AudioCodes Mediant™ Media Gateways

SIP

Mediant 2000

User's Manual

Version 5.6

Document #: LTRT-68808

November 2008

Table of Contents

List of Figures

List of Tables

Notice

This document describes the AudioCodes Mediant 2000 SIP gateway.

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, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/support.

This document is subject to change without notice.

Date Published: November-18-2008

Tip: 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 **ALT** and ← keys

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, CTI^2, CTI Squared, InTouch, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, 3GX, TrunkPack, VoicePacketizer, VoIPerfect, What's Inside Matters, Your Gateway To VoIP, are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.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

Document #	Manual Name
LTRT-523xx (where *xx* is the document version)	Product Reference Manual
LTRT-690xx	Mediant 3000 & Mediant 2000 & TP Series SIP Release Notes
LTRT-701xx	Mediant 2000 & IPmedia 2000 SIP-MGCP-MEGACO Installation Manual
LTRT-665xx	CPE Configuration Guide for IP Voice Mail
LTRT-400xx	IP-to-IP SIP Call Routing Application Note

Warning: The device is supplied as a sealed unit and must only be serviced by qualified service personnel.

Note: The term *device*, used throughout this manual, refers to the Mediant 2000 media gateway, unless otherwise specified.

Note: Where ‘network’ appears in this manual, it means Local Area Network (LAN), Wide Area Network (WAN), etc. accessed via the device’s Ethernet interface.

Note: The terms *IP-to-Tel* and *Tel-to-IP* refer to the direction of the call relative to the AudioCodes device. *IP-to-Tel* refers to calls received from the IP network and destined to the PSTN/PBX (i.e., telephone connected directly or indirectly to the device); *Tel-to-IP* refers to calls received from the PSTN/PBX and destined for the IP network.

1 Overview

This manual provides you with the information for installing, configuring, and operating the Mediant 2000 SIP gateway (referred to throughout this manual as *device*).

The device is a SIP-based Voice-over-IP (VoIP) media gateway. the device enables voice, fax, and data traffic to be sent over the same IP network.

The device provides excellent voice quality and optimized packet voice streaming over IP networks. The device uses the award-winning, field-proven VoIPerfect™ voice compression technology, typically implemented in AudioCodes products.

The device incorporates 1, 2, 4, 8 or 16 E1, T1, or J1 spans for direct connection to the Public Switched Telephone Network (PSTN) / Private Branch Exchange (PBX) through digital telephony trunks. The device also provides SIP trunking capabilities for Enterprises operating with multiple Internet Telephony Service Providers (ITSP) for VoIP services. The device includes two 10/100Base-TX Ethernet ports, providing redundancy connection to the network.

The device supports up to 480 simultaneous VoIP or Fax over IP (FoIP) calls, supporting various Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) protocols such as EuroISDN, North American NI2, Lucent™ 4/5ESS, Nortel™ DMS100 and others. In addition, it supports different variants of Channel Associated Signaling (CAS) protocols for E1 and T1 spans, including MFC R2, E&M immediate start, E&M delay dial/start, loop start and ground start.

The device, best suited for large and medium-sized VoIP applications is a compact device, comprising a 19-inch, 1U chassis with optional dual AC or single DC power supplies. The deployment architecture can include several devices in branch or departmental offices, connected to local PBXs. Call routing is performed by the devices using internal routing or SIP Proxy(s).

The device enables users to make cost-effective, long distance or international telephone/fax calls between distributed company offices, using their existing telephones/fax. These calls can be routed over the existing network using state-of-the-art compression techniques, ensuring that voice traffic uses minimum bandwidth.

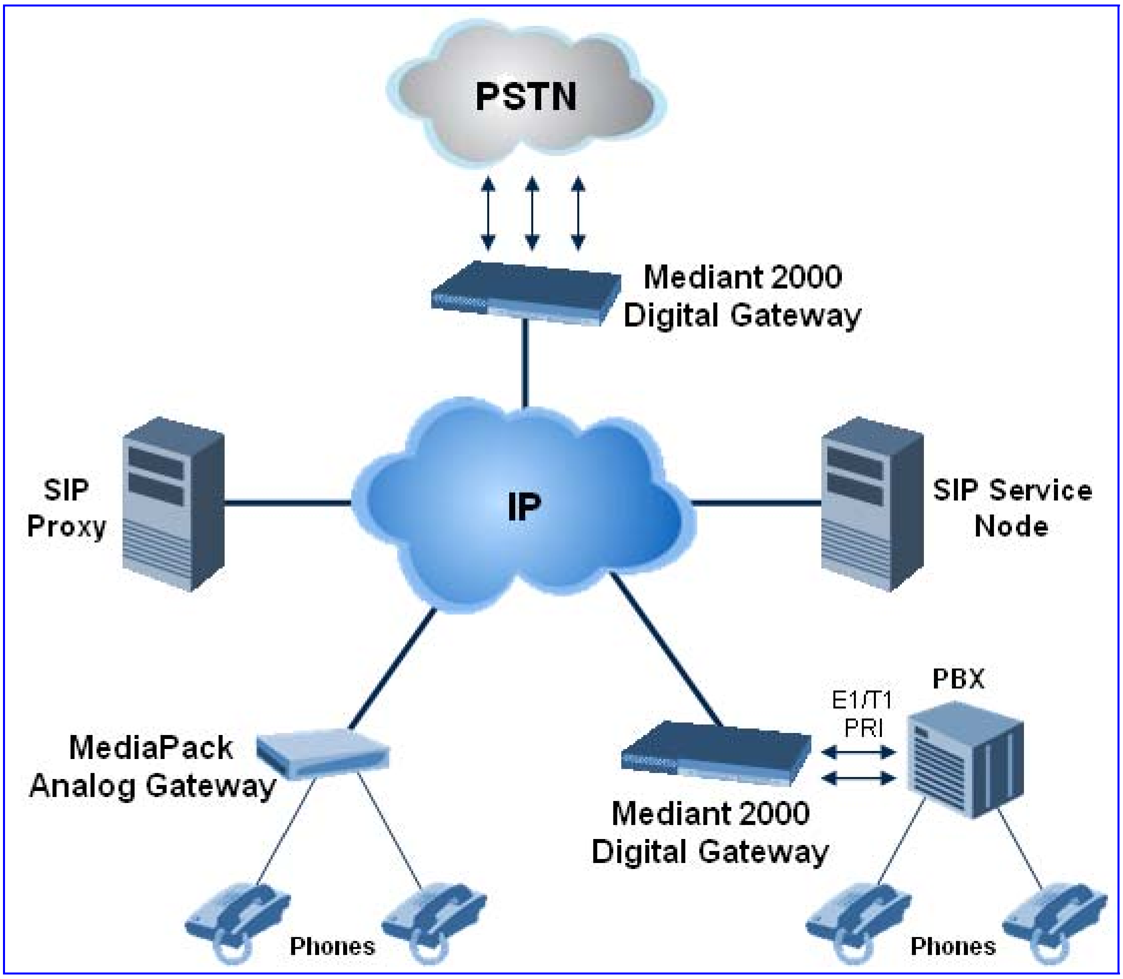
The device can also route calls over the network using SIP signaling protocol, enabling the deployment of Voice over Packet solutions in environments where access is enabled to PSTN subscribers by using a trunking device. This provides the ability to transmit voice and telephony signals between a packet network and a TDM network.

Notes:

- The device is offered as a 1-module (up to 240 channels or 8 trunk spans) or 2-module (for 480 channels or 16 trunk spans only) platform. The latter configuration supports two TrunkPack modules, each having its own IP address. Configuration instructions in this document relate to the device as a 1-module platform and must be repeated for the second module as well.
- For channel capacity, refer to the device's specifications in "Selected Technical Specifications" on page 409.

The figure below illustrates a typical device applications VoIP network:

Figure 1-1: Mediant 2000 Typical Application



1.1 SIP Overview

Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol used on the gateway for creating, modifying, and terminating sessions with one or more participants. These sessions can include Internet telephone calls, media announcements, and conferences.

SIP invitations are used to create sessions and carry session descriptions that enable participants to agree on a set of compatible media types. SIP uses elements called Proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies and provide features to users.

SIP also provides a registration function that enables users to upload their current locations for use by Proxy servers. SIP implemented in the gateway, complies with the Internet Engineering Task Force (IETF) RFC 3261 (refer to http://www.ietf.org).

2 Configuration Concepts

You can configure the device's parameters (including upgrading the software, and uploading configuration and auxiliary files), using the following tools:

- An HTTP-based Embedded Web Server (Web interface), using any standard Web browser (described in "Web-based Management" on page 19).
- A configuration file referred to as the *ini* file (refer to "ini File Configuration" on page 255).
- Simple Network Management Protocol (SNMP) browser software (refer to the *Product Reference Manual*).
- AudioCodes' Element Management System (refer to *AudioCodes' EMS User's Manual* or *EMS Product Description*).

Note: To initialize the device by assigning it an IP address, a firmware file (*cmp*), and a configuration file (*ini* file), you can use AudioCodes' BootP/TFTP utility, which accesses the device using its MAC address (refer to the *Product Reference Manual*).

Reader’s Notes

3 Web-Based Management

The device's Embedded Web Server (*Web interface*) provides FCAPS (fault management, configuration, accounting, performance, and security) functionality. The Web interface allows you to remotely configure your device for quick-and-easy deployment, including uploading of configuration (software upgrade) and auxiliary files, and resetting the device. The Web interface provides real-time, online monitoring of the device, including display of alarms and their severity. In addition, it displays performance statistics of voice calls and related traffic parameters.

The Web interface provides a user-friendly, graphical user interface (GUI), which can be accessed using any standard Web browser (e.g., Microsoft™ Internet Explorer). Access to the Web interface is controlled by various security mechanisms such as login user name and password, read / write privileges, and limiting access to specific IP addresses.

Notes:

- The Web interface allows you to configure most of the device's parameters. Those parameters that are not available in the Web interface can be configured using the *ini* file.
- Certain Web interface pages are feature-key dependant, and therefore, only appear if your device's feature key supports the features relating to these pages (refer to “Upgrading the Software Upgrade Key” on page 233).
- Throughout this section, parameters enclosed in square brackets [...] depict the *ini* file parameters for configuring the device using the *ini* file.

3.1 Computer Requirements

To use the device's Web interface, the following is required:

- A connection to the Internet network (World Wide Web).
- A network connection to the device's Web interface.
- One of the following Web browsers:
  - Microsoft™ Internet Explorer™ (version 6.0 or later).
  - Netscape™ Navigator™ (version 7.2 or later).
  - Mozilla Firefox® (version 1.5.0.10 or later).
- Recommended screen resolution of 1024 x 768 pixels, or 1280 x 1024 pixels.

Note: Your Web browser must be JavaScript-enabled in order to access the Web interface.

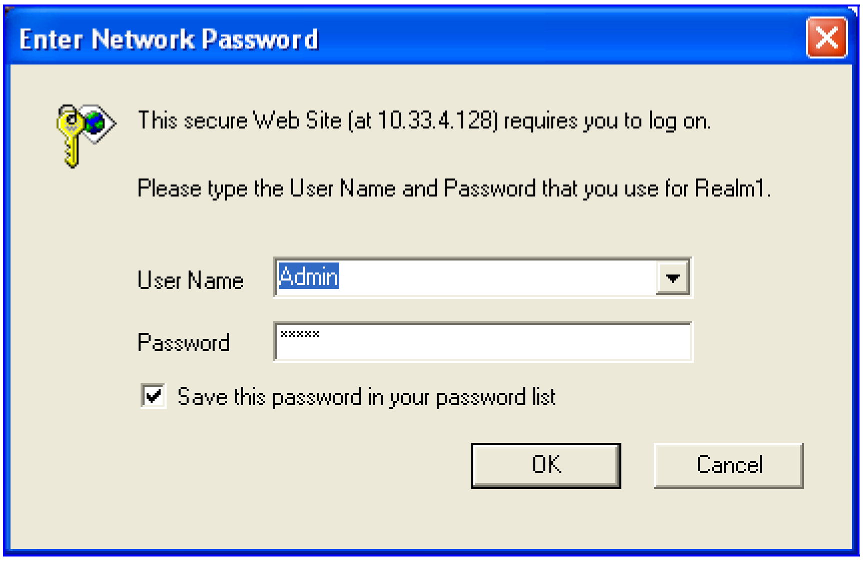
3.2 Accessing the Web Interface

The Web interface can be opened using any standard Web browser (refer to "Computer Requirements" on page 19). When initially accessing the Web interface, use the default user name ('Admin') and password ('Admin'). For changing the login user name and password, refer to "Configuring the Web User Accounts" on page 99).

➢ To access the Web interface, take these 4 steps:

1. Open a standard Web browser application.
2. In the Web browser's Uniform Resource Locator (URL) field, specify the device's IP address (e.g., http://10.1.10.10); the Web interface's 'Enter Network Password' dialog box appears, as shown in the figure below:

Figure 3-1: Enter Network Password Screen



Enter Network Password

This secure Web Site (at 10.33.4.128) requires you to log on.

Please type the User Name and Password that you use for Realm1.

User Name: Admin

Password: *****

☑ Save this password in your password list

3. In the 'User Name' and 'Password' fields, enter the case-sensitive, user name and password.
4. Click the **OK** button; the Web interface is accessed, displaying the 'Home' page (for a detailed description of the 'Home' page, refer to "Using the Home Page" on page 46).

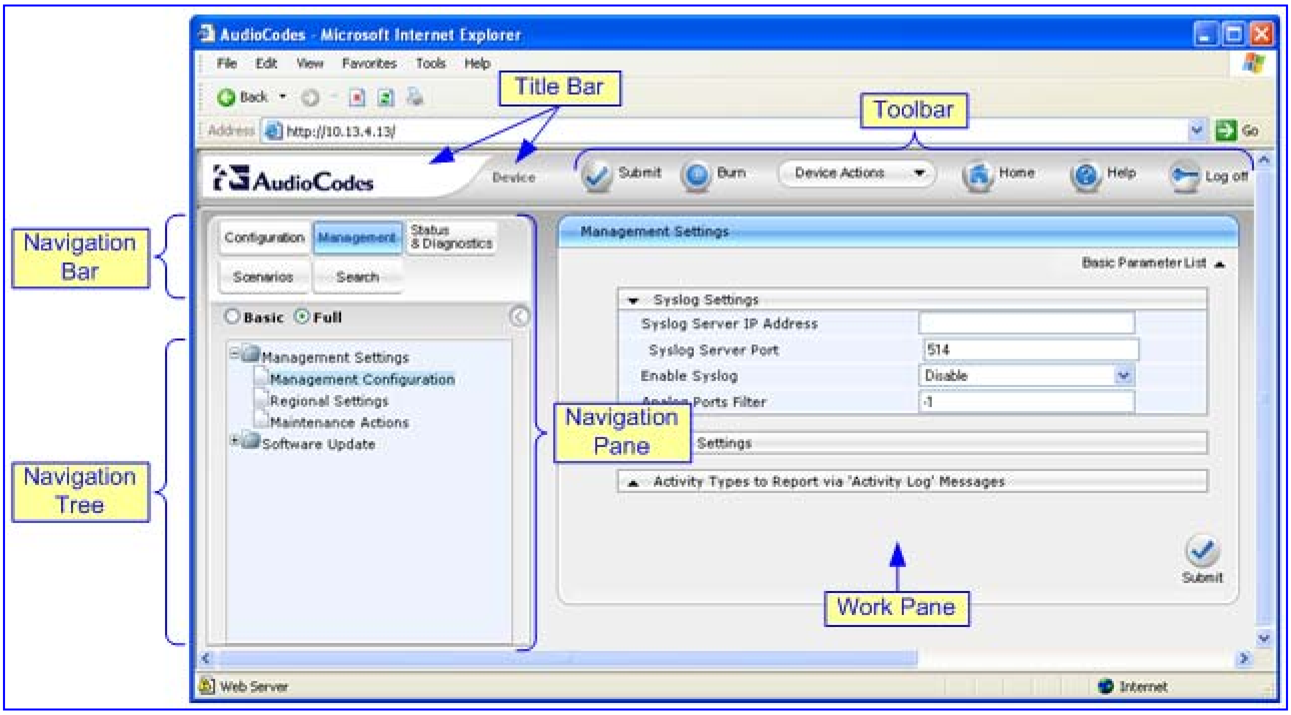
Note: If access to the device's Web interface is denied ("Unauthorized") due to Microsoft Internet Explorer security settings, perform the following troubleshooting procedures:

1. Delete all cookies in the Temporary Internet Files folder. If this does not resolve the problem, the security settings may need to be altered (continue with Step 2).
2. In Internet Explorer, navigate to **Tools** menu > **Internet Options** > **Security** tab > **Custom Level**, and then scroll down to the Logon options and select **Prompt for username and password**. Select the **Advanced** tab, and then scroll down until the HTTP 1.1 Settings are displayed and verify that **Use HTTP 1.1** is selected.
3. Quit and start the Web browser again.

3.3 Getting Acquainted with the Web Interface

The figure below displays the general layout of the Graphical User Interface (GUI) of the Web interface:

Figure 3-2: Main Areas of the Web Interface GUI



Syslog Server IP Address:
Syslog Server Port: 514
Enable Syslog: Disable
Analog Ports Filter: -1

The Web GUI is composed of the following main areas:

- **Title bar:** Displays the corporate logo and product name. For replacing the logo with another image or text, refer to "Replacing the Corporate Logo" on page 41. For customizing the product name, refer to "Customizing the Product Name" on page 44.
- **Toolbar:** Provides frequently required command buttons for configuration (refer to "Toolbar" on page 21).
- **Navigation Pane:** Consists of the following areas:
  - **Navigation bar:** Provides tabs for accessing the configuration menus (refer to "Navigation Tree" on page 23), creating a Scenario (refer to "Scenarios" on page 34), and searching *ini* file parameters that have corresponding Web interface parameters (refer to "Searching for Configuration Parameters" on page 32).
  - **Navigation tree:** Displays the elements pertaining to the tab selected on the Navigation bar (tree-like structure of the configuration menus, Scenario Steps, or Search engine) .
- **Work pane:** Displays configuration pages where all configuration is performed (refer to "Working with Configuration Pages" on page 25).

3.3.1 Toolbar

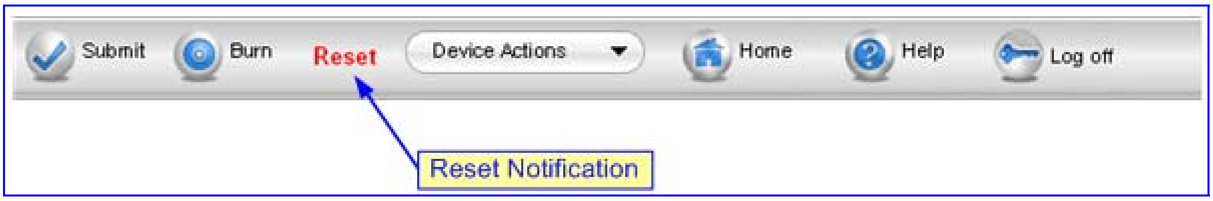
The toolbar provides command buttons for quick-and-easy access to frequently required commands, as described in the table below:

Table 3-1: Description of Toolbar Buttons

Icon	Button Name	Description
✓	**Submit**	Applies parameter settings to the device (refer to "Saving Configuration" on page 230). **Note:** This icon is grayed out when not applicable to the currently opened page.
◉	**Burn**	Saves parameter settings to flash memory (refer to "Saving Configuration" on page 230).
Device Actions ▾	**Device Actions**	Opens a drop-down menu list with frequently needed commands: ▪ **Load Configuration File:** opens the 'Configuration File' page for loading an *ini* file (refer to "Backing Up and Restoring Configuration" on page 240). ▪ **Save Configuration File:** opens the 'Configuration File' page for saving the *ini* file to a PC (refer to "Backing Up and Restoring Configuration" on page 240). ▪ **Reset:** opens the 'Maintenance Actions' page for resetting the device (refer to "Resetting the Device" on page 228). ▪ **Software Upgrade Wizard:** opens the 'Software Upgrade Wizard' page for upgrading the device's software (refer to "Software Upgrade Wizard" on page 236).
⌂	**Home**	Opens the 'Home' page (refer to "Using the Home Page" on page 46).
?	**Help**	Opens the Online Help topic of the currently opened configuration page in the Work pane (refer to "Getting Help" on page 45).
🔑	**Log off**	Logs off a session with the Web interface (refer to "Logging Off the Web Interface" on page 49).

Note: If you modify parameters that take effect only after a device reset, after you click the **Submit** button, the toolbar displays the word "Reset" (in red color), as shown in the figure below. This is a reminder to later save ('burn') your settings to flash memory and reset the device.

Figure 3-3: "Reset" Displayed on Toolbar



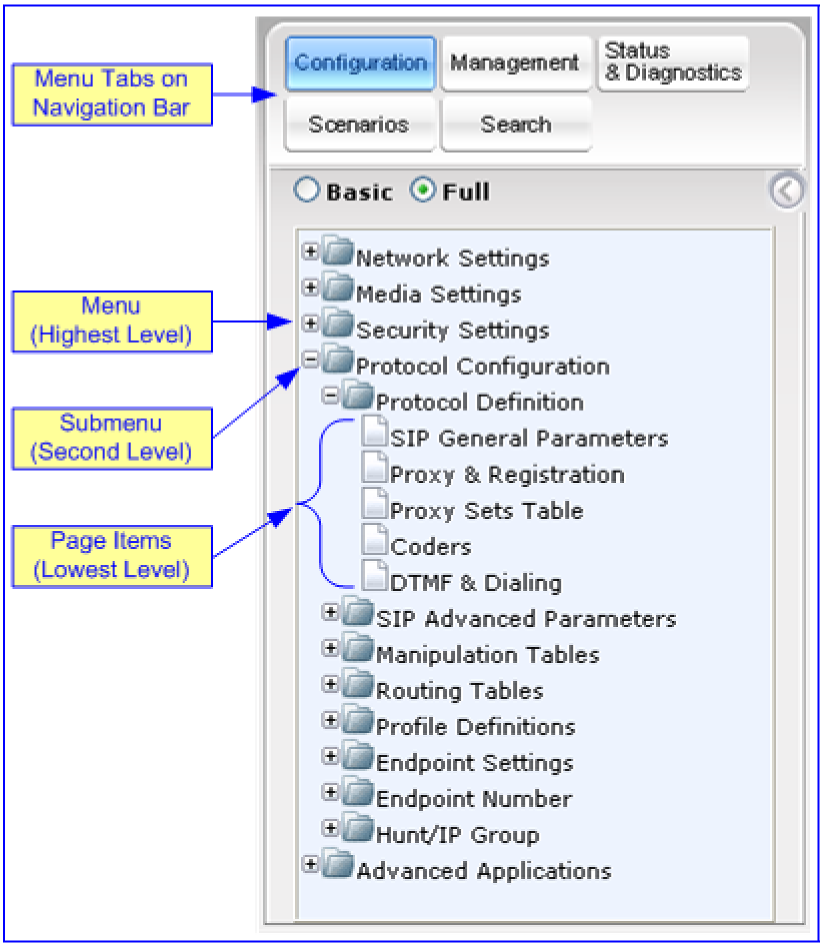
3.3.2 Navigation Tree

The Navigation tree, located in the Navigation pane, displays the menus (pertaining to the menu tab selected on the Navigation bar) used for accessing the configuration pages. The Navigation tree displays a tree-like structure of menus. You can easily drill-down to the required page item level to open its corresponding page in the Work pane.

The terminology used throughout this manual for referring to the hierarchical structure of the tree is as follows:

- *menu*: first level (highest level)
- *submenu*: second level - contained within a menu.
- *page item*: last level (lowest level in a menu) - contained within a menu or submenu.

Figure 3-4: Terminology for Navigation Tree Levels



➢ To view menus in the Navigation tree, take this step:

- On the Navigation bar, select the required tab:
  - **Configuration** (refer to "Configuration Tab" on page 50)
  - **Management** (refer to "Management Tab" on page 220)
  - **Status & Diagnostics** (refer to "Status & Diagnostics Tab" on page 241)

➢ To navigate to a page, take these 2 steps:

1. Navigate to the required page item, by performing the following:
   - Drilling-down using the **plus** ⊞ signs to expand the menus and submenus
   - Drilling-up using the **minus** ⊟ signs to collapse the menus and submenus
2. Select the required page item; the page opens in the Work pane.

3.3.2.1 Displaying Navigation Tree in Basic and Full View

You can view an expanded or reduced Navigation tree display regarding the number of listed menus and submenus. This is relevant when using the configuration tabs (**Configuration**, **Management**, and **Status & Diagnostics**) on the Navigation bar.

The Navigation tree menu can be displayed in one of two views:

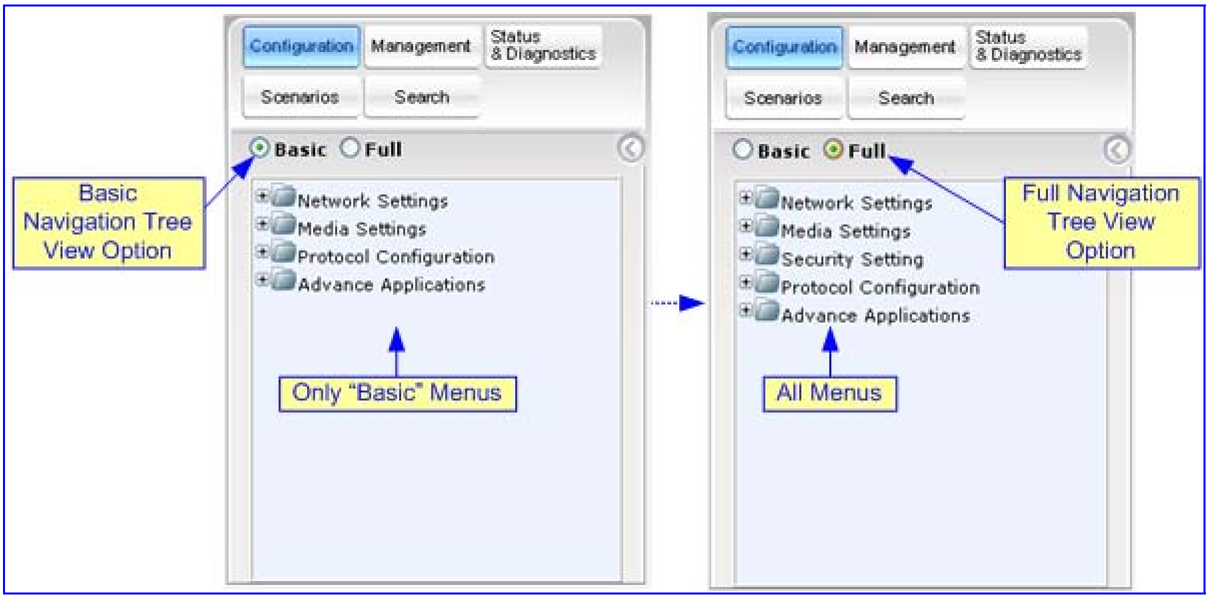
- **Basic:** displays only commonly used menus
- **Full:** displays all the menus pertaining to a configuration tab.

The advantage of the Basic view is that it prevents "cluttering" the Navigation tree with menus that may not be required. Therefore, a Basic view allows you to easily locate required menus.

➢ To toggle between Full and Basic view, take this step:

- Select the **Basic** option (located below the Navigation bar) to display a reduced menu tree; select the **Full** option to display all the menus. By default, the **Basic** option is selected.

Figure 3-5: Navigation Tree in Basic and Full View



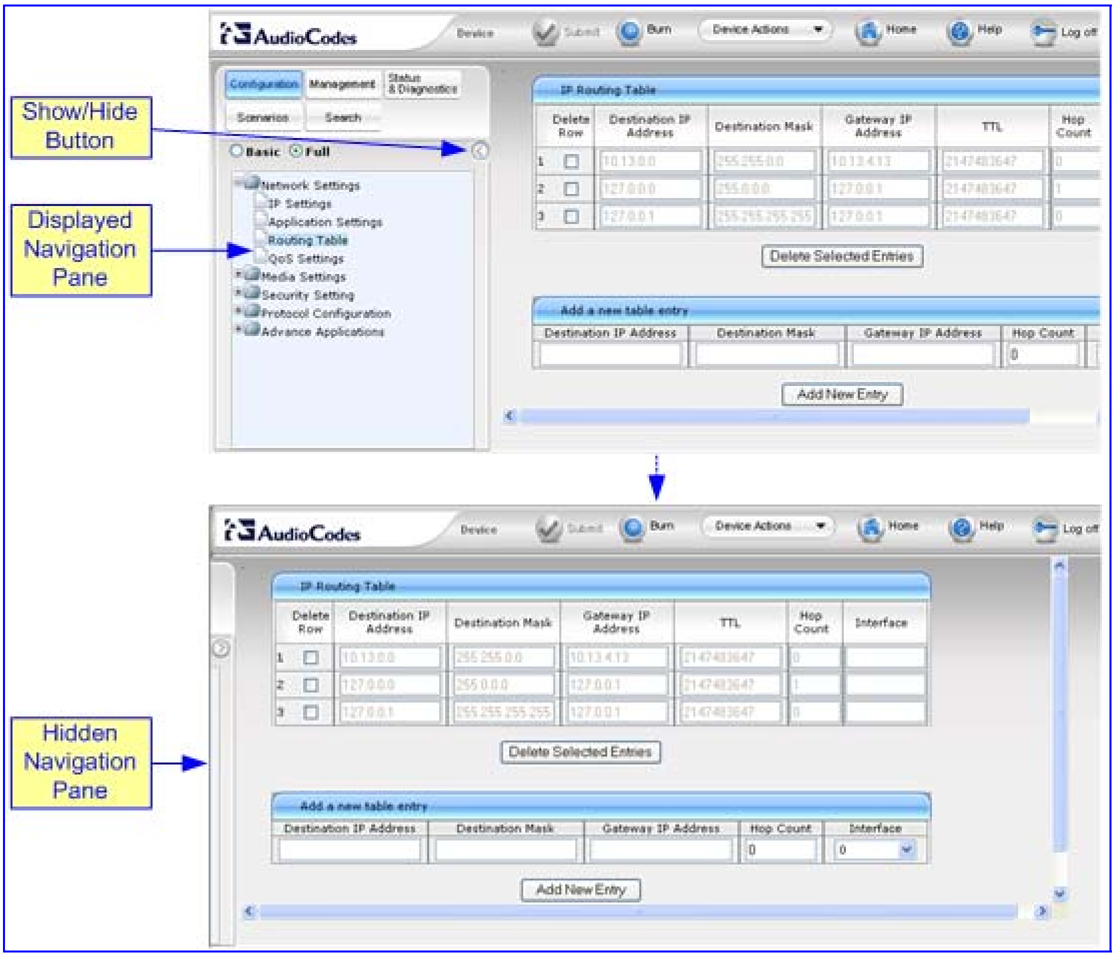
Note: When in Scenario mode (refer to "Scenarios" on page 34), the Navigation tree is displayed in 'Full' view (i.e., all menus are displayed in the Navigation tree).

3.3.2.2 Showing / Hiding the Navigation Pane

The Navigation pane can be hidden to provide more space for elements displayed in the Work pane. This is especially useful when the Work pane displays a page with a table that's wider than the Work pane and to view the all the columns, you need to use scroll bars. The arrow button located just below the Navigation bar is used to hide and show the Navigation pane.

- **To hide the Navigation pane:** click the left-pointing arrow ‹ ; the pane is hidden and the button is replaced by the right-pointing arrow button.
- **To show the Navigation pane:** click the right-pointing arrow › ; the pane is displayed and the button is replaced by the left-pointing arrow button.

Figure 3-6: Showing and Hiding Navigation Pane



IP Routing Table

	Delete Row	Destination IP Address	Destination Mask	Gateway IP Address	TTL	Hop Count	Interface
1	□	10.13.0.0	255.255.0.0	10.13.4.13	2147483647	0	
2	□	127.0.0.0	255.0.0.0	127.0.0.1	2147483647	1	
3	□	127.0.0.1	255.255.255.255	127.0.0.1	2147483647	0	

Add a new table entry

Destination IP Address	Destination Mask	Gateway IP Address	Hop Count	Interface
			0	0

3.3.3 Working with Configuration Pages

The configuration pages contain the parameters for configuring the device. The configuration pages are displayed in the Work pane, which is located to the right of the Navigation pane.

3.3.3.1 Accessing Pages

The configuration pages are accessed by clicking the required page item in the Navigation tree.

➢ To open a configuration page in the Work pane, take these 2 steps:

1. On the Navigation bar, click the required tab:
   - **Configuration** (refer to "Configuration Tab" on page 50)
   - **Management** (refer to "Management Tab" on page 220)
   - **Status & Diagnostics** (refer to "Status & Diagnostics Tab" on page 241)

   The menus of the selected tab appears in the Navigation tree.
2. In the Navigation tree, drill-down to the required page item; the page opens in the Work pane.

You can also access previously opened pages, by clicking your Web browser's **Back** button until you have reached the required page. This is useful if you want to view pages in which you have performed configurations in the current Web session.

Notes:

- You can also access certain pages from the **Device Actions** button located on the toolbar (refer to "Toolbar" on page 21).
- To view all the menus in the Navigation tree, ensure that the Navigation tree is in 'Full' view (refer to "Displaying Navigation Tree in Basic and Full View" on page 24).
- To get Online Help for the currently opened page, refer to "Getting Help" on page 45.
- Certain pages may not be accessible if your Web user account's access level is low (refer to "Configuring the Web User Accounts" on page 99).

3.3.3.2 Viewing Parameters

For convenience, some pages allow you to view a reduced or expanded display of parameters. A reduced display allows you to easily identify required parameters, enabling you to quickly configure your device.

The Web interface provides you with two methods for handling the display of page parameters:

- Display of "basic" and "advanced" parameters (refer to "Displaying Basic and Advanced Parameters" on page 27)
- Display of parameter groups (refer to "Showing / Hiding Parameter Groups" on page 28)

Note: Certain pages may only be read-only if your Web user account's access level is low (refer to "Configuring the Web User Accounts" on page 99). If a page is read-only, 'Read-Only Mode' is displayed at the bottom of the page.

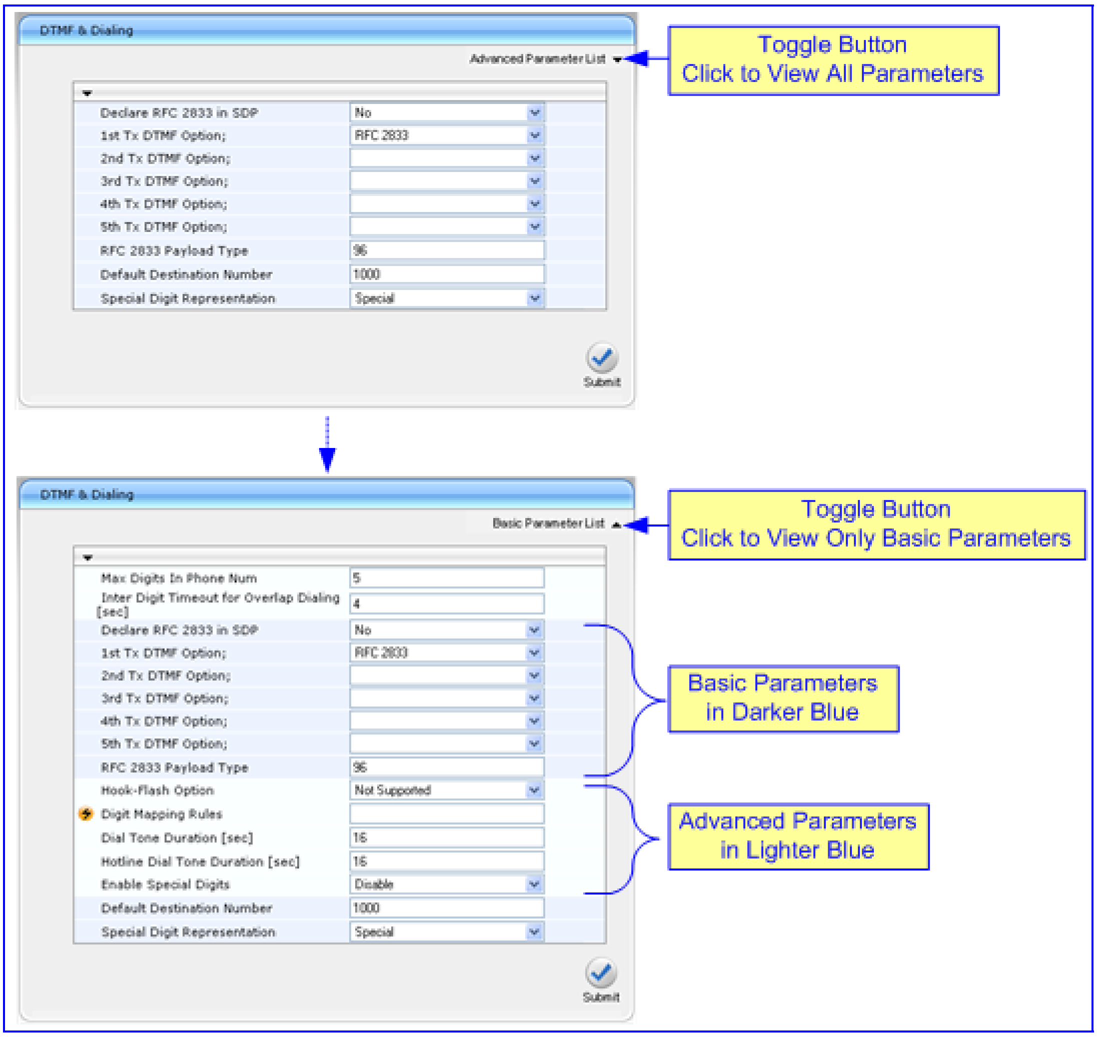
3.3.3.2.1 Displaying Basic and Advanced Parameters

Some pages provide you with an **Advanced Parameter List** / **Basic Parameter List** toggle button that allows you to show or hide advanced parameters (in addition to displaying the basic parameters). This button is located on the top-right corner of the page and has two states:

- **Advanced Parameter List** button with down-pointing arrow: click this button to display all parameters.
- **Basic Parameter List** button with up-pointing arrow: click this button to show only common (*basic*) parameters.

The figure below shows an example of a page displaying basic parameters only, and then showing advanced parameters as well, using the **Advanced Parameter List** button.

Figure 3-7: Toggling between Basic and Advanced Page View



Declare RFC 2833 in SDP	No
1st Tx DTMF Option;	RFC 2833
2nd Tx DTMF Option;	
3rd Tx DTMF Option;	
4th Tx DTMF Option;	
5th Tx DTMF Option;	
RFC 2833 Payload Type	96
Default Destination Number	1000
Special Digit Representation	Special

Toggle Button
Click to View All Parameters

Max Digits In Phone Num	5
Inter Digit Timeout for Overlap Dialing [sec]	4
Declare RFC 2833 in SDP	No
1st Tx DTMF Option;	RFC 2833
2nd Tx DTMF Option;	
3rd Tx DTMF Option;	
4th Tx DTMF Option;	
5th Tx DTMF Option;	
RFC 2833 Payload Type	96
Hook-Flash Option	Not Supported
Digit Mapping Rules	
Dial Tone Duration [sec]	16
Hotline Dial Tone Duration [sec]	16
Enable Special Digits	Disable
Default Destination Number	1000
Special Digit Representation	Special

Toggle Button
Click to View Only Basic Parameters

Basic Parameters
in Darker Blue

Advanced Parameters
in Lighter Blue

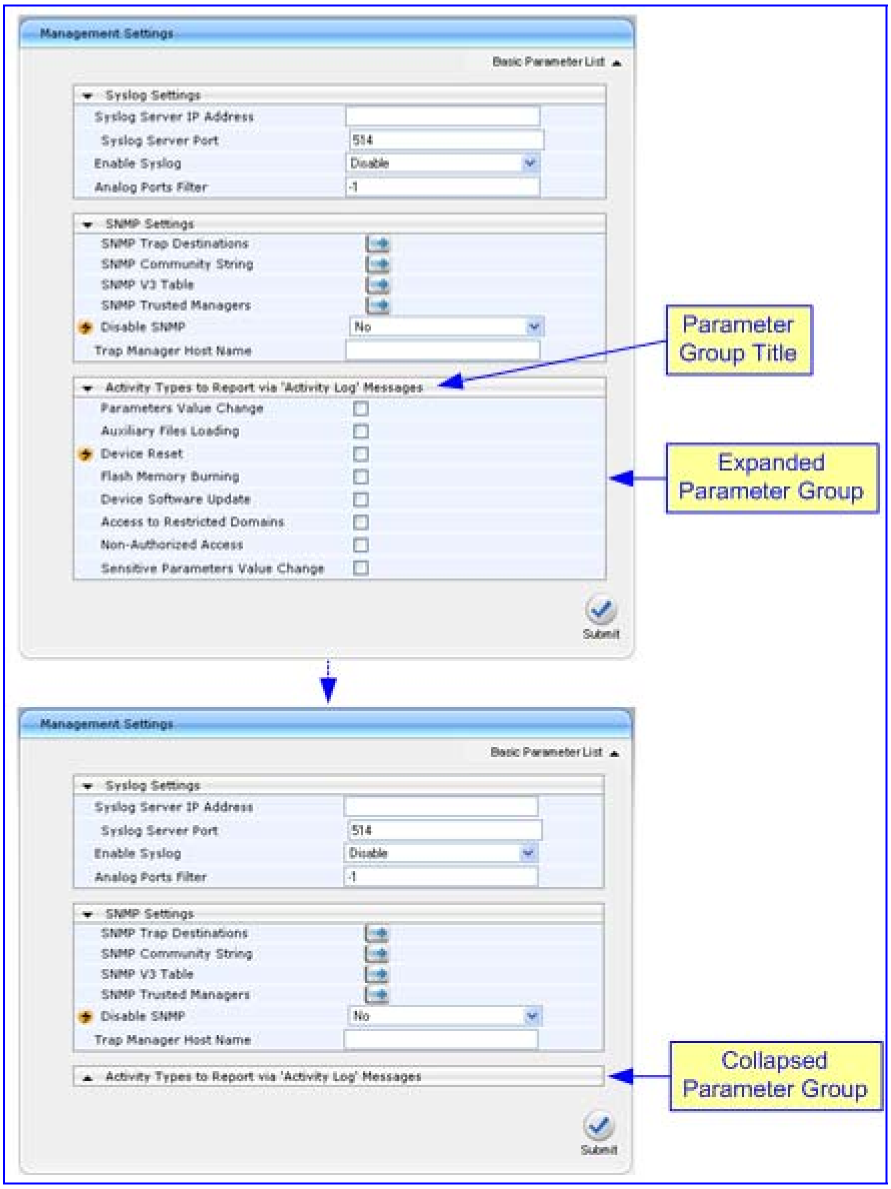
For ease of identification, the basic parameters are displayed with a darker blue color background than the advanced parameters.

Note: When the Navigation tree is in 'Full' mode (refer to "Navigation Tree" on page 23), configuration pages display all their parameters (i.e., the 'Advanced Parameter List' view is displayed).

3.3.3.2.2 Showing / Hiding Parameter Groups

Some pages provide groups of parameters, which can be hidden or shown. To toggle between hiding and showing a group, simply click the group name button that appears above each group. The button appears with a down-pointing or up-pointing arrow, indicating that it can be collapsed or expanded when clicked, respectively.

Figure 3-8: Expanding and Collapsing Parameter Groups



Management Settings

Basic Parameter List ▲

▼ Syslog Settings
- Syslog Server IP Address:
- Syslog Server Port: 514
- Enable Syslog: Disable
- Analog Ports Filter: -1

▼ SNMP Settings
- SNMP Trap Destinations
- SNMP Community String
- SNMP V3 Table
- SNMP Trusted Managers
- Disable SNMP: No
- Trap Manager Host Name:

▼ Activity Types to Report via 'Activity Log' Messages
- Parameters Value Change □
- Auxiliary Files Loading □
- Device Reset □
- Flash Memory Burning □
- Device Software Update □
- Access to Restricted Domains □
- Non-Authorized Access □
- Sensitive Parameters Value Change □

Submit

Management Settings

Basic Parameter List ▲

▼ Syslog Settings
- Syslog Server IP Address:
- Syslog Server Port: 514
- Enable Syslog: Disable
- Analog Ports Filter: -1

▼ SNMP Settings
- SNMP Trap Destinations
- SNMP Community String
- SNMP V3 Table
- SNMP Trusted Managers
- Disable SNMP: No
- Trap Manager Host Name:

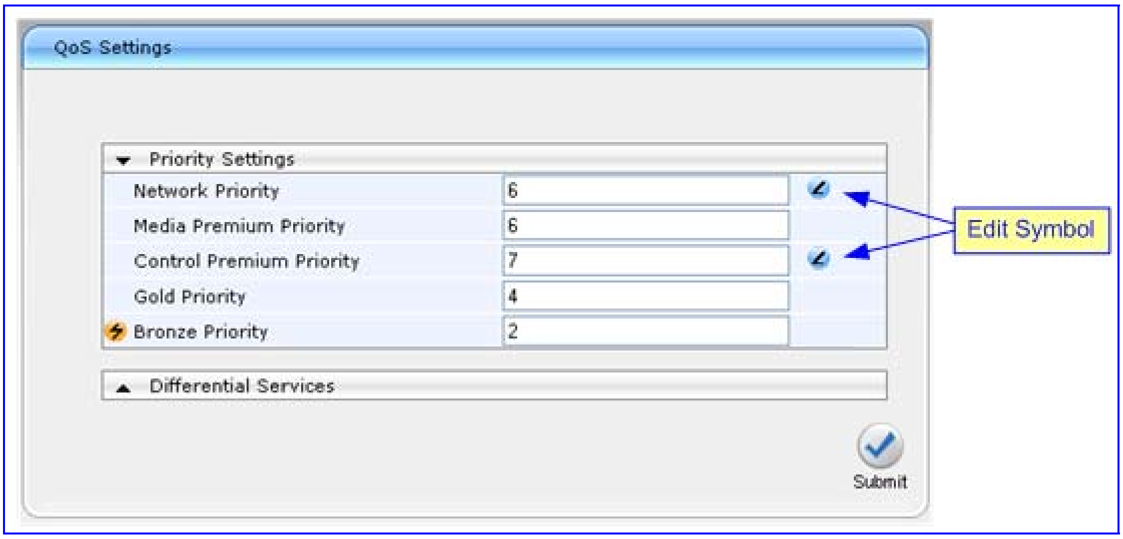
▲ Activity Types to Report via 'Activity Log' Messages

Submit

3.3.3.3 Modifying and Saving Parameters

When you change parameter values on a page, the **Edit** ✎ symbol appears to the right of these parameters. This is especially useful for indicating the parameters that you have currently modified (before applying the changes). After you save your parameter modifications (refer to the procedure described below), the **Edit** symbols disappear.

Figure 3-9: Editing Symbol after Modifying Parameter Value



QoS Settings

▼ Priority Settings

Network Priority	6	✎
Media Premium Priority	6	
Control Premium Priority	7	✎
Gold Priority	4	
⚡ Bronze Priority	2	

▲ Differential Services

➢ To save configuration changes on a page to the device's volatile memory (RAM), take this step:

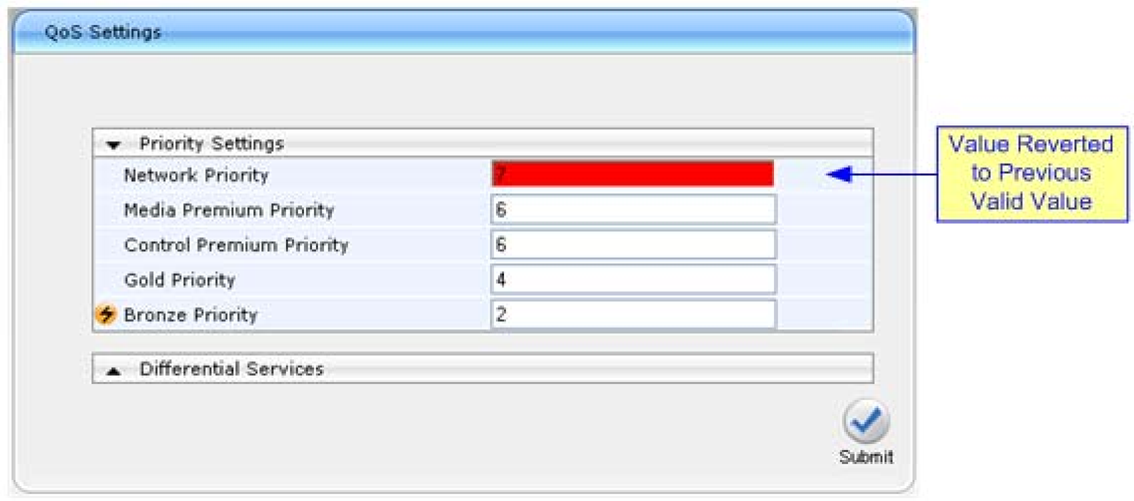
- Click the **Submit** ✓ button, which is located near the bottom of the page in which you are working; modifications to parameters with on-the-fly capabilities are immediately applied to the device and take effect; other parameters (displayed on the page with the lightning ⚡ symbol) are not changeable on-the-fly and require a device reset (refer to "Resetting the Device" on page 228) before taking effect.

Notes:

- Parameters saved to the volatile memory (by clicking **Submit**), revert to their previous settings after a hardware or software reset (or if the device is powered down). Therefore, to ensure parameter changes (whether on-the-fly or not) are retained, you need to save ('burn') them to the device's non-volatile memory, i.e., flash (refer to "Saving Configuration" on page 230).
- If you modify a parameter value and then attempt to navigate away from the page without clicking **Submit**, a message box appears notifying you of this. Click **Yes** to save your modifications or **No** to ignore them.

If you enter an invalid parameter value (e.g., not in the range of permitted values) and then click **Submit**, a message box appears notifying you of the invalid value. In addition, the parameter value reverts to its previous value and is highlighted in red, as shown in the figure below:

Figure 3-10: Value Reverts to Previous Valid Value



QoS Settings

▼ Priority Settings

Network Priority	7
Media Premium Priority	6
Control Premium Priority	6
Gold Priority	4
Bronze Priority	2

▲ Differential Services

Value Reverted to Previous Valid Value

3.3.3.4 Entering Phone Numbers in Various Tables

Phone numbers or prefixes that you enter in various tables throughout the Web interface such as the 'Tel to IP Routing' table, must only be entered as digits without any other characters. For example, if you wish to enter the phone number 555-1212, it must be entered as 5551212 without the hyphen (-). If the hyphen is entered, the entry is invalid.

3.3.3.5 Working with Tables

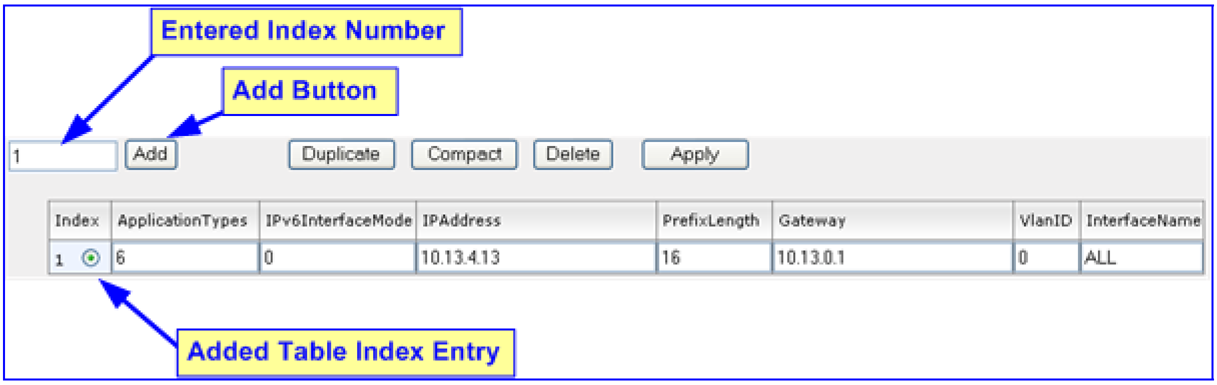
The Web interface includes many configuration pages that provide tables for configuring the device. Some of these tables provide the following command buttons:

- **Add:** adds an index entry to the table.
- **Duplicate:** duplicates a selected, existing index entry.
- **Compact:** organizes the index entries in ascending, consecutive order.
- **Delete:** deletes a selected index entry.
- **Apply:** saves the configuration.

➢ To add an entry to a table, take these 2 steps:

1. In the 'Add' field, enter the desired index entry number, and then click **Add**; an index entry row appears in the table:

Figure 3-11: Adding an Index Entry to a Table



Index	ApplicationTypes	IPv6InterfaceMode	IPAddress	PrefixLength	Gateway	VlanID	InterfaceName
1 ⦿	6	0	10.13.4.13	16	10.13.0.1	0	ALL

2. Click **Apply** to save the index entry.

Notes:

- Before you can add another index entry, you must ensure that you have applied the previously added index entry (by clicking **Apply**).
- If you leave the 'Add' field blank and then click **Add**, the existing index entries are all incremented by one and the newly added index entry is assigned the index 0.

➢ To add a copy of an existing index table entry, take these 3 steps:

1. In the 'Index' column, select the index that you want to duplicate; the **Edit** button appears.
2. Click **Edit**; the fields in the corresponding index row become available.
3. Click **Duplicate**; a new index entry is added with identical settings as the selected index in Step 1. In addition, all existing index entries are incremented by one and the newly added index entry is assigned the index 0.

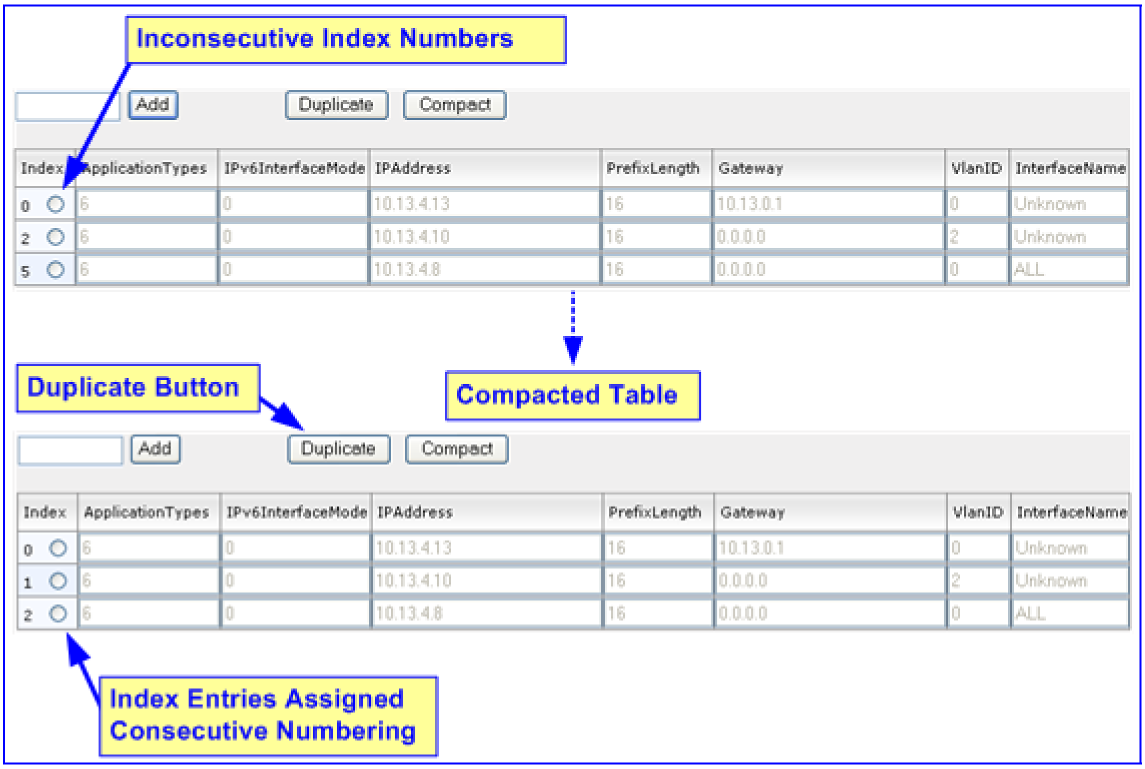
➢ To edit an existing index table entry, take these 3 steps:

1. In the 'Index' column, select the index corresponding to the table row that you want to edit.
2. Click **Edit**; the fields in the corresponding index row become available.
3. Modify the values as required, and then click **Apply**; the new settings are applied.

➢ To organize the index entries in ascending, consecutive order, take the following step:

- Click **Compact**; the index entries are organized in ascending, consecutive order, starting from index 0. For example, if you added three index entries 0, 4, and 6, then the index entry 4 is re-assigned index number 1 and the index entry 6 is re-assigned index number 2.

Figure 3-12: Compacting a Web Interface Table


Inconsecutive Index Numbers
Add
Duplicate
Compact
Duplicate Button
Compacted Table
Add
Duplicate
Compact
Index Entries Assigned Consecutive Numbering

Index	ApplicationTypes	IPv6InterfaceMode	IPAddress	PrefixLength	Gateway	VlanID	InterfaceName
0 ○	6	0	10.13.4.13	16	10.13.0.1	0	Unknown
2 ○	6	0	10.13.4.10	16	0.0.0.0	2	Unknown
5 ○	6	0	10.13.4.8	16	0.0.0.0	0	ALL

Index	ApplicationTypes	IPv6InterfaceMode	IPAddress	PrefixLength	Gateway	VlanID	InterfaceName
0 ○	6	0	10.13.4.13	16	10.13.0.1	0	Unknown
1 ○	6	0	10.13.4.10	16	0.0.0.0	2	Unknown
2 ○	6	0	10.13.4.8	16	0.0.0.0	0	ALL

➢ To delete an existing index table entry, take these 3 steps:

1. In the 'Index' column, select the index corresponding to the table row that you want to delete.
2. Click **Delete**; the table row is removed from the table.

3.3.4 Searching for Configuration Parameters

The Web interface provides a search engine that allows you to search any *ini* file parameter that is configurable by the Web interface (i.e., has a corresponding Web parameter). You can search for a specific parameter (e.g., "EnableIPSec") or a sub-string of that parameter (e.g., "sec"). If you search for a sub-string, all parameters that contain the searched sub-string in their names are listed.

➢ To search for *ini* file parameters configurable in the Web interface, take these 4 steps:

1. On the Navigation bar, click the **Search** tab; the Search engine appears in the Navigation pane.

2. In the 'Search' field, enter the parameter name or sub-string of the parameter name that you want to search. If you have performed a previous search for such a parameter, instead of entering the required string, you can use the 'Search History' drop-down list to select the string (saved from a previous search).

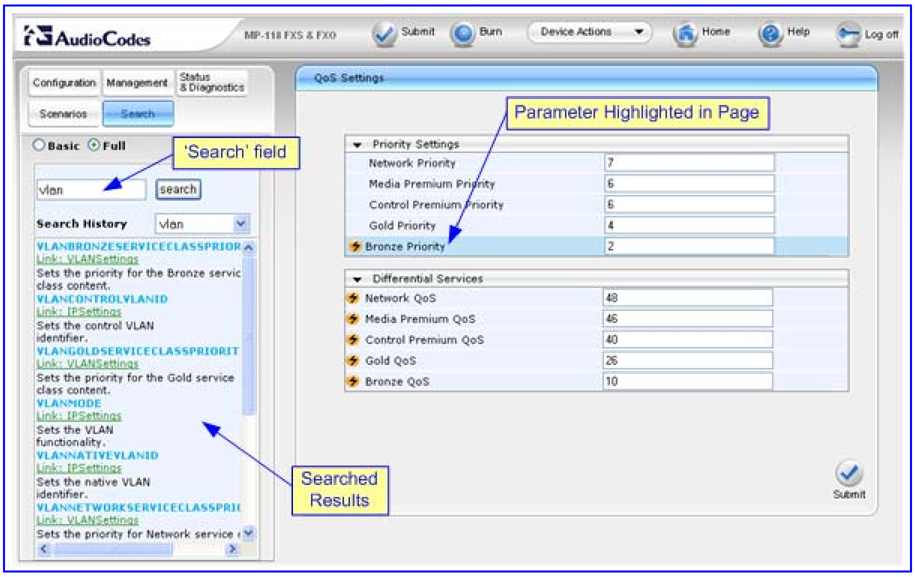
3. Click **Search**; a list of located parameters based on your search appears in the Navigation pane.

   Each searched result displays the following:

   - *ini* file parameter name
   - Link (in green) to its location (page) in the Web interface
   - Brief description of the parameter

4. In the searched list, click the required parameter (link in green) to open the page in which the parameter appears; the relevant page opens in the Work pane and the searched parameter is highlighted for easy identification, as shown in the figure below:

Figure 3-13: Searched Result Screen



vlan

Search History: vlan

VLANBRONZESERVICECLASSPRIOR
Link: VLANSettings
Sets the priority for the Bronze servic class content.
VLANCONTROLVLANID
Link: IPSettings
Sets the control VLAN identifier.
VLANGOLDSERVICECLASSPRIORIT
Link: VLANSettings
Sets the priority for the Gold service class content.
VLANMODE
Link: IPSettings
Sets the VLAN functionality.
VLANNATIVEVLANID
Link: IPSettings
Sets the native VLAN identifier.
VLANNETWORKSERVICECLASSPRI
Link: VLANSettings
Sets the priority for Network service

Priority Settings	
Network Priority	7
Media Premium Priority	6
Control Premium