
SS7 SNTIMERS T24 ITU;
SS7_SN_TIMERS_TABLE 0 = TENERIFF_0, 800, 1000, 30000, 30000, 2000,
1400, 5000, 4000, 15000, 10000, 500;
[\SS7 SN TIMERS TABLE]

[SS7 LINKSET TIMERS TABLE]
FORMAT SS7 LKSETTIMERS INDEX = SS7 LKSETTIMERS NAME,
SS7 LKSETTIMERS T1SLT, SS7 LKSETTIMERS T2SLT, SS7 LKSETTIMERS T1,
SS7 LKSETTIMERS T2, SS7 LKSETTIMERS T3, SS7 LKSETTIMERS T4,
SS7 LKSETTIMERS T5, SS7 LKSETTIMERS T7, SS7 LKSETTIMERS T12,
SS7 LKSETTIMERS T13, SS7 LKSETTIMERS T14, SS7 LKSETTIMERS T17,
SS7_LKSETTIMERS_T22_ITU, SS7_LKSETTIMERS_T23_ITU;
```

```
SS7 LINKSET TIMERS TABLE 0 = DELHI 0, 8000, 30000, 800, 1400, 800,
800, 800, 1000, 1500, 800, 2000, 1500, 180000, 180000;
[\SS7_LINKSET_TIMERS_TABLE]

; ************************************
; SS7 TIMERS - ANSI
; ************************************

 [SS7_SN_TIMERS_TABLE]
FORMAT SS7 SNTIMERS INDEX = SS7 SNTIMERS NAME, SS7 SNTIMERS T6,
SS7 SNTIMERS T8, SS7 SNTIMERS T10, SS7 SNTIMERS T11,
SS7_SNTIMERS_T15, SS7_SNTIMERS_T16, SS7_SNTIMERS_T22_ANSI,
SS7 SNTIMERS T23 ANSI, SS7 SNTIMERS T24 ANSI,
SS7 SNTIMERS T25 ANSI, SS7 SNTIMERS T26 ANSI,
SS7_SNTIMERS_T28_ANSI, SS7_SNTIMERS_T29_ANSI,
SS7 SNTIMERS T30 ANSI;
SS7 SN TIMERS TABLE 1 = BABILON 0, 800, 1000, 30000, 30000, 2000,
1400, 180000, 180000, 5000, 30000, 12000, 3000, 60000, 30000;
[\SS7 SN TIMERS TABLE]

[SS7_LINKSET_TIMERS_TABLE]
FORMAT SS7 LKSETTIMERS INDEX = SS7 LKSETTIMERS NAME,
SS7 LKSETTIMERS T1SLT, SS7 LKSETTIMERS T2SLT, SS7 LKSETTIMERS T1,
SS7_LKSETTIMERS_T2, SS7_LKSETTIMERS_T3, SS7_LKSETTIMERS_T4,
SS7 LKSETTIMERS T5, SS7 LKSETTIMERS T12, SS7 LKSETTIMERS T13,
SS7 LKSETTIMERS T14, SS7 LKSETTIMERS T17, SS7 LKSETTIMERS T20 ANSI,
SS7_LKSETTIMERS_T21_ANSI;
SS7 LINKSET TIMERS TABLE 1 = HANOI 0, 8000, 30000, 800, 1400, 800,
800, 800, 1000, 1500, 2000, 1500, 90000, 90000;
[\SS7_LINKSET_TIMERS_TABLE]

[SS7 SN TABLE]
FORMAT SS7 SN INDEX = SS7 SN NAME, SS7 SN TRACE LEVEL,
SS7 SN ADMINISTRATIVE STATE, SS7 SN VARIANT, SS7 SN NI,
SS7 SN SP STP, SS7 SN OPC, SS7 SN ROUTESET CONGESTION WINSIZE,
SS7 SN TIMERS INDEX, SS7 SN ISUP APP, SS7 SN SCCP APP,
SS7 SN BISUP APP, SS7 SN ALCAP APP;
SS7 SN TABLE 0 = SN 0, 0, 2, 1, 0, 0, 11, 8, 0, 4, 4, 4, 4;
[\SS7 SN TABLE]

 [ SS7 LINK TABLE ]
FORMAT SS7 LINK INDEX = SS7 LINK NAME, SS7 LINK TRACE LEVEL,
SS7 LINK ADMINISTRATIVE STATE,SS7 LINK L2 TYPE,
SS7 LINK L3 TYPE,SS7 LINK GROUP ID, SS7 LINK M2UA IF ID;
SS7 LINK TABLE 0 = link 0 SP A, 0, 2, 2, 2, 4, 50;
SS7 LINK TABLE 1 = link 1 SP B, 0, 2, 2, 2, 4, 12;
SS7 LINK TABLE 2 = link 2 SP C, 0, 2, 2, 2, 4, 18;
SS7 LINK TABLE 3 = link 3 SP D, 0, 2, 2, 2, 4, 1;
[\SS7_LINK_TABLE]

[ SS7 LINKSET TABLE ]
FORMAT SS7_LINKSET_SN_INDEX, SS7_LINKSET_LINKSET_INDEX =
SS7 LINKSET NAME, SS7 LINKSET ADMINISTRATIVE STATE,
SS7 LINKSET DPC, SS7 LINKSET TIMERS INDEX;
SS7_LINKSET_TABLE 0, 0 = lkset0_sp_A, 2, 10, 0;
[ \SS7 LINKSET TABLE ]

[ SS7_LINKSETLINK_TABLE ]
FORMAT SS7 LINKSETLINK SN INDEX, SS7 LINKSETLINK LINKSET INDEX,
SS7 LINKSETLINK INNER LINK INDEX = SS7 LINKSETLINK LINK NUMBER,
SS7_LINKSETLINK_LINK_SLC;
SS7 LINKSETLINK TABLE 0, 0, 0 = 0, 0;
SS7 LINKSETLINK TABLE 0, 0, 1 = 1, 1;
SS7_LINKSETLINK_TABLE 0, 0, 2 = 2, 2;
SS7 LINKSETLINK TABLE 0, 0, 3 = 3, 3;
[ \SS7 LINKSETLINK TABLE ]
```

```
[ SS7 ROUTESET TABLE ]
FORMAT SS7 ROUTESET SN INDEX, SS7 ROUTESET INDEX =
SS7_ROUTESET_NAME, SS7_ROUTESET_ADMINISTRATIVE_STATE,
SS7 ROUTESET DPC;
SS7 ROUTESET TABLE 0, 0 = RTESET0 SP A, 2, 10;
[ \SS7 ROUTESET TABLE ]


[ SS7 ROUTESETROUTE TABLE ]
FORMAT SS7 ROUTESETROUTE SN INDEX,
SS7 ROUTESETROUTE ROUTESET INDEX,
SS7 ROUTESETROUTE INNER ROUTE INDEX =
SS7 ROUTESETROUTE LINKSET NUMBER, SS7 ROUTESETROUTE PRIORITY;
SS7 ROUTESETROUTE TABLE 0, 0, 0 = 0, 0;
[ \SS7 ROUTESETROUTE TABLE ]

[ SS7 SIG IF GROUP TABLE ]
FORMAT SS7 SIG IF GR INDEX = SS7 IF GR ID,SS7 SIG SG MGC,
SS7 SIG LAYER, SS7 SIG TRAF MODE, SS7 SIG T REC, SS7 SIG T ACK,
SS7 SIG T HB, SS7 SIG MIN ASP, SS7 SIG BEHAVIOUR,
SS7 LOCAL SCTP PORT, SS7 SIG NETWORK;
;
; M3UA SG SIDE DEFINITION:
;
SS7_SIG_IF_GROUP_TABLE 1 =  1, 83, 3, 1, 2000, 2000, 30000, 1, 0,
2905, 1;
[ \SS7 SIG IF GROUP TABLE ]

[ SS7 SIG IF GROUP TABLE ]
FORMAT SS7 SIG IF GR INDEX = SS7 IF GR ID,SS7 SIG SG MGC,
SS7_SIG_LAYER, SS7_SIG_TRAF_MODE, SS7_SIG_T_REC, SS7_SIG_T_ACK,
SS7 SIG T HB, SS7 SIG MIN ASP, SS7 SIG BEHAVIOUR,
SS7 LOCAL SCTP PORT, SS7 SIG NETWORK, SS7 DEST SCTP PORT,
SS7_DEST_IP, SS7_MGC_MX_IN_STREAM, SS7_MGC_NUM_OUT_STREAM;
;
; M2UA MGC SIDE DEFINITION:
;
SS7 SIG IF GROUP TABLE 4 =  4, 77, 2, 1, 2000, 2000, 30000, 1, 0,
2904, 1,2904,168.100.0.2,3,3;
[ \SS7_SIG_IF_GROUP_TABLE ]


[ SS7_SIG_INT_ID_TABLE ]
FORMAT SS7 SIG IF ID INDEX = SS7 SIG IF ID VALUE,
SS7 SIG IF ID NAME, SS7 SIG IF ID OWNER GROUP, SS7 SIG IF ID LAYER,
SS7_SIG_IF_ID_NAI, SS7_SIG_M3UA_SPC;
SS7 SIG INT ID TABLE 0 = 100, BELFAST12, 1, 3, 0, 11;
SS7 SIG INT ID TABLE 1 = 50, AMSTERDAM1, 4, 2, 0,  0;
SS7_SIG_INT_ID_TABLE 2 = 12, GAUDA,      4, 2, 1,  0;
SS7 SIG INT ID TABLE 3 = 18, PRAGUE,     4, 2, 2,  0;
SS7 SIG INT ID TABLE 4 = 1, PARIS ,      4, 2, 3,  0;
[ \SS7_SIG_INT_ID_TABLE ]
```

19.2.3 SS7 MTP2 Tunneling ini File Example

'For the SS7 MTP2 Tunneling *ini* file example, take into account the following notes:

- This *ini* file acts as MTP2 tunneling central side (M2UA Media Gateway Controller links).

- There are 8 SS7 links - 4 links of type: MTP2 Media Gateway Controller, and 4 links of type MTP2. Each pair of links (1 MTP2 Media Gateway Controller and 1 MTP2) defines an MTP2 tunnel.
- There is 1 interface that is used for the M2UA Media Gateway Controller <=> M2UA SG connection.
- There are 4 interface IDs defined: 1 per link (M2UA Media Gateway Controller side).
- This file is intended for ITU link variant (E1 trunks).

➢ To load the example of an SS7 MTP2 Tunneling *ini* file, take these 4 steps:

1. Load this *ini* file (as shown below, 'SS7 MTP2 Tunneling *ini* File Example - Media Gateway Controller') on a Tunnel central gateway (MTP2 Media Gateway Controller).
2. Load the *ini* file as shown in 'SS7 MTP2 Tunneling *ini* File Example - SG' on a tennel remote gateway (MTP2 SG). The Media Gateway Controller gateway connects (over IP) to the SG gateway. For more information on loading an *ini* file, refer to the "Software Upgrade Wizard" on page 190.
3. In the Media Gateway Controller gateway, change the parameter'SS7_DEST_IP' to the actual IP address of the M2UA SG gateway.
4. Change the value of the 'SyslogServerIP' parameter in the Media Gateway Controller and SG gateways to your Syslog server IP address.

The following is an example of SS7 MTP2 Tunneling *ini* File

```
MGCONTROLPROTOCOLTYPE = 2
[TDM BUS configuration]

; 1=aLaw  3=ulaw
PCMLawSelect=    1

; EXT BUS=5   H110=4   QSLAC=3   FRAMERS=2   SC BUS=1   MVIP BUS=0
TDMBusType=        2

; 0=2048kbps, 2=4096kbps, 3=8192kbps
TDMBusSpeed=   3

;1 - internal, 3 - mvip, 4 - Network, 8 - h110a, 9 - h110b, 10 -
Netref
TDMBUSCLOCKSOURCE= 1

MGCONTROLPROTOCOLTYPE = 2
PROVISIONEDCALLAGENTS = 10.10.2.77
[Trunk Configuration]

;e1 euro isdn=1 t1 isdn=2 ;e1 cas r2=8 (8 for fcd); e1 trans 62=5
ProtocolType = 5

TraceLevel   = 0
; acCLOCK MASTER ON =1
CLOCKMASTER= 1

;acUSER TERMINATION SIDE = 0
TerminationSide = 1

;acEXTENDED SUPER FRAME=0
FramingMethod = 0

;acB8ZS = 0   2 for E1_CAS - FCD
```

```
LineCode = 0

Q931RELAYMODE = 0

[SS7]

SS7 MTP2 PARAM TIMER T1 0=50000
SS7 MTP2 PARAM TIMER T2 0=150000
SS7 MTP2 PARAM TIMER T3 0=1000
SS7 MTP2 PARAM TIMER T4E 0=500
SS7 MTP2 PARAM TIMER T4N 0=8200
SS7 MTP2 PARAM TIMER T5 0=100
SS7 MTP2 PARAM TIMER T6 0=3000
SS7 MTP2 PARAM TIMER T7 0=2000
;
[syslog]
;SYSLOGSERVERIP = 168.100.0.1
ENABLESYSLOG = 1

WATCHDOGSTATUS = 0

[ SS7 LINK TABLE ]
FORMAT SS7_LINK_INDEX = SS7_LINK_NAME, SS7_LINK_TRACE_LEVEL,
SS7 LINK ADMINISTRATIVE STATE,SS7 LINK L2 TYPE, SS7 LINK L3 TYPE,
SS7 LINK GROUP ID, SS7 LINK M2UA IF ID;
SS7_LINK_TABLE 1 = new_link_1, 0, 2, 2, 3, 4, 50;
SS7 LINK TABLE 3 = new link 3, 0, 2, 2, 3, 4, 12;
SS7 LINK TABLE 5 = new link 5, 0, 2, 2, 3, 4, 18;
SS7_LINK_TABLE 7 = new_link_7, 0, 2, 2, 3, 4,  1;

[ \SS7 LINK TABLE ]

[ SS7 LINK TABLE ]
FORMAT SS7 LINK INDEX = SS7 LINK NAME, SS7 LINK TRACE LEVEL,
SS7_LINK_ADMINISTRATIVE_STATE,SS7_LINK_L2_TYPE, SS7_LINK_L3_TYPE,
SS7 LINK TRUNK NUMBER,SS7 LINK TIMESLOT NUMBER,
SS7 LINK LAYER2 VARIANT,SS7 LINK MTP2 ATTRIBUTES,SS7 CONGESTION LOW
_M ARK, SS7_CONGESTION_HIGH_MARK, SS7_LINK_TNL_MGC_LINK_NUMBER,
SS7 LINK TNL ALIGNMENT MODE, SS7 LINK TNL CONGESTION MODE,
SS7 LINK TNL WAIT START COMPLETE TIMER,
SS7_LINK_TNL_OOS_START_DELAY_TIMER,
SS7 LINK TNL WAIT OTHER SIDE INSV TIMER;


SS7 LINK TABLE 0 = new link 0, 0, 2, 1, 3, 0, 15, 1, 0, 5, 50, 1,
1,  0, 30000, 5000, 30000;
SS7_LINK_TABLE 2 = new_link_2, 0, 2, 1, 3, 3, 12, 1, 0, 5, 50, 3,
1, 0, 30000, 5000, 30000;
SS7 LINK TABLE 4 = new link 4, 0, 2, 1, 3, 6,  7, 1, 0, 5, 50, 5,
1, 0, 30000, 5000, 30000;
SS7 LINK TABLE 6 = new link 6, 0, 2, 1, 3, 7,  3, 1, 0, 5, 50, 7,
1, 0, 30000, 5000, 30000;
[ \SS7_LINK_TABLE ]

[ SS7 SIG IF GROUP TABLE ]
FORMAT SS7_SIG_IF_GR_INDEX = SS7_IF_GR_ID,SS7_SIG_SG_MGC,
SS7 SIG LAYER, SS7 SIG TRAF MODE, SS7 SIG T REC, SS7 SIG T ACK,
SS7 SIG T HB, SS7 SIG MIN ASP, SS7 SIG BEHAVIOUR,
SS7_LOCAL_SCTP_PORT, SS7_SIG_NETWORK, SS7_DEST_SCTP_PORT,
SS7 DEST IP, SS7 MGC MX IN STREAM, SS7 MGC NUM OUT STREAM;
SS7 SIG IF GROUP TABLE 4 = 4, 77, 4, 1, 2000, 2000, 30000, 1, 0,
2904, 1,2904,168.100.0.2,3,3;

[ \SS7 SIG IF GROUP TABLE ]

[ SS7_SIG_INT_ID_TABLE ]
```

```
FORMAT SS7 SIG IF ID INDEX = SS7 SIG IF ID VALUE,
SS7 SIG IF ID NAME, SS7 SIG IF ID OWNER GROUP, SS7 SIG IF ID LAYER,
SS7_SIG_IF_ID_NAI, SS7_SIG_M3UA_SPC;
SS7 SIG INT ID TABLE 7 = 50, BELFAST12, 4, 2, 1, 0;
SS7 SIG INT ID TABLE 8 = 12, AMSTERDAM, 4, 2, 3, 0;
SS7_SIG_INT_ID_TABLE 9 = 18, ROTERDAM , 4, 2, 5, 0;
SS7 SIG INT ID TABLE 10 = 1, GAUDA    , 4, 2, 7, 0;
[ \SS7_SIG_INT_ID_TABLE ]
```

The following is an example of SS7 MTP2 Tunneling *ini* File Example - SG.

```
[TDM BUS configuration]

; 1=aLaw  3=ulaw
PCMLawSelect=    1

; EXT BUS=5   H110=4   QSLAC=3   FRAMERS=2   SC BUS=1   MVIP BUS=0
TDMBusType=        2

; 0=2048kbps, 2=4096kbps, 3=8192kbps
TDMBusSpeed=   3
;1 - internal, 3 - mvip, 4 - Network, 8 - h110a, 9 - h110b, 10 -
Netref
TDMBUSCLOCKSOURCE= 1
[Trunk Configuration]

;e1 euro isdn=1 t1 isdn=2 ;e1 cas r2=8 (8 for fcd); e1 trans 62=5
ProtocolType = 5

TraceLevel   = 0

; acCLOCK MASTER ON =1
CLOCKMASTER= 1

TerminationSide = 1

;acEXTENDED SUPER FRAME=0
FramingMethod = 0

;acB8ZS = 0   2 for E1 CAS - FCD
LineCode = 0

Q931RELAYMODE = 0

; for ss7 configuration . 77 is for  SS7 debug with TSL and 0 is
noth ing
; 7 is for M2ua DRAFT 7 ; 101 for UAL netbricks
PSTNRESERVED3=  101

[MEGACO]

PROVISIONEDCALLAGENTS = 10.10.2.77

[megaco conference support]

MGControlprotocoltype =2

ATMPHYTYPE=1

; 0=Internal Clock, 1=rx signal derived clk
PHYCLKSOURCE=0

[syslog]
SYSLOGSERVERIP = 168.100.0.1
```

```
ENABLESYSLOG = 1
WATCHDOGSTATUS = 0

[ SS7_LINK_TABLE ]
FORMAT SS7 LINK INDEX = SS7 LINK NAME, SS7 LINK TRACE LEVEL,
SS7 LINK ADMINISTRATIVE STATE,SS7 LINK L2 TYPE, SS7 LINK L3 TYPE,
SS7 LINK TRUNK NUMBER,SS7 LINK TIMESLOT NUMBER,SS7 LINK M2UA IF ID;

SS7 LINK TABLE 0 = new link 0, 0, 2, 1,1,  1, 15,50;
SS7 LINK TABLE 1 = new link 1, 0, 2, 1,1,  2, 12, 12;
SS7 LINK TABLE 2 = new link 2, 0, 2, 1, 1, 4,  7,18;
SS7 LINK TABLE 3 = new link 3, 0, 2, 1, 1, 5,  3,1;

[\SS7 LINK TABLE]

[ SS7 SIG IF GROUP TABLE ]
FORMAT SS7 SIG IF GR INDEX = SS7 IF GR ID,SS7 SIG SG MGC,
SS7 SIG LAYER, SS7 SIG TRAF MODE, SS7 SIG T REC, SS7 SIG T ACK,
SS7 SIG T HB, SS7 SIG MIN ASP, SS7 SIG BEHAVIOUR,
SS7 LOCAL SCTP PORT, SS7 SIG NETWORK;
SS7 SIG IF GROUP TABLE 4 =  4,83, 2, 1, 2000, 2000, 30000, 1, 0,
2904, 1;
[ \SS7_SIG_IF_GROUP_TABLE ]

[ SS7 SIG INT ID TABLE ]
FORMAT SS7_SIG_IF_ID_INDEX = SS7_SIG_IF_ID_VALUE,
SS7 SIG IF ID NAME, SS7 SIG IF ID OWNER GROUP, SS7 SIG IF ID LAYER,
SS7 SIG IF ID NAI, SS7 SIG M3UA SPC;
SS7_SIG_INT_ID_TABLE 7 = 50, BELFAST12, 4, 2, 0, 0;
SS7 SIG INT ID TABLE 8 = 12, AMSTERDAM, 4, 2, 1, 0;
SS7 SIG INT ID TABLE 9 = 18, ROTERDAM , 4, 2, 2, 0;
SS7_SIG_INT_ID_TABLE 10 = 1, GAUDA    , 4, 2, 3, 0;
[ \SS7 SIG INT ID TABLE ]
```

19.3 SS7 Tunneling: Feature Description

The SS7 tunneling feature facilitates peer-to-peer transport of SS7 links between gateways that support this unique MTP2 Tunneling application (M2TN) for transferring SS7 MTP2 link data over IP. In this scenario, both sides of the link are pure TDM switches and are unaware of the IP tandem that is utilized between them. Using M2TN, the network operator can support SS7 connections over IP, carrying MTP level 3, as well as higher level SS7 layers (e.g., user parts and application protocols, such as TUP, ISUP, SCCP, TCAP, etc.).

M2TN uses standard protocols, such as SigTran (RFC 2719 Architectural Framework for Signaling Transport), SCTP (RFC 2960, Stream Control Transmission Protocol), M2UA (RFC 3331), and MTP2 User Adaptation Layer, the latter being used for transporting SS7-MTP2 signaling information over IP. M2UA architecture and M2TN architecture are shown in the figures below.

Figure 19-4: M2UA Architecture

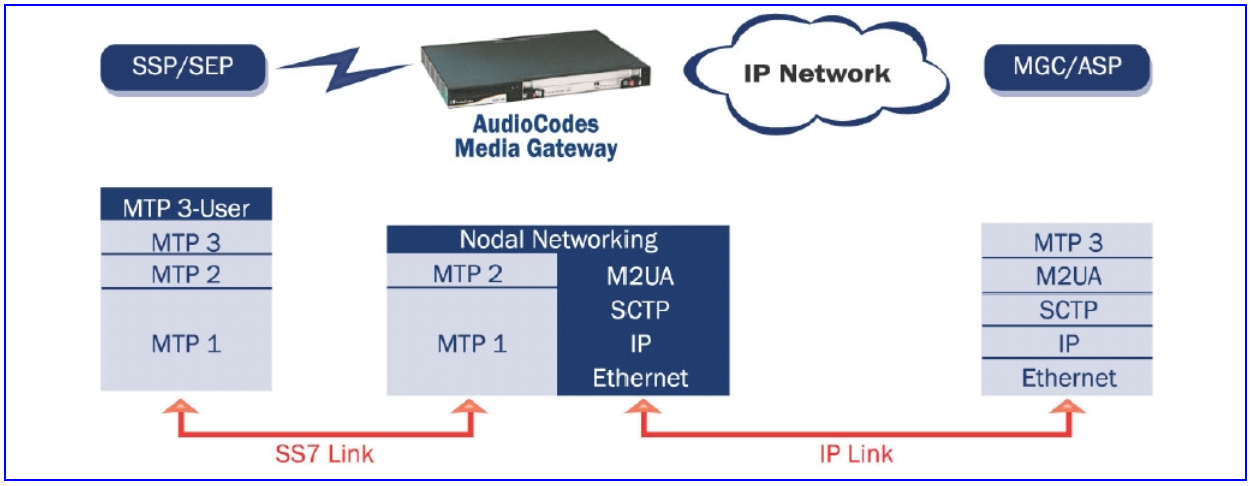
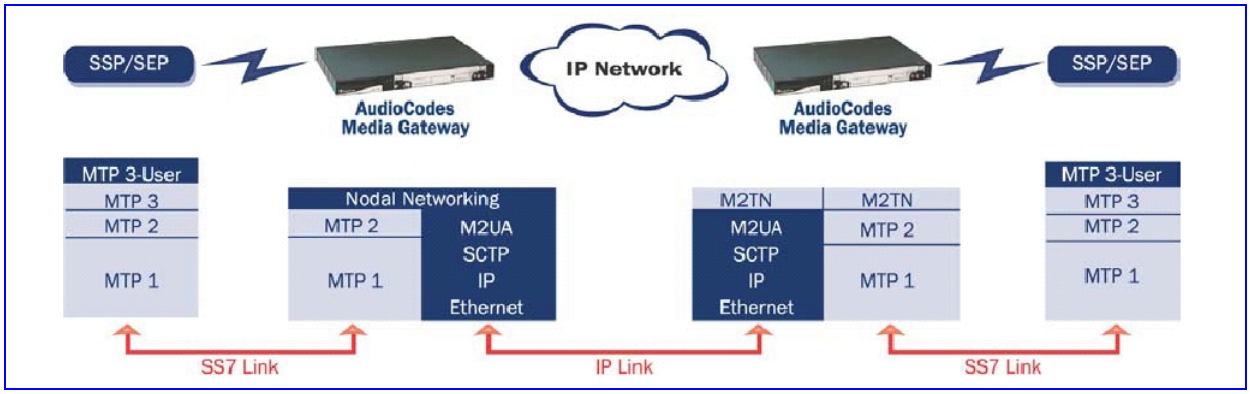


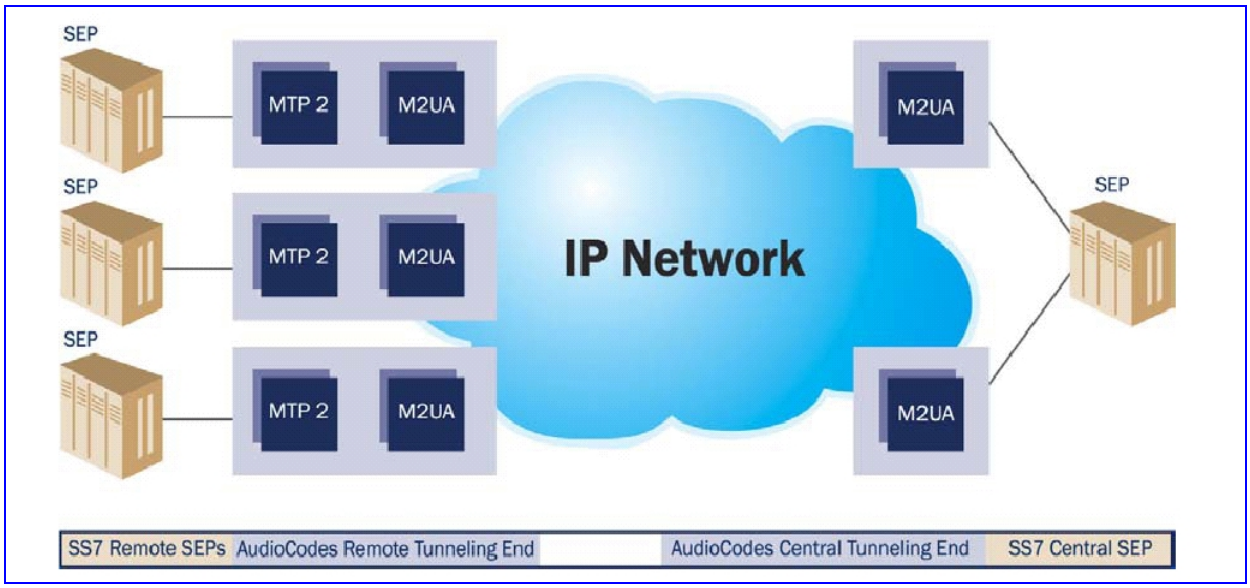
Figure 19-5: M2TN Architecture



19.3.1 MTP2 Tunneling Technology

The SS7 Tunneling technology is based on a pairing of remote and central gateways, as shown in the figure below. The remote gateways are configured to backhaul MTP layer 2 signaling over the IP network using standard M2UA protocol (over SCTP protocol). The function of the M2TN entity is to transmit traffic and handle all management events between MTP2 on the TDM side and M2UA's Media Gateway Controller entity on the IP side. Only the actual SS7 message (MSU) data is sent. Management of the SS7 link is performed using M2UA without transporting the MTP2 LSSU and FISU messages over IP. These messages, in addition to MTP2 timing, are terminated and supported, respectively, by the remote and central sides. Therefore, the MTP2 connections are not affected by the fact that they are transported over IP.

Figure 19-6: Protocol Architecture for MTP2 Tunneling



19.3.2 SS7 Characteristics

- Only standard protocols are used on external interfaces (MTP2 on PSTN side, and M2UA over SCTP on IP side) - the M2TN application resides internally in the MG 3200 gateway.
- No extra signaling point codes are required; both endpoints are unaware that the SS7 connection is via IP.
- Several links from multiple SS7 nodes can be concentrated into a single board on the "Central" side (using several SCTP associations per gateway).
- MG 3200 gateways can handle both SS7 MTP2 Tunneling and voice concurrently (does not require additional gateway or other server).
- Voice and signaling may be transferred on same E1/T1 trunk (F-Links).
- IP traffic can be monitored via standard sniffing tools (e.g. protocol analyzers).

Reader's Notes

20 Appendix - Utilities

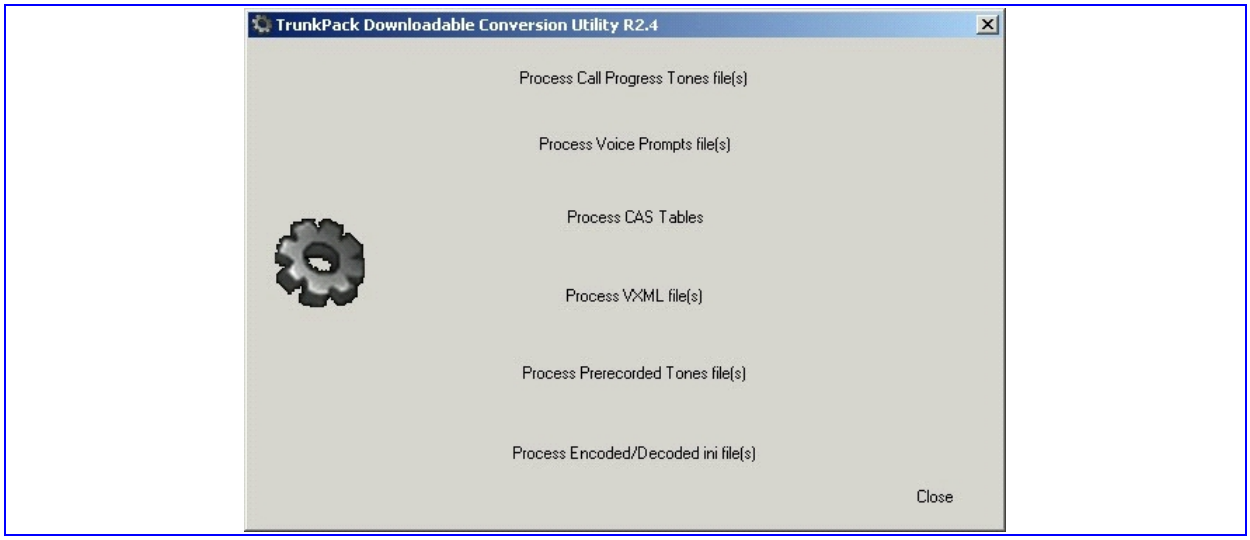
This section describes the functionality and operation of a list of utilities supplied with the TrunkPack software package.

20.1 TrunkPack Downloadable Conversion Utility

LOCATION:

```
.\Utilities\ Downloadables Construction Utility\DConvert240.exe
```

Figure 20-1: Downloadable Conversion Utility Opening Screen



This utility is used to generate the following:

- Process Call Progress Tones file(s)
- Process Voice Prompts file(s)
- Process CAS Tables **(Even though this utility is listed in the main menu, it is NOT applicable to MG 3200)**
- Process VXML file(s) **(Even though this utility is listed in the main menu, it is NOT applicable to MG 3200)**
- Process Prerecorded Tones file(s)
- Process Encoded/Decoded ini file(s)

The files constructed using these utilities can be used when:

- Using an *ini* file during BootP/DHCP session
- Using the Web Interface

Some files may have usage restrictions as described under their usage information.

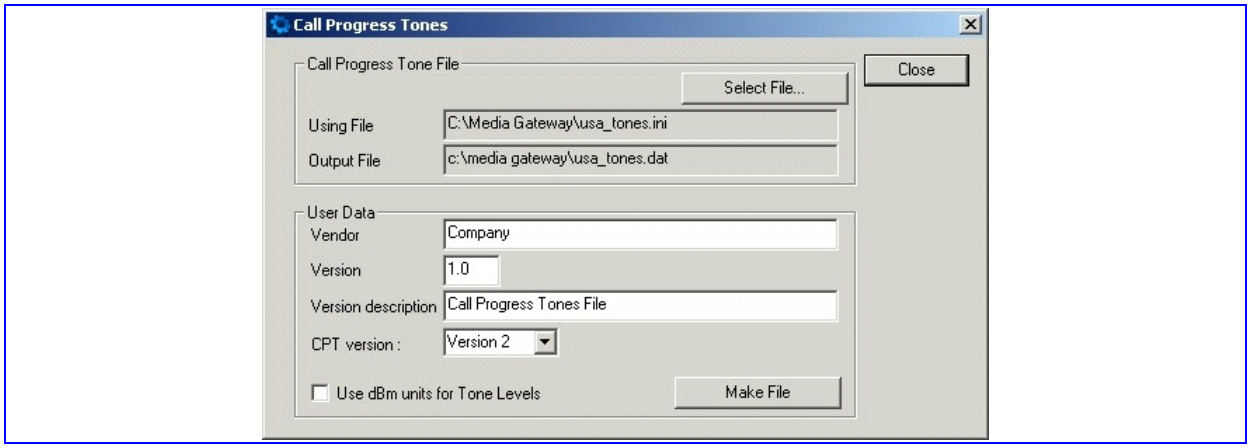
20.1.1 Process Call Progress Tones file(s)

20.1.1.1 Converting a CPT ini File to a Binary dat File

➢ **To convert a CPT ini file to a binary dat file, take these 8 steps:**

1. Create a CPT *ini* file using the direction in "Modifying the Call Progress Tones File" on page 74 or by editing a CPT *ini* file provided by Nortel.
2. Execute *DConvert240.exe* and click the **Process Call Progress Tones file(s)** button. The Call Progress Tones dialog appears.

Figure 20-2: Call Progress Tones Screen



3. Click the **Select File . . .** button and navigate to the location of the CPT *ini* file that you want to convert.
4. Select the desired file and click **Open**. The name and path of both the CPT *ini* file and the *dat* file appear in the **Using File** field and **Output File** field respectively. (The file names and paths are identical except for the file extension.)
5. Fill in the **Vendor, Version** and **Version Description** fields.
   - **Vendor** field - 256 characters maximum
   - **Version** feld - must be made up an integer, followed by a period "**.**", then followed by another integer (e.g., 1.2, 23.4, 5.22)
   - **Description** field - 256 characters maximum
6. The default value of the CPT version drop-down list is **Version 3**. Do one of the following:
   - If the software version release you are using is 4.4, in the **CPT Version** drop-down list, select **Version 2**.
   - If the software device version release is prior to version 4.4, in the **CPT Version** drop-down list, select **Version 1** (to maintain backward compatibility).
7. The **Use dBm units for tone levels** checkbox is not checked as the default. To use -dBm units for setting the Call Progress Tone and User Defined Tone Levels, click a

checkmark into the **Use dBm units for tone levels** checkbox. This checkbox should be checked to maintain backward compatibility.

Note: The default value of the **dBm units for tone levels** checkbox is left unchecked for backward compatibility with versions prior to version 4.4.

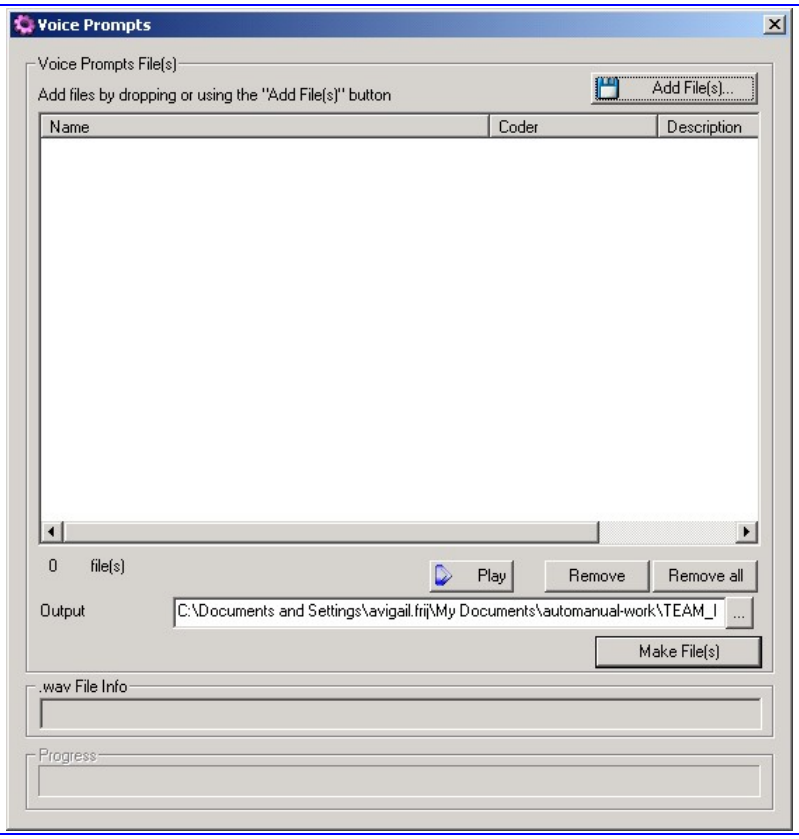
8. Click the **Make File** button. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

20.1.2 Process Voice Prompts file(s)

➢ To generate a Voice Prompts file, take these 12 steps:

1. Create raw Voice Prompt files. From version 4.2, the **DConvert** utility supports *wav* files as well.
2. Execute *DConvert240.exe* and click the **Process Voice Prompts file(s)** button. The Voice Prompts window appears.

Figure 20-3: Voice Prompts Screen



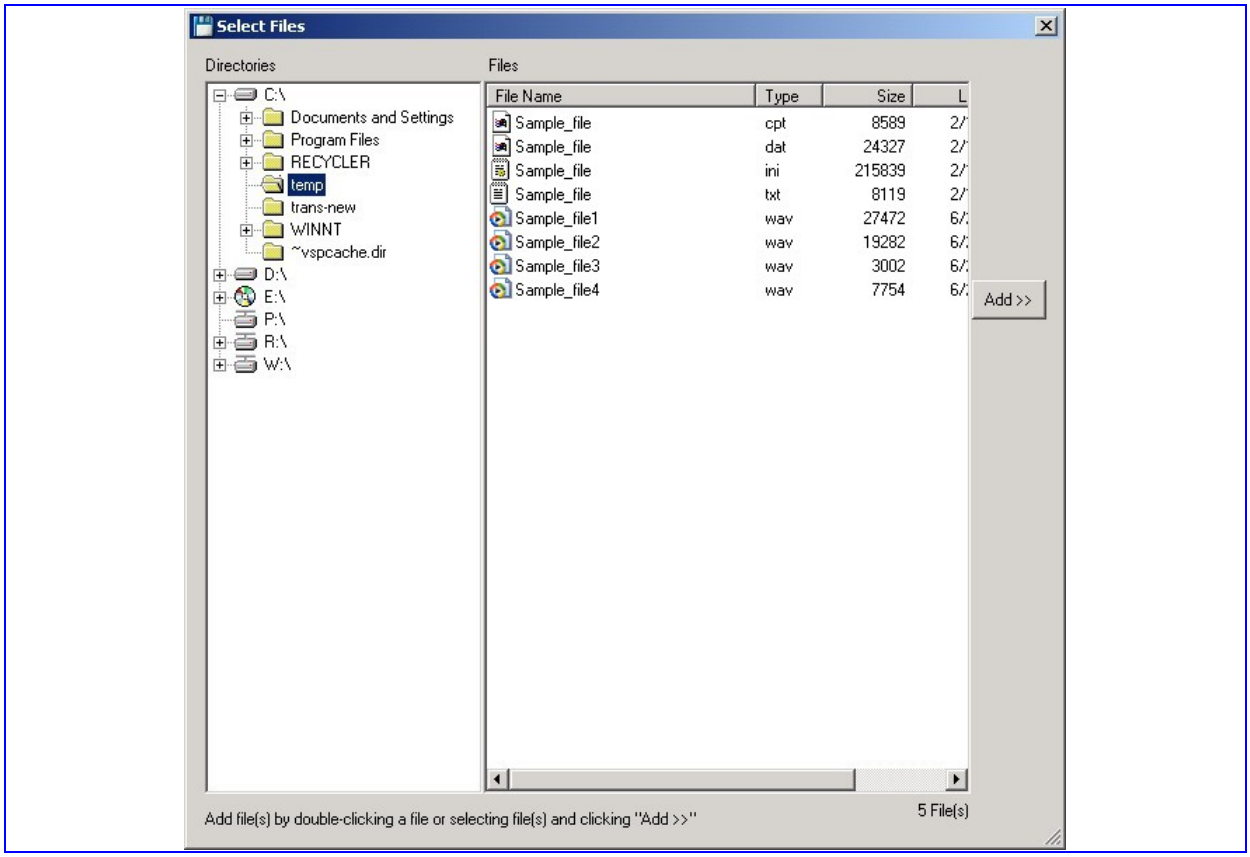
3. Select the raw Voice Prompt files (created in Step 1) step either by one of these actions:

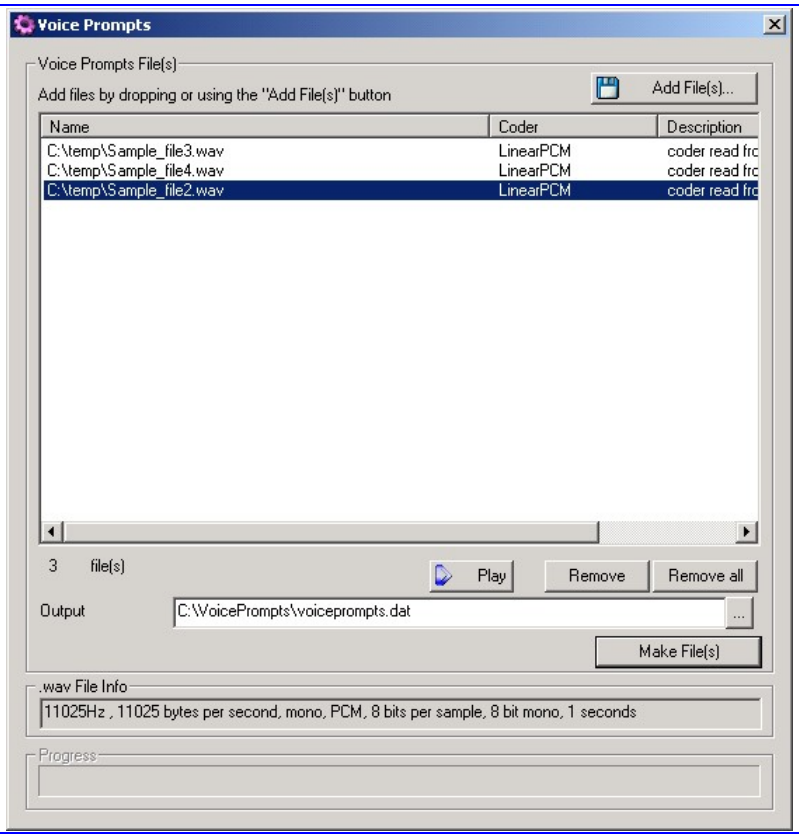
a. Click the **Add Files** button in the upper right corner. The Add Files window appears. (Refer to the figure, "Select Files Window" below.)

Navigate to the appropriate file.

Select it and click the **Add>>** button. To close the Add Files window, click the Exit button. (Press the **Esc** key to cancel changes.)

Figure 20-4: Select Files Window





b. From any location on the PC, select the appropriate files and drag-drop them into the Voice Prompts window.

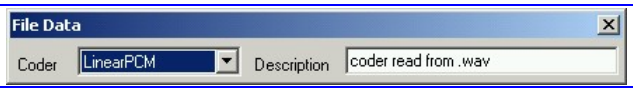
4. Arrange the files as desired by dragging and dropping them from one location in the list to another location.

Note: The sequence of files in the "Add Files..." window defines the Voice Prompt ID.

5. Use the **Play** button to preview the sound of the *wav* file. Use the **Remove** and **Remove all** buttons to remove files in the list as needed.

6. Select a coder for each file by first selecting the file (or files) and then double-clicking or right-clicking on it. The File Data window appears.

Figure 20-5: File Data Window



7. From the **Coder** drop-down list, select a coder type (to be used by the acPlayVoicePrompt() function).

8. In the **Description** field, enter a description (optional).

Note: For *wav* files, a coder is automatically selected from the *wav* file header.

9. Close the File Data dialog by clicking on the Exit button. (Press the **Esc** key to cancel changes.). You are returned to the Voice Prompts window.
10. The default **Output** file name is *voiceprompts.dat*.You can modify it. Or, Use the Browse button to select a different Output file. Navigate to the desired file and select it. The selected file name and its path appear in the **Output** field.
11. Click the **Make File(s)** button to generate the Voice Prompts file. The Progress bar at the bottom of the window is activated. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.
12. The generated file can be used only for downloading using the *ini* file facility or using acOpenRemoteBoard() in full configuration operation mode. When using the acAddVoicePrompt(), use the single raw voice prompt files.

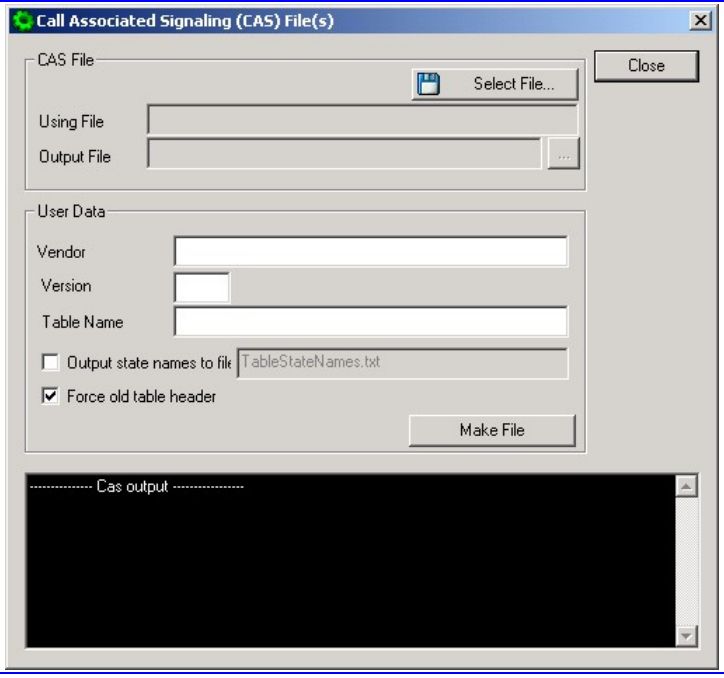
20.1.3 Process CAS Tables

➢ To produce a CAS table, take these 10 steps:

1. Construct the CAS protocol *xxx.txt* and *xxx.h* files.
2. Copy the files generated in the previous step (or at least the *xxx.h* file) to the same directory in which *DConvert240.exe* is located and make sure that the two following files, *CASSetup.h* and *CPP.exe,* are also located in this same directory.

3. Execute *DConvert240.exe* and click the **Process CAS Tables** button. The Call Associated Signaling (CAS) Window appears.

Figure 20-6: Call Associated Signaling (CAS) Screen



4. Click the **Select File** button. A Browse window appears.
5. Navigate to the desired location and select the file to be converted. (This automatically designates the output file as the same name and path, but with the *dat* extension. The Table Name is also automatically designated.)
6. Fill in the **Vendor** and **Version** fields.
   - **Vendor** Field - 32 characters maximum
   - **Version** Field - must be made up an integer, followed by a period "**.**", then followed by another integer (e.g., 1.2, 23.4, 5.22)
7. Modify the **Table Name** if desired.
8. For troubleshooting purposes, you can click a check into the **Output state names to file** checkbox. This activates the file name field in which the default file name, **TableState Names.txt** appears. You can modify the file name if desired. The file is located in the same directory as the **Using file** and **Output file** designated above.
9. If the file to be converted uses the **new table header**, un-check the **Force old table header** checkbox.
10. Click the **Make File** button. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

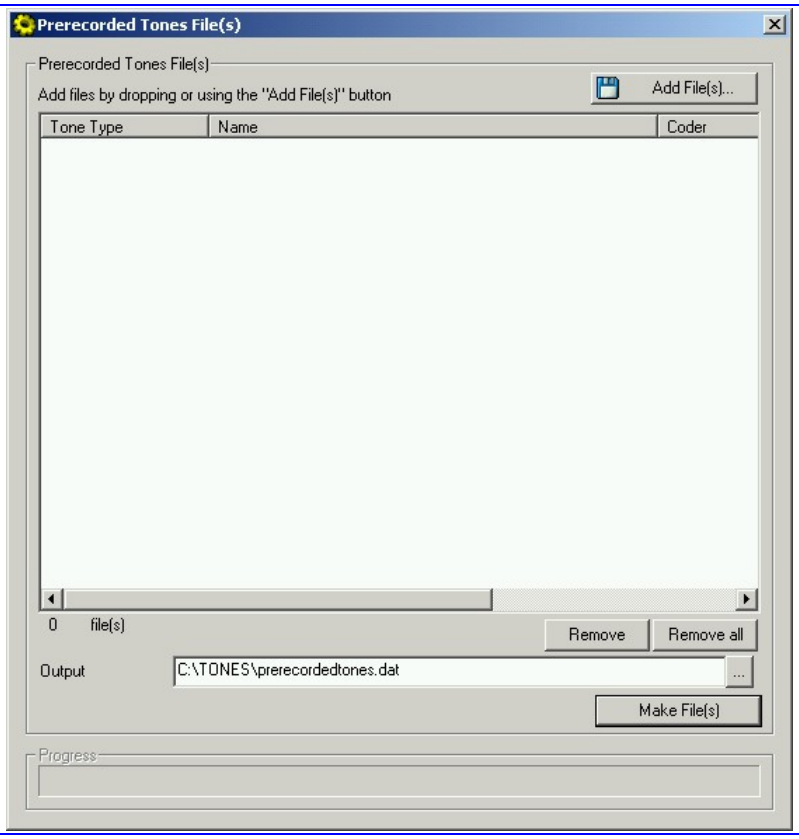
On the bottom of the Call Assisted Signaling (CAS) Files(s) window, the Cas output log box displays the log generated by the process. It can be copied as needed. The information in it is **NOT** retained after the window is closed.

20.1.4 Process Prerecorded Tones file(s)

➢ To generate a Prerecorded Tones file, take these 11 steps:

1. Prior to the conversion process, the user should prepare the appropriate prerecorded tones file(s).
2. Execute *DConvert240.exe* and press the **Process Prerecorded Tones file(s)** button. The Prerecorded Tones file(s) window appears.

Figure 20-7: Prerecorded Tones File(s) Screen



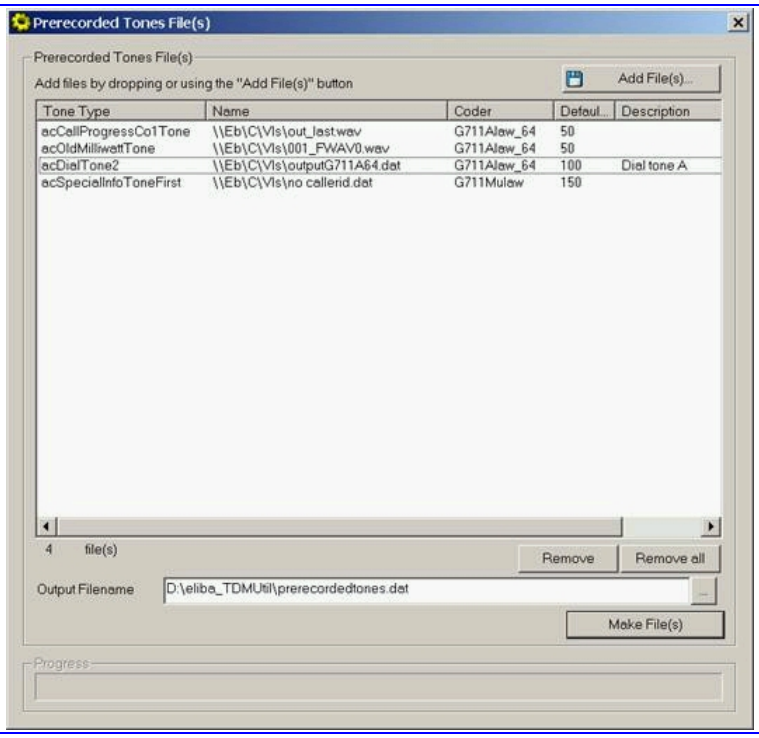
3. Select the raw Prerecorded Tones files (created in Step 1) utilizing one of these actions:

a. Click the **Add Files** button in the upper right corner. The Add Files window appears. (Refer to the figure, Select Files Window.)

Navigate to the appropriate file.

Select it and click the **Add>>** button. (To close the Add Files window, click the Exit button. Press the **Esc** key to cancel changes.) You are returned to the Prerecorded Tones file(s) window.

Figure 20-8: Prerecorded Tones File(s) Screen with wav Files



b. From any location on the PC, select the appropriate files and drag-drop them into the Voice Prompts window.

4. To define a tone type, coder and default duration for each file, select the file (or group of files to be set the same) and double click or right click on it. The File Date window appears.

Figure 20-9: File Data Dialog Box

5. From the **Type** drop-down list, select a Ring parameter type.

6. From the **Coder** drop-down list, select a coder type (G.711 A-law_64, G.711 µ-law, or Linear PCM).

7. In the **Description** field, enter a description (optional).

8. In the **Default** field, enter the duration in msec.

9. Click the Exit button. (Press the **Esc** key to cancel changes.) You are returned to the Prerecorded Tones file(s) window.

10. The default **Output** file name is *prerecordedtones.dat*.You can modify it. Or, Use the Browse button to select a different Output file. Navigate to the desired file and select it. The selected file name and its path appear in the **Output** field.

11. Click **Make File(s)** button. The Progress bar at the bottom of the window is activated. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

20.1.5 Process Encoded/Decoded ini file(s)

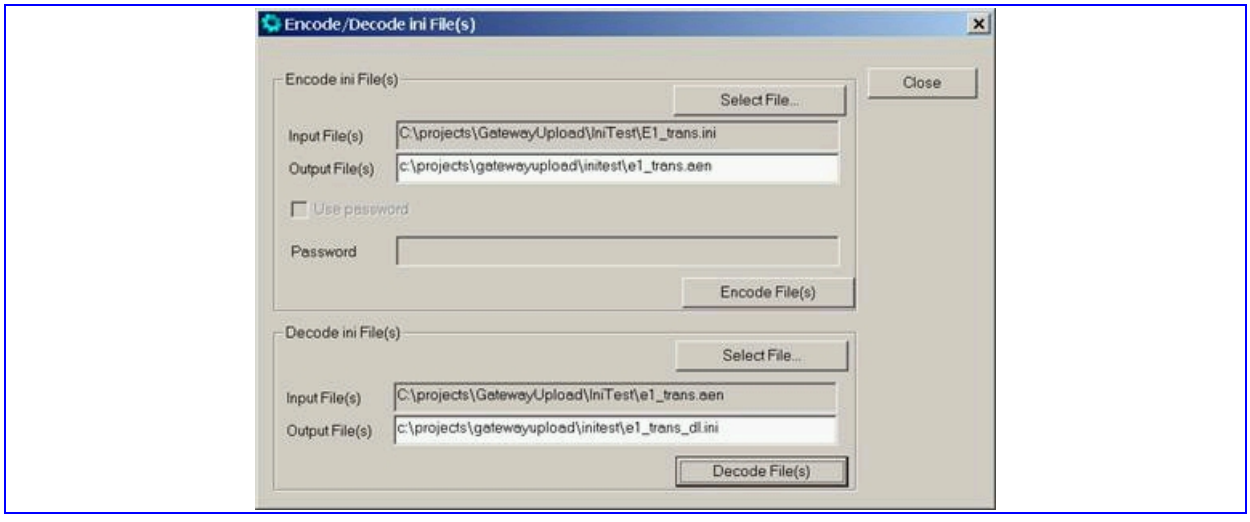
The *ini* file can be both encoded and decoded using the **DConvert** utility (*DConvert240.exe*). Encoding usually takes place before downloading an *ini* file to the board while decoding usually takes place after uploading an *ini* file from the board.

➢ To Encode an *ini* file, take these 4 steps:

1. Prior to the encoding process, the user should prepare the appropriate *ini* file either by uploading from the board or by constructing one (refer to "Initialization (ini) File" on page 59).

   Execute *DConvert240.exe* and click the **Process Encoded** *ini* **file(s)** button. The Encoded *ini* file(s) window appears.

Figure 20-10: Encoded ini File(s) Screen



2. In the **Encode Ini File(s)** area, click the **Select File…** Button. A Browse window appears.

3. Navigate to the desired location and select the *ini* file to be encoded. (This automatically designates the output file as the same name and path, but with the *aen* extension.

Note: The Password field is to be implemented in a future version.

4. Click the **Encode File(s)** button. The encoded file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

The encoded *ini* file can be loaded using the regular *ini* file procedure. To upload a file from a device, use the Web Interface (refer to "Software Update" on page 189).

➢ To Decode an *ini* file follow these 4 steps:

1. Prior to the decoding process the user should prepare the appropriate encoded *ini* file either by uploading from the board or by using the encoding process on an exiting *ini* file.
2. Execute *DConvert240.exe* and click the **Process Encoded** *ini* **file(s)** button.
3. In the **Decode Ini File(s)** area, click **Select File(s)** and select the *aen* file to be decoded. (This automatically designates the output file as the same name and path, but with the extension, *_dl.ini*.
4. Click the **Decode File(s)** button. The decoded file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

Note: The decoding process verifies the input file for validity. Any change made to the encoded file causes an error and the decoding process is aborted.

20.2 PSTN Trace Utilities

LOCATION:

```
.\Utilities\
```

DESCRIPTION:

These utilities are designed to convert PSTN trace binary files to text format. The binary PSTN trace files are generated when the user sets the PSTN interface to trace mode.

OPERATION:

Generating a Trace/audit Text File for CAS Protocols

➢ To generate a readable text file out of the binary trace file when using CAS protocols, take these 3 steps:

1. Rename the PSTN trace binary file to *CASTrace0.dat*.
2. Copy it to the same directory in which the translation utility, *CAS_Trace.exe*, is located.

3. Run *CAS_Trace.exe* (no arguments are required). The text file, *CASTrace0.txt,* is created.

Generating a Trace/audit Text File for ISDN/SS7/ATM Protocols

➢ To generate a readable text file out of the binary trace file when using ISDN/SS7/ATM protocols, take these 2 steps:

1. Copy the PSTN trace binary file to the same directory in which the translation utility *CONVERT_TRACE.BAT* is located. The following files should reside in the same directory: *Dumpview.exe*, *Dumpview.cfg* and *ReadMe.txt*.

   Read carefully the *ReadMe.txt* in order to understand the usage of the translation utility.

2. Run the *CONVERT_TRACE.BAT*. The text file is created.

20.3 Enabling PSTN Trace via the Web

This section contains direction on starting and collecting the PSTN trace via the Web. (Refer to the figure below for a view of the Trunk Traces). Also, note if the PSTN trace is of a ISDN/SS7/ATM or CAS collection based on the physical device involved in the trace. This information is needed to properly parse the captured data.

➢ To start and collect the PSTN trace via the Web, take these 12 steps:

1. Run the UDP2File utility.
2. Determine the trace file name.
3. Determine the UDP port.
4. Mark the PSTN Trace check box.
5. Click the **Run** button. The UDP2File utility starts to collect the trace messages.
6. Activate the Web page by entering <MG 3200 IP address>/FAE and choose the Trunk Traces tab (e.g.,http://10.8.8.101/FAE).
7. Use the user and password, which is the same for the unit.
8. In the Web page, set the trace level of each trunk.
9. Enable the trace via the Web.
10. Determine the UDP port (the same as in step 3).
11. Click the SUBMIT button. The board starts to send the trace messages.

12. In the UDP2File utility (Refer to the figure below) you should see the number in the packets counter increasing.

Figure 20-11: Trunk Traces Screen

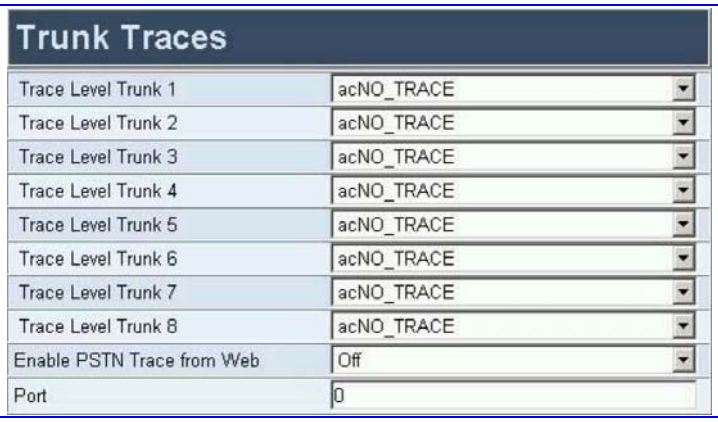


Figure 20-12: UDP2File Utility Dialog Box

20.4 MEGACO Tester Utility

LOCATION:

```
.\Utilities\
```

DESCRIPTION:

This utility serves as a simulation for the H.248 Call Agent. It can send any H.248 command, as well as run complicated scripts. This utility can be used to exercise the MAGACO clients embedded in TrunkPack series boards and modules.

OPERATION:

The MEGACO tester demo application operation is self-explanatory.

Reader's Notes

21 Appendix - H.248 Compliance

The H.248 Compliance Matrix table below summarizes the supported H.248 features. The Reference column in the table refers to IETF RFC 3015 from September 2002.

21.1 H.248 Compliance Matrix

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
7	**Commands supported:**		
	Add	Yes	
	Modify	Yes	
	Subtract	Yes	
	Move	Yes	
	AuditValue	Yes	
	AuditCapabilities	Yes	
	Notify	Yes	
	ServiceChange	Yes	
7.1	**Descriptors**		
7.1.1	**Specifying Parameters:**		
	Fully specified	Yes	
	Under specified	Yes	
	Over specified	Yes	
	Handling unspecified mandatory parameters.	Yes	
	Wildcarded termination ID	Yes	
7.1.2	**Modem Descriptor:**		
	V.18	No	
	V.22	No	
	V.22bis	No	
	V.32	No	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	V.32bis	No	
	V.34	No	
	V.90	No	
	V.91	No	
	Synchronous ISDN	No	
7.1.3	**Multiplex Descriptor:**		
	H.221	No	
	H.223	No	
	H.226	No	
	V.76	No	
7.1.4	**Media Descriptor:**		
	Termination State Descriptor	Yes	
	Stream Descriptor	Yes	
	Local Control Descriptor	Yes	
	Local Descriptor	Yes	
	Remote Descriptor	Yes	
7.1.5	**Termination State Descriptor:**		
	Service State:		
	Test	Yes	
	Out of service	Yes	
	In service	Yes	
	EventBufferControl:	Yes	
7.1.6	**Stream Descriptor:**		
		Yes	
7.1.7	**Local Control Descriptor:**		
	Mode:		
	Send-only	Yes	
	Receive-only	Yes	
	Send/receive	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	Inactive	Yes	
	Loop-back	Yes	
	ReserveGroup	No	
	ReserveValue	No	
7.1.8	**Local & Remote Descriptors:**		
	Unspecified Local Descriptor	Yes	
	Unspecified Remote Descriptor	Yes	
	Empty Local Descriptor	Yes	
	Empty Remote Descriptor	Yes	
	Multiple groups	No	
7.1.9	**Event Descriptor**		
	EventBufferControl		
	Lockstep	Yes	
	Off	Yes	
7.1.10	**Event Buffer Descriptor**		
		Yes	
7.1.11	**Signal Descriptor**		
	Signal Types		
	On/off	Yes	
	Timeout	Yes	
	Brief	Yes	
	Sequential signal list	Yes	
	Simultaneous signals	No	
	Keep active	Yes	
7.1.12	**Audit Descriptor**		
	Modem	No	
	Mux	No	
	Events	Yes	
	Media	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	Signals	Yes	
	Observed events	Yes	
	DigitMap	Yes	
	Statistics	Yes	
	Packages	Yes	
	EventBuffer	Yes	
	Empty descriptor	Yes	
7.1.13	**Service Change Descriptor**		
	ServiceChangeMethod	Yes	
	ServiceChangeReason	Yes	
	ServiceChangeAddress	Yes	
	ServiceChangeDelay	Yes	
	ServiceChangeProfile	Yes	
	ServiceChangeVersion	Yes	
	ServiceChangeMGCId	Yes	
	TimeStamp	Yes	
7.1.14	**Digit Map Descriptor**		
	Digit Map Names	Yes	
	StartTimer (T)	Yes	
	ShortTimer (S)	Yes	
	LongTimer (L)	Yes	
	DurationModifier (z)	Yes	
	Any digit 0-9 (x)	Yes	
	Zero or more repetitions (.)	Yes	
7.1.15	**Statistics Descriptor**		
	Octets sent	Yes	
	Octets received	Yes	
	Empty AuditDescriptor in “Sub”	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
7.1.16	**Package Descriptor**		
		Yes	
7.1.17	**Observed Events Descriptor**		
	Request Identifier	Yes	
	Event	Yes	
	Detection Time	Yes	
7.1.18	**Topology Descriptor**		**Topology used only for conference**
	Isolate	Yes	
	Oneway	Yes	
	Bothway	Yes	
	CHOOSE wildcard	Yes	
	ALL wildcard	Yes	
7.2	**Command API**		
7.2.1	**Add**		
	Termination ID	Yes	
	MediaDescriptor	Yes	
	ModemDescriptor	No	
	MuxDescriptor	No	
	EventsDescriptor	Yes	
	SignalsDescriptor	Yes	Only one signal per channel Up to 30 signals in a signal list
	DigitMapDescriptor	Yes	
	AuditDescriptor	Yes	
7.2.2	**Modify**		
	Termination ID	Yes	
	MediaDescriptor	Yes	
	ModemDescriptor	No	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	MuxDescriptor	No	
	EventsDescriptor	Yes	
	SignalsDescriptor	Yes	Only one signal per channel Up to 30 signals in a signal list
	DigitMapDescriptor	Yes	
	AuditDescriptor	Yes	
7.2.3	**Subtract**		
	Termination ID	Yes	
	AuditDescriptor	Yes	
	Statistical Parameters return	Yes	
7.2.4	**Move**		
	Termination ID	Yes	
	MediaDescriptor	Yes	
	ModemDescriptor	No	
	MuxDescriptor	No	
	EventsDescriptor	Yes	
	SignalsDescriptor	Yes	Only one signal per channel Up to 30 signals in a signal list
	DigitMapDescriptor	Yes	
	AuditDescriptor	Yes	
7.2.5	**Audit Value**		
	TerminationID	Yes	
	Wildcard	Yes	
	AuditDescriptor	Yes	
	Media	Yes	
	Modem	No	
	Mux	No	
	Event	Yes	
	Signal	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	DigitMap	Yes	
	ObservedEvents	Yes	
	EventBuffer	Yes	
	Statistics	Yes	
	Packages	Yes	
7.2.6	**Audit Capabilities**		
	TerminationID	Yes	
	Wildcard	Yes	
	AuditDescriptor	Yes	
	Media	Yes	
	Modem	No	
	Mux	No	
	Event	Yes	
	Signal	Yes	
	DigitMap	Yes	
	ObservedEvents	Yes	
	EventBuffer	Yes	
	Statistics	Yes	
	Packages	Yes	
7.2.7	**Notify**		
		Yes	
7.2.8	**Service Change**		
	Termination ID	Yes	
	Wildcard	Yes	
	"Root" Termination	Yes	
	ServiceChangeMethod		
	Graceful	No	
	Forced	Yes	
	Restart	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	Disconnected	Yes	
	Handoff	Yes	
	Failover	Yes	
	Extension	No	
	ServiceChangeReason		
	900 Service Restored	Yes	
	901 Cold Boot	Yes	
	902 Warm Boot	No	
	903 MGC Direct Change	Yes	
	904 Termination Malfunctioning	No	
	905 Term Taken out of Service	No	
	906 Loss of lower layer connectivity	Yes	
	907 Transmission Failure	Yes	
	908 MG Impending Failure	No	
	909 MGC Impending Failure	No	
	910 Media Capability Failure	No	
	911 Modem Capability Failure	No	
	912 Mux Capability Failure	No	
	913 Signal Capability Failure	No	
	914 Event Capability Failure	No	
	915 State Loss	No	
	ServiceChangeDelay	No	
	ServiceChangeAddress	Yes	
	ServiceChangeProfile	Yes	
	ServiceChangeVersion	Yes	
	ServiceChangeMgcId	Yes	
	TimeStamp	Yes	
7.2.9	**Manipulating and Auditing Context Attributes**		
		Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
7.2.10	**Generic Command Syntax**		
	Text Encoding	Yes	
	Binary Encoding	Yes	
7.3	**Command Error**		
	400 - Bad Request	Yes	
	401 - Protocol Error	Yes	
	402 - Unauthorized	No	
	403 - Syntax Error in Transaction	Yes	
	404 - Syntax Error in TransactionReply	Yes	
	405 - Syntax Error in TransactionPending	Yes	
	406 - Version not Supported	No	
	410 - Incorrect Identifier	Yes	
	411 - Unknown ContextId	Yes	
	412 - No ContextId Available	Yes	
	421 - Unknown Action	Yes	
	422 - Syntax Error In Action	Yes	
	430 - Unknown TerminationId	Yes	
	431 - No TerminationId Matched a Wildcard	Yes	
	432 - Out of Termination Id / No TerminationId Available	Yes	
	433 - TerminationId is already in a context	Yes	
	440 - Unsupported or unknown Package	Yes	
	441 - Missing RemoteDescriptor	Yes	
	442 - Syntax Error in Command	Yes	
	443 - Unsupported or unknown Command	Yes	
	444 - Unsupported or unknown Descriptor	Yes	
	445 - Unsupported or unknown Property	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	446 - Unsupported or unknown Parameter	Yes	
	447 - Descriptor not legal in this command	Yes	
	448 - Descriptor appears twice in a command	Yes	
	450 - No such property in this package	Yes	
	451 - No such event in this package	Yes	
	452 - No such signal in this package	Yes	
	453 - No such statistic in this package	Yes	
	454 - No such parameter value in this package	Yes	
	455 - Parameter illegal in this Descriptor	Yes	
	456 - Parameter or Property appears twice in this Descriptor	Yes	
	471 - Implied Add for Multiplex failure	Yes	
	500 - Internal Gateway Error	Yes	
	501 - Not Implemented	Yes	
	502 - Not ready	Yes	
	503 - Service Unavailable	No	
	504 - Command Received from unauthorized entity	No	
	505 - Command Received before Restart Response	Yes	
	510 - Insufficient resources	Yes	
	512 - Media Gateway unequipped to detect requested Event	Yes	
	513 - Media Gateway unequipped to generate requested Signals	Yes	
	514 - MG cannot send the specified announcement	Yes	
	515 - Unsupported Media Type	Yes	
	517 - Unsupported or Invalid Mode	Yes	
	518 - Event Buffer Full	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
	519 - Out Of Space To Store Digit Map	Yes	
	520 - Media Gateway does not have a digit map	Yes	
	521 - Termination is "Service Changing"	No	
	526 - Insufficient Bandwidth	No	
	529 - Internal Hardware Failure	No	
	530 - Temporary Hardware Failure	No	
	531 - Permanent Network Failure	No	
	540 - Unexpected Initial hook state	No	
	581 - Does not Exist	Yes	
8.	**Transactions**		
8.1	**Common Parameters**		
8.1.1	**Transaction Identifiers**		
	TransactionID	Yes	
	Use of TransactionId '0'	Yes	
8.1.2	**Context Identifiers**		
	ContextID	Yes	
	CHOOSE Wildcard	Yes	
	All Wildcard	Yes	
8.2	**Transaction API**		
8.2.1	**Transaction Request**		
	Multiple actions per request	Yes	
8.2.2	**Transaction Reply**		
	Multiple actions per reply	Yes	
8.2.3	**Transaction Pending**		
	Transaction Pending Support	No	
	normalMGEcecutionTime	Yes	
	normalMGCEcecutionTime	Yes	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
8.3	**Messages**		
	Receive Messages	Yes	
	Send Messages	Yes	
9	**Transport**		
	Transport over UDP	Yes	
	Transport over TCP	No	
9.1	**Ordering of Commands**		
		Yes	
9.2	**Protection Against the Restart Avalanche**		
	Use of default MWD per platform	No	
	Random restart delay	No	
	Random seed selection	No	
	Detection of local activity	No	
10	**Security Considerations**		
		No	
11	**MG-MGC Control Interface**		
11.1	**Multiple Virtual Gateways**	**No**	
11.2	**Cold Start**		
	Primary Call Agent support	Yes	
	Secondary Call Agents support	Yes	
	Cyclic check for Call Agent	Yes	
11.3	**Negotiation of Protocol Version**		
		No	

Table 21-1: H.248 Compliance Matrix

Reference (in RFC 3015)	Item	Support	Comments
11.4	**Failure of an MG**		
		No	
11.5	**Failure of an MGC**		
		Yes	

Reader's Notes

22 Appendix - SNMP Traps

This section provides information regarding proprietary traps currently supported in the MG 3200. Note that traps whose purposes are alarms are different from traps whose purposes are not alarms, e.g., logs.

Currently, all traps have the same structure, which is made up of the same 11 varbindsAn example is: 1.3.6.1.4.1.5003.9.10.1.21.1

The source varbind is made up of a string that details the component from which the trap is being sent, forwarded by the hierarchy in which it resides. For example, an alarm from an SS7 link has the following string in its source varbind: acBoard#1/SS7#0/SS7Link#6

In this example, the SS7 link number is specified as 6 and is part of the only SS7 module in the device that is placed in slot number 1 (in a chassis) and is the module to which this trap is related. For devices where there are no chassis options the slot number of the board is always 1.

22.1 Alarm Traps

The following provides information relating to those alarms that are raised as the result of a generated SNMP trap. The component name described within each of the following section headings refers to the string that is provided in the acBoardTrapGlobalsSource trap varbind. In all the following discussions, to clear a generated alarm the same notification type is sent but with the severity set to 'cleared'.

22.1.1 Component: Board#<n>

<n> is the slot number when the TP-1610 resides in a chassis and is 1 when the device is stand alone.

Table 22-1: acBoardFatalError Alarm Trap

Alarm:	acBoardFatalError
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.1
Default Severity	Critical
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Board Fatal Error: <text>
Status Changes:	
Condition:	Any fatal error
Alarm status:	Critical
<text> value:	A run-time specific string describing the fatal error

Table 22-1: acBoardFatalError Alarm Trap

Alarm:	acBoardFatalError
Condition:	After fatal error
Alarm status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	Capture the alarm information and the syslog close, if active. Contact your first-level support group. The support group will likely want to collect additional data from the device and then perform a reset.

Table 22-2: acBoardConfigurationError Alarm Trap

Alarm:	acBoardConfigurationError
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.2
Default Severity	critical
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Board Config Error: <text>
Status Changes:	
Condition:	A configuration error was detected
Alarm status:	critical
<text> value:	A run-time specific string describing the configuration error.
Condition:	After configuration error
Alarm status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	Inspect the run-time specific string to determine the nature of the configuration error. Fix the configuration error using the appropriate tool: web interface, EMS, or *ini* file. Save the configuration and if necessary reset the device.

Table 22-3: acBoardTemperatureAlarm Alarm Trap

Alarm:	acBoardTemperatureAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.3
Default Severity	critical
Event Type:	equipmentAlarm
Probable Cause:	temperatureUnacceptable (50)

Table 22-3: acBoardTemperatureAlarm Alarm Trap

Alarm:	acBoardTemperatureAlarm
Alarm Text:	Board temperature too high
Status Changes:	
Condition:	Temperature is above 60 degrees C (140 degrees F)
Alarm status:	critical
Condition:	After raise, temperature falls below 55 degrees C (131 degrees F)
Alarm status:	cleared
Corrective Action:	Inspect the system. Determine if all fans in the system are properly operating.

Table 22-4: acBoardEvResettingBoard Alarm Trap

Alarm:	acBoardEvResettingBoard
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.5
Default Severity	critical
Event Type:	equipmentAlarm
Probable Cause:	outOfService (71)
Alarm Text:	User resetting board
Status Changes:	
Condition:	When a soft reset is triggered via either web interface or SNMP.
Alarm status:	critical
Condition:	After raise
Alarm status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	A network administrator has taken action to reset the device. No corrective action is needed.

Table 22-5: acFeatureKeyError Alarm Trap

Alarm:	acFeatureKeyError
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.6
Default Severity	critical

Table 22-5: acFeatureKeyError Alarm Trap

Alarm:	acFeatureKeyError
Event Type:	processingErrorAlarm
Probable Cause:	configurationOrCustomizationError (7)
Alarm Text:	Feature key error
Status Changes:	
Condition:	This alarm's support is pending
Alarm status:	
Note:	**This alarm's support is pending**

22.1.2 Component: AlarmManager#0

Table 22-6: acActiveAlarmTableOverflow Alarm Trap

Alarm:	acActiveAlarmTableOverflow
OID:	1.3.6.1.4.15003.9.10.1.21.2.0.12
Default Severity	Major
Event Type:	processingErrorAlarm
Probable Cause:	resourceAtOrNearingCapacity (43)
Alarm Text:	Active alarm table overflow
Status Changes:	
Condition:	Too many alarms to fit in the active alarm table
Alarm status:	Major
Condition:	After raise
Alarm status:	Status stays major until reboot. A clear trap is not sent.
Note:	The status stays major until reboot as it denotes a possible loss of information until the next reboot. If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in the active alarm table.

Table 22-6: acActiveAlarmTableOverflow Alarm Trap

Alarm:	acActiveAlarmTableOverflow
Corrective Action:	Some alarm information may have been lost, but the ability of the device to perform its basic operations has not been impacted. A reboot is the only way to completely clear a problem with the active alarm table. Contact your first-level group.

22.1.3 Component: EthernetLink#0

This trap is related to the Ethernet Link Module (the #0 numbering does not apply on the physical Ethernet link).

Table 22-7: acBoardEthernetLinkAlarm Alarm Trap

Alarm:	acBoardEthernetLinkAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Default Severity	Critical
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Ethernet link alarm: <text>
Status Changes:	
Condition:	Fault on single interface
Alarm status:	Major
<text> value:	Redundant link is down
Condition:	Fault on both interfaces
Alarm status:	critical
<text> value:	No Ethernet link
Condition:	Both interfaces are operational
Alarm status:	cleared
Corrective Action:	Ensure that both Ethernet cables are plugged into the back of the system. Inspect the system's Ethernet link lights to determine which interface is failing. Reconnect the cable or fix the network problem

Table 22-8: acgwAdminStateChange Alarm Trap

Alarm:	acgwAdminStateChange
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.7
Default Severity	Major
Event Type:	processingErrorAlarm
Probable Cause:	outOfService (71)
Alarm Text:	Network element admin state change alarm Gateway is <text>
Status Changes:	
Condition:	Admin state changed to shutting down
Alarm status:	Major
<text> value:	shutting down. No time limit.
Condition:	Admin state changed to locked
Alarm status:	Major
<text> value:	locked
Condition:	Admin state changed to unlocked
Alarm status:	cleared
Corrective Action:	A network administrator has taken an action to lock the device. No corrective action is required.

Table 22-9: acOperationalStateChange Alarm Trap

Alarm:	acOperationalStateChange
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.15
Default Severity	Major
Event Type:	processingErrorAlarm
Probable Cause:	outOfService (71)
Alarm Text:	Network element operational state change alarm. Operational state is disabled.
Note:	**This alarm is raised if the operational state of the node goes to disabled. The alarm is cleared when the operational state of the node goes to enabled.**
Status Changes:	
Condition:	Operational state changed to disabled

Table 22-9: acOperationalStateChange Alarm Trap

Alarm:	acOperationalStateChange
Alarm status:	Major
Condition:	Operational state changed to enabled
Alarm status:	cleared
Note:	**In both ATM and IP systems, the operational state of the node is disabled if the device fails to properly initialize. In ATM systems, the operational state of the node is also disabled if there are no ATM ports available for use. An ATM port is available for use if it is unlocked and enabled.**
Corrective Action:	In ATM and IP systems, check for initialization errors. Look for other alarms and syslogs that might provide additional information about the error. In an ATM system, also check for ATM port status and alarms. If any ATM ports are disabled, then attempt to bring them back into service.

22.1.4 Component: SS7#0

Table 22-10: acSS7LinkStateChangeAlarm Trap

Alarm:	acSS7LinkStateChangeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.19
Default Severity	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Alarm Text:	*** SS7 *** Link %i is %s $s
Status Changes:	
Condition:	Operational state of the SS7 link becomes 'BUSY'.
Alarm status:	Major
<text> value:	%i - <Link number> %s - <state name>: { "OFFLINE", "BUSY", "INSERVICE"} %s – IF link has MTP3 layer, then this string equals: (SP %i linkset %i slc %i) Where: %i - <SP number>

Table 22-10: acSS7LinkStateChangeAlarm Trap

Alarm:	acSS7LinkStateChangeAlarm
	%i - <Link-Set number> %i - <SLC number> Otherwise there is NO additional text.
Additional Info1 varbid	BUSY
Condition:	Operational state of the link becomes 'IN-SERVICE' or 'OFFLINE'.
Alarm status:	cleared
Corrective Action:	For full details see the SS7 section and SS7 MTP2 and MTP3 relevant standards.

Table 22-11: acSS7LinkInhibitStateChangeAlarm Trap

Alarm:	acSS7LinkInhibitStateChangeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.20
Default Severity	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Alarm Text:	*** SS7 *** Link %i (SP %i linkset %i slc %i) is %s
Status Changes:	
Condition:	SS7 link becomes inhibited (local or remote).
Alarm status:	Major
<text> value:	%i - <Link number> %i - <SP number> %i - <Link-Set number> %i - <SLC number> %s - <congestion state>: { "UNINHIBITED", "INHIBITED" }
Additional Info1 varbind	INHIBITED
Condition:	Link becomes uninhibited - local AND remote
Alarm status:	cleared

Table 22-11: acSS7LinkInhibitStateChangeAlarm Trap

Alarm:	acSS7LinkInhibitStateChangeAlarm
Corrective Action:	Make sure the link is uninhibited – on both local and remote sides
Note:	**This alarm is raised for any change in the remote or local inhibition status.**

Table 22-12: acSS7LinkBlockStateChangeAlarm

Alarm:	acSS7LinkBlockStateChangeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.21
No	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Note:	**Support pending**

Table 22-13: acSS7LinkCongestionStateChangeAlarmTrap

Alarm:	acSS7LinkCongestionStateChangeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.22
Default Severity	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Alarm Text:	*** SS7 *** Link %i is %s %s
Status Changes:	
Condition:	SS7 link becomes congested (local or remote).
Alarm status:	Major
<text> value:	%i - <Link number> %s – IF link has MTP3 layer, then this string equals: (SP %i linkset %i slc %i) Where: %i - <SP number> %i - <Link-Set number>

Table 22-13: acSS7LinkCongestionStateChangeAlarmTrap

Alarm:	acSS7LinkCongestionStateChangeAlarm
	%i - <SLC number> Otherwise there is NO additional text. %s - <congestion state>: { "UNCONGESTED", "CONGESTED" }
Additional Info1 varbind	CONGESTED
Condition:	Link becomes un-congested - local AND remote.
Alarm status:	cleared
Corrective Action:	Reduce SS7 traffic on that link.
Note :	**This alarm is raised for any change in the remote or local congestion status.**

Table 22-14: acSS7LinkSetStateChangeAlarm Trap

Alarm:	acSS7LinkSetStateChangeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.23
Default Severity	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Alarm Text:	*** SS7 *** Linkset %i on SP %i is %s
Status Changes:	
Condition:	Operational state of the SS7 link-set becomes BUSY.
Alarm status:	Major
<text> value:	%i - <Link-Set number> %i - <SP number> %s - <state name: { "OFFLINE", "BUSY", "INSERVICE"}
Additional Info1 varbind	BUSY
Condition:	Operational state of the link-set becomes IN-SERVICE or OFFLINE
Alarm status:	cleared

Table 22-14: acSS7LinkSetStateChangeAlarm Trap

Alarm:	acSS7LinkSetStateChangeAlarm
Corrective Action:	For full details see the SS7 section and SS7 MTP3 relevant standards

Table 22-15: acSS7RouteSetStateChangeAlarm Trap

Alarm:	acSS7RouteSetStateChangeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.24
Default Severity	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Alarm Text:	*** SS7 *** Routeset %i on SP %i is %s
Status Changes:	
Condition:	Operational state of the SS7 route-set becomes BUSY
Alarm status:	Major
<text> value:	%i - <Route-Set number> %i - <SP number> %s - <state name: { "OFFLINE", "BUSY", "INSERVICE"}
Additional Info:	BUSY
Condition:	Operational state of the route-set becomes IN-SERVICE or OFFLINE
Alarm status:	cleared
Corrective Action:	For full details see the SS7 section and SS7 MTP3 relevant standards

Table 22-16: acSS7SNSetStateChangeAlarmTrap

Alarm:	acSS7SNSetStateChangeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.25
Default Severity	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Alarm Text:	*** SS7 *** SP %i is %s
Status Changes:	
Condition:	Operational state of the SS7 node becomes BUSY
Alarm status:	Major
<text> value:	%i - <SP number> %s - <state name: { "OFFLINE", "BUSY", "INSERVICE"}
Additional Info1 varbind	BUSY
Condition:	Cleared when the operational state of the node becomes IN-SERVICE or OFFLINE
Alarm status:	cleared
Corrective Action:	Signaling Node must complete its MTP3 restart procedure and become un-isolated For full details see the SS7 section and SS7 MTP3 relevant standards

Table 22-17: acSS7RedundancyAlarm

Alarm:	acSS7RedundancyAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.26
No	Major
Event Type:	communicationsAlarm
Probable Cause:	other
Note:	**Support pending**

22.2 Log Traps (Notifications)

This section details traps that are not alarms. These traps are sent out with the severity varbind value of "indeterminate". These traps do not clear, they do not appear in the alarm history or active tables. One log trap that does send out clear is acPerformanceMonitoringThresholdCrossing.

Table 22-18: acKeepAlive Log Trap

Alarm:	acKeepAlive
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.16
Default Severity	Indeterminate
Event Type:	other (0)
Probable Cause:	other (0)
Alarm Text:	Keep alive trap
Status Changes:	
Condition:	The STUN client in the board is enabled and has either identified a NAT or is not finding the STUN server The *ini* file contains the following line: 'SendKeepAliveTrap=1'
Trap status:	Trap is sent
Note:	**Keep-alive is sent out every x second.x =0. 9 of the time defined in the NatBindingDefaultTimeout parameter**

Table 22-19: acPerformanceMonitoringThresholdCrossing Log Trap

Alarm:	acPerformanceMonitoringThresholdCrossing
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.27
Default Severity	Indeterminate
Event Type:	other (0)
Probable Cause:	other (0)
Alarm Text:	"Performance: Threshold alarm was set ", with source = name of performance counter which caused the trap
Status Changes:	
Condition:	A performance counter has crossed the high threshold
Trap status:	Indeterminate
Condition:	A performance counter has crossed the low threshold
Trap status:	cleared

22.3 Other Traps

The following are provided as SNMP traps and are not alarms.

Table 22-20: coldStart Trap

Trap Name:	coldStart
OID:	1.3.6.1.6.3.1.1.5.1
MIB	SNMPv2-MIB
Note:	This is a trap from the standard SNMP MIB.

Table 22-21: authenticationFailure Trap

Trap Name:	authenticationFailure
OID:	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB

Table 22-22: acBoardEvBoardStarted Trap

Trap Name:	acBoardEvBoardStarted
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
MIB	AcBoard
Severity	cleared
Event Type:	equipmentAlarm
Probable Cause:	Other(0)
Alarm Text:	Initialization Ended
Note:	This is the Enterprise application cold start trap.

22.4 Trap Varbinds

Every Enterprise trap described above provides the following fields (known as 'varbinds'). Refer to the AcBoard MIB for additional details on these varbinds.

- acBoardTrapGlobalsName
- acBoardTrapGlobalsTextualDescription

- acBoardTrapGlobalsSource
- acBoardTrapGlobalsSeverity
- acBoardTrapGlobalsUniqID
- acBoardTrapGlobalsType
- acBoardTrapGlobalsProbableCause
- acBoardTrapGlobalsAdditionalInfo1
- acBoardTrapGlobalsAdditionalInfo2
- acBoardTrapGlobalsAdditionalInfo3

Note that acBoardTrapGlobalsName is actually a number. The value of this varbind is 'X' minus 1, where 'X' is the last number in the trap OID. For example, the 'name' of acBoardEthernetLinkAlarm is '9'. The OID for acBoardEthernetLinkAlarm is 1.3.6.1.4.1.5003. 9.10.1.21.2.0.10.

Reader's Notes

23 Appendix - Customizing the Web Interface

OEM customers incorporating the MG 3200 into their portfolios can customize the device's Web interface to suit their specific corporate logo and product naming conventions.

OEM customers can customize the Web interface's title bar (the defaulttitle bar is shown in the figure, "Web Interface Title Bar", below and an example of a customized title bar is shown in the figure, "Customized Web Interface Title Bar" below.)

Note: The product name appears according to what is provided and utilized together with the Web Interface.

Equation 2: Web Interface Title Bar

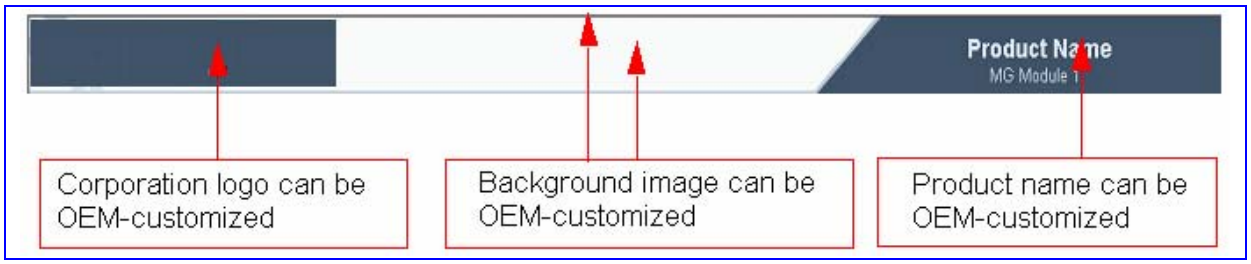


Figure 23-1: Customized Web Interface Title Bar

23.1 Company & Product Bar Components

The Title bar is composed of 3 components:

- Replacing the main corporation logo - refer to "Replacing the Main Corporate Logo" on page 397
- Replacing the title bar's background image file - refer to "Replacing the Title Bar's Background Image File" on page 400
- Customizing the product's name - Refer to "Customizing the Product's Name" on page 401

23.2 Replacing the Main Corporate Logo

The main corporate logo can be replaced either with a different logo image file (refer to "Replacing the Main Corporate Logo with an Image File" below) or with a text string' (refer to Replacing the Main Corporate Logo with a Te'xt String.)

Note: When the main corporate logo is replaced, the defaultlogo in the main menu bar on the left (refer to "About the Web Interface Screen" on page 146) and the defaultlogo in the Software Upgrade Wizard (refer to "Software Upgrade Wizard" on page 190) disappear.

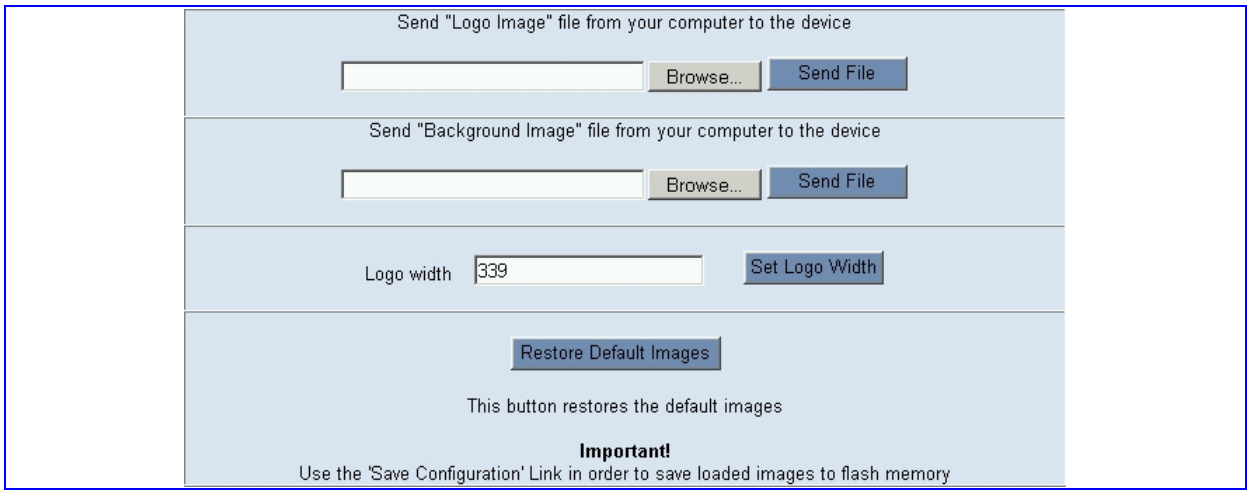
23.2.1 Replacing the Main Corporate Logo with an Image File

Note: Use a gif, jpg or jpeg file for the logo image. It is important that the image file has a fixed height of 59 pixels (the width can be configured). The total size limit for the image files is 128 k bytes if both files are loaded. Each file type (Logo file or BKG file) should not exceed 64 k bytes).

➢ **To replace the default logo with your own corporate logo via the Web interface, take these 8 steps:**

1. Access the Embedded Web Server (refer to “Accessing the Embedded Web Server” on page 144).
2. In the browser's **URL** field, enter the IP address of the location of the Web Interface Application, followed by /**AdminPage**.
3. If you have not accessed this page for a while, you are prompted for your user name and Password. Enter them and press **OK**.
4. On the Main-menu bar to the left, click the **Logo Image Download** option. The Image Download screen appears.

Figure 23-2: Logo Image Download Screen



5. Click the **Browse** button in the **Send Logo Image File from your computer to the device** box. Navigate to the folder that contains the logo image file you want to download.
6. Click the **Send File** button. The file is sent to the device. When the download is complete, the screen is automatically refreshed and the new logo image is displayed.

7. Check the appearance of the logo to verify that it appears as desired. If you want to modify the width of the logo (the default width is 339 pixels), in the **Logo Width** field, enter the new width (in pixels) and press the **Set Logo Width** button.
8. Save the image to flash memory by clicking the Save Configuration button on the Save Configuration screen. The new logo appears on all Web interface screens.

Note: If you encounter any problem during the loading of the files, or you want to restore the default images, click the **Restore Default Images** button.

➢ To replace the default logo with your own corporate logo image via the ini file, take these 2 steps:

1. Place your corporate logo image file in the same folder in which the device's ini file is located (i.e. the same location defined in the BootP/TFTP server). For detailed information on the BootP/TFTP server, refer to the Appendix, "BootP/TFTP Server" on page 223 .
2. Add/modify the two ini file parameters in the table below according to the procedure described in "Software Upgrade Wizard" on page 190.

Note: Loading the device's ini file via the 'Configuration File' screen in the Web interface does not load the corporate logo image file as well.

Table 23-1: Customizable Logo ini File Parameters for the Image File

Parameter	Description
LogoFileName	The name of the image file containing your corporate logo. Use a gif, jpg or jpeg image file. The default is the provided logo file. **Note:** The length of the name of the image file is limited to 47 characters.
LogoWidth	Width (in pixels) of the logo image. **Note:** The optimal setting depends on the resolution settings. The default value is 339, which is the width of the displayed logo.

23.2.2 Replacing the Main Corporate Logo with a Text String

The main corporate logo can be replaced with a text string. To replace the default logo with a text string via the Web interface, modify the two *ini* file parameters in the table below according to the procedure described in"Modifying '*ini*' File Parameters via the Web Interface's AdminPage" on page 402.

Table 23-2: Customizable Logo ini File Parameters for the String Text

Parameter	Description
UseWebLogo	0 = Logo image is used (default value). 1 = Text string is used instead of a logo image.
WebLogoText	Text string that replaces the logo image. The string can be up to 15 characters.

23.3 Replacing the Background Image File

The background image file is repeated across the width of the screen. The number of times the image is repeated depends on the width of the background image and screen resolution. When choosing your background image, keep this in mind.

Note: Use a gif, jpg or jpeg file for the background image. It is important that the image file has a fixed height of 59 pixels. The total size limit for the image files is 128 k bytes if both files are loaded. Each file type (Logo file or BKG file) should not exceed 64 k bytes)

➢ To replace the background image via the Web interface, take these 7 steps:

1. Access the Embedded Web Server (refer to “Accessing the Embedded Web Server” on page 144).
2. In the browser's **URL** field, enter the IP address of the location of the Web Interface Application, followed by /**AdminPage**.
3. If you have not accessed this page for a while, you are prompted for your user name and Password. Enter them and press **OK**.
4. On the Main-menu bar to the left, click the **Image Download** option. The Image Download screen appears.(shown in the figure, 'Image Download Screen' above).
5. Click the **Browse** button in the **Send Background Image File from your computer to gateway** box. Navigate to the folder that contains the background image file you want to download.
6. Click the **Send File** button. The file is sent to the device. When the download is complete, the screen is automatically refreshed and the new background image is displayed.
7. Save the image to the flash memory by clicking the **Save Configuration** button on the Save Configuration screen. The new background appears on all Web interface screens.

Note: If you encounter any problem during the loading of the files, or you want to restore the default images, click the **Restore Default Images** button.

➢ To replace the background image via the ini file, take these 2 steps:

1. Place your background image file in the same folder in which the device's ini file is located (i.e. the same location defined in the BootP/TFTP server). For detailed information on the BootP/TFTP server, refer to the Appendix, 'BootP/TFTP Server" on page 223.
2. Add/modify the ini file parameters in the table below according to the procedure described "Software Upgrade Wizard" on page 190.

Note: Loading the device's ini file via the Configuration File screen in the Web interface does not load the background image file as well.

Table 23-3: Customizable Background ini File Parameters

Parameter	Description
BkgImageFileName	The name of the file containing the new background. Use a gif, jpg or jpeg image file. The default is provided background file. **Note:** The length of the name of the image file is limited to 47 characters.

23.4 Customizing the Product Name

The Product Name text string can be modified according to OEMs specific requirements.

- To replace the default product name with a text string via the Web interface, modify the two *ini* file parameters in the table below according to the procedure described in' 'Modifying '*ini*' File Parameters via the Web Interface's AdminPage" on page 402.
- To replace the default product name with a text string via the *ini* file, add/modify the two *ini* file parameters in the table below according to the procedure described in' 'Software Upgrade Wizard" on page 190.

Table 23-4: Customizable Product Name ini File Parameters

Parameter	Description
UseProductName	0 = Don't change the product name (default). 1 = Enable product name change.
UserProductName	Text string that replaces the product name. The default is "MG 3200". The string can be up to 29 characters.

23.4.1 Customizing the Web Browser Title Bar

Figure 23-3: Default Web Browser Title Bar

Upon customizing the logo section of the screen as described in "Replacing the Main Corporate Logo" on page 397, the default string on the Web browser's title bar changes to the text string held in the WebLogoText parameter. If this parameter holds an empty string, the browser's title bar contains only its own name.

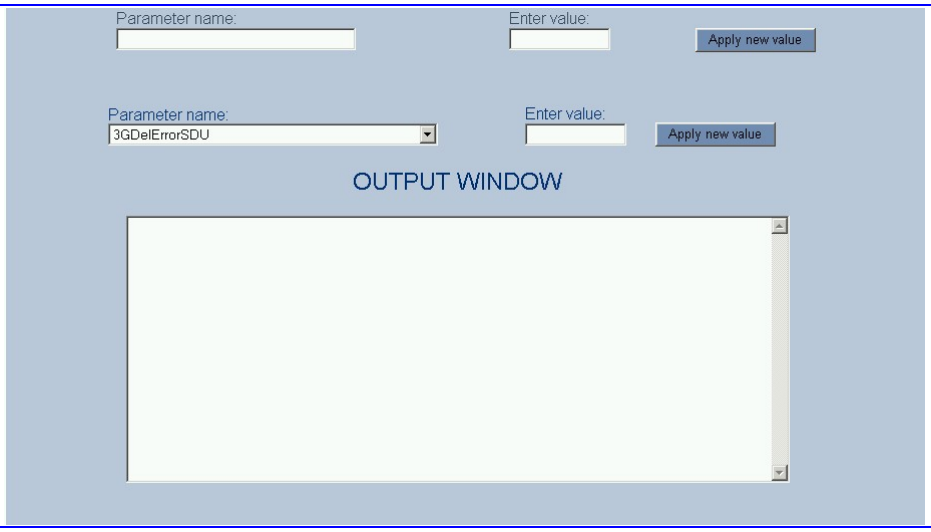
23.5 Modifying ini File Parameters via the Web Interface's AdminPage

➢ To modify ini file parameters via the AdminPage, take these 7 steps:

1. Open the Web Interface Application, using the directions in the Device Management section of the accompanying the MG 3200 user's manual.
2. In the browser's **URL** field, enter the IP address of the location of the Web Interface Application, followed by /**AdminPage**.
3. If you have not accessed this page for a while, you are prompted for your user name and Password. Enter them and press **OK**.

4. Click the **INI Parameters** option, the ini Parameters screen is displayed.

Figure 23-4: ini Parameters Screen



5. In the **Parameter Name** dropdown list, select the required ini file parameter.
6. In the **Enter Value** text box to the right, enter the parameter's new value.
7. Click the **Apply new value** button to the right. The ini Parameters screen is refreshed, the parameter name with the new value appears in the fields at the top of the screen and the Output Window displays a log displaying information on the operation.

Note: You cannot load the image files (e.g., logo/background image files) to the device by choosing a file name parameter in this screen.

Reader's Notes

24 Appendix – Disable MG 3200 Traffic Prior to Software Upgrade

Disabling MG3200 traffic from Call Server side involves performing 'Manual Busy' on all the trunks on the MG3200.

Maintenance actions (e.g. Post, BSY, RTS, etc…) on trunks can be performed via the Trunk Maintenance Manager (TMM). For TMM overview, refer to section 'Trunk Maintenance Manager' in the appropriate Solution-level Basics NTP doc (NN1044x-100) (x can be from 1 to 6, depending on the particular Solution).

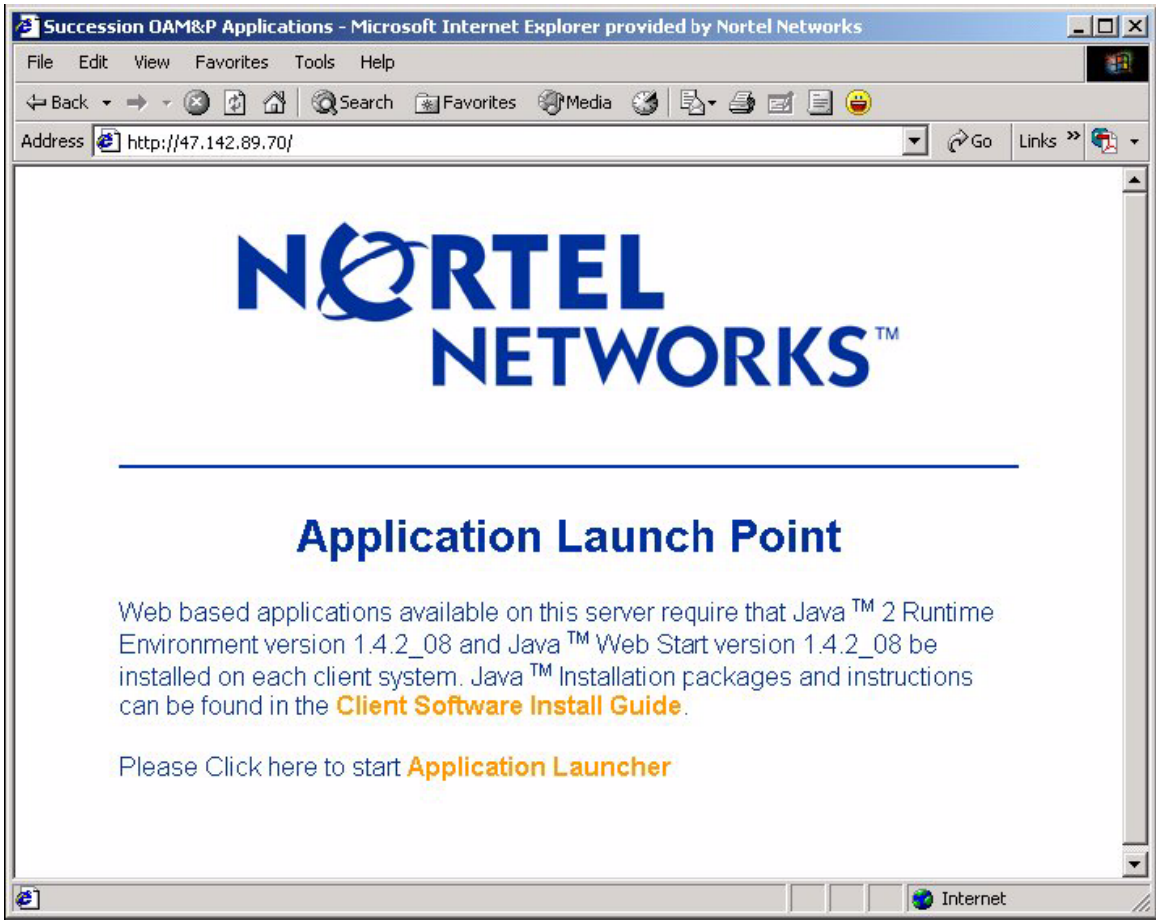
The following guidelines are for Manual Busy the trunks using TMM:

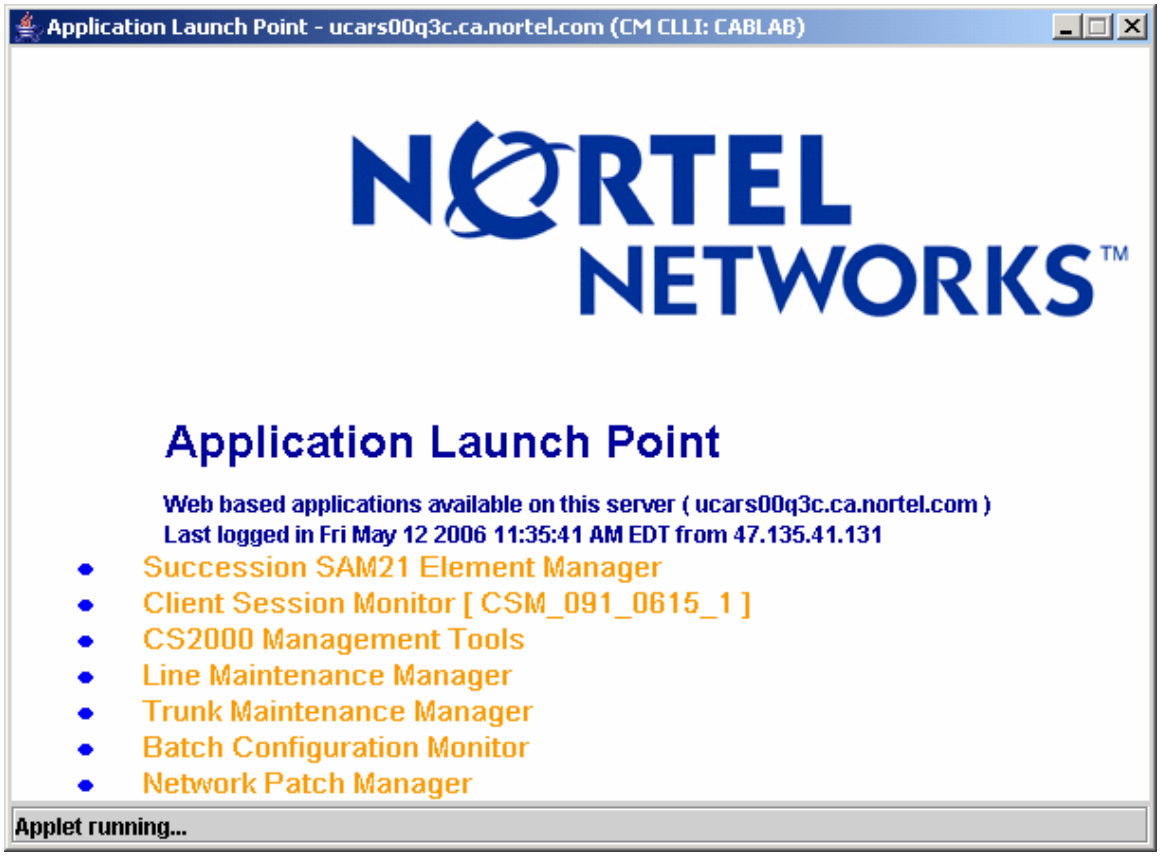
1. Access the Trunk Maintenance Manager

For info on how to access the Trunk Maintenance Manager, refer to the procedure “Launching the CS 2000 Management Tools and NPM client applications” in the ATM/IP Security and Administration document, NN10402-600.

From the Application Launch Point screen, select ‘Trunk Maintenance Manager’ application.

Sample screenshots:



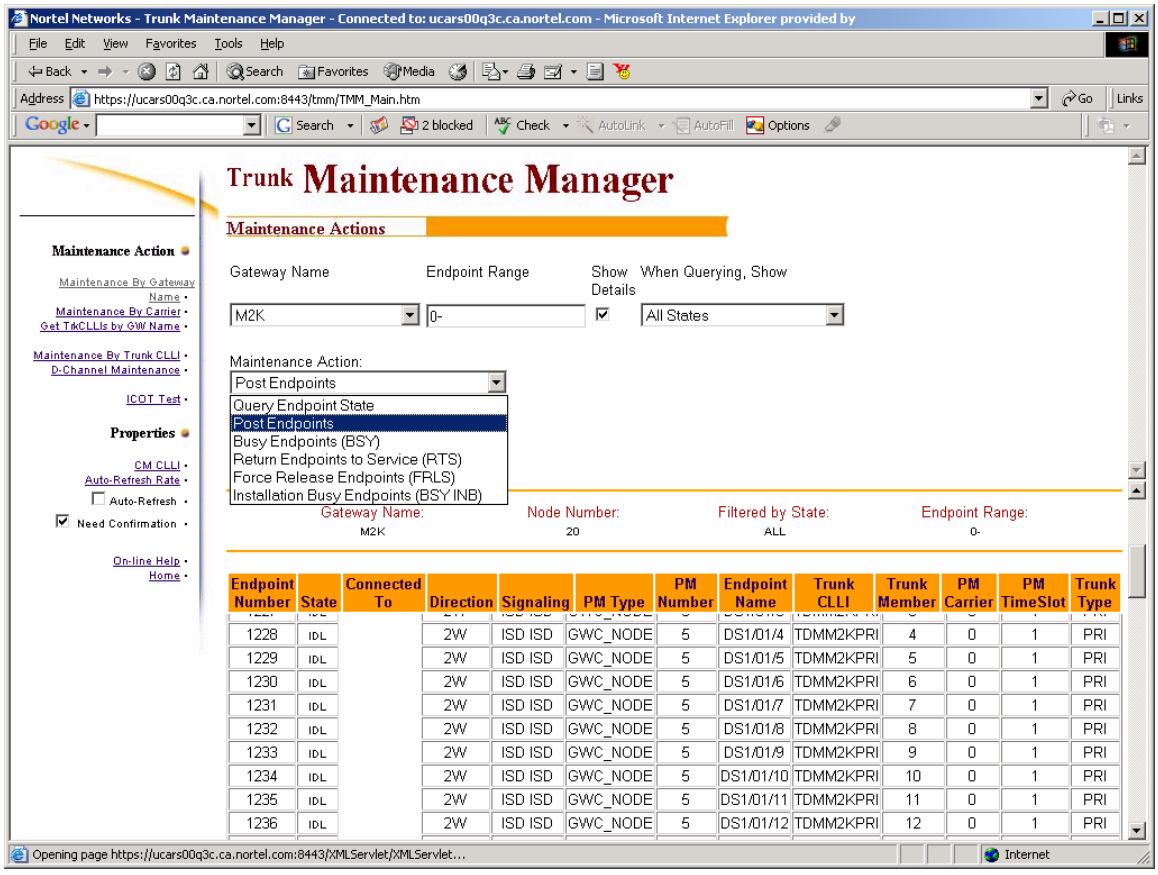


For procedures on how to perform trunk maintenance activities using the TMM, refer to the procedure 'Performing Trunk Maintenance using the Trunk Maintenance Manager' in the ATM/IP Solution-level Fault Management document, NN10408-900.

2. From the Trunk Maintenance Manager screen, post the trunks:
   a. select 'Maintenance By Gateway Name' under the 'Maintenance Action' section.
   b. From the 'Gateway Name' pull-down list, select the MG3200 Gateway name
   c. Check mark on the 'Show Details' box.
   d. From the 'Maintenance Action' pull-down list, select 'Post Endpoints'
   e. Click Go

All the trunks on the specific MG3200 are displayed. Verify the Trunk CLLI to ensure they are the right trunks to be Man Bsy'ed.

Sample screenshot:



3. Busy out the trunks:
From the 'Maintenance Action' pull-down list, select 'Busy Endpoints (BSY)'

4. Verify that the state of the trunks are in Man Busy state

25 Appendix – Resume MG 3200 Traffic after Software Upgrade is Completed

Resume MG3200 traffic from Call Server side after completion of Software Upgrade involves performing 'Return to Service' on all the trunks on the MG3200.

Follow the same procedure described in Appendix – Disable MG 3200 Traffic Prior to Software Upgrade on page 405, with the exception of step 3 and 4, where the following actions are to be performed instead:

- RTS the trunks:

From the 'Maintenance Action' pull-down list, select 'Return Endpoints to Servive (RTS)'

- Verify that the state of the trunks are in IDL state

26 Appendix - Regulatory Information

Safety Notices

Installation and service of this gateway must only be performed by authorized, qualified service personnel.

Industry Canada Notice

This equipment meets the applicable Industry Canada Terminal Equipment technical specifications. This is confirmed by the registration numbers. The abbreviation, IC, before the registration number signifies that registration was performed based on a declaration of conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Caution Laser

The SB-1610 board may contain a Class I Laser/LED emitting device, as defined by 21CFR 1040 and IEC825.

Do NOT stare directly into the beam or fiber optic terminations as this can damage your eyesight.

Digital Device Warnings

This equipment complies with Part 68 of the FCC rules and the requirements adopted by ACTA. On the interface card module of this equipment is a label that contains a product identifier in the format US: AC1ISNANTP1610. If requested this number must be provided to the telephone company.

The Telephone company may make changes in the facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service. Should you experience trouble with this telephone equipment, contact: Nortel at www.nortel.com. **Do not attempt to repair this equipment!**

Facility Interface Code: 04DU9.BN, 04DU9.DN, 04DU9.1KN, 4DU9.ISN

Service Order Code: 6.0N

USOC Jack Type: RJ21X or RJ48C

It this gateway causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also you will be advised of your right to file complaint with the FCC if you believe it is necessary.

Network Information and Intent of Use

The products are for access to ISDN at 2048 kb/s and for access to G.703 Leased lines at 2048 kb/s.

Network Compatibility

The products support the Telecom networks in EU that comply with TBR4 and TBR13.

Telecommunication Safety

The safety status of each port is declared and detailed in the table below:

Ports	Safety Status
E1 or T1	TNV-1
Ethernet (100 Base-T)	SELV

TNV-1: Telecommunication network voltage circuits whose normal operating voltages do not exceed the limits for SELV under normal operating conditions and on which over voltages from telecommunication networks are possible.

SELV: Safety extra low voltage circuit.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

27 Index

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W


Original
printed on
recycled paper
and available on
CD or Web site


CERTIFIED QMS
SI
ISO 9001:
2000
THE STANDARDS INSTITUTION OF ISRAEL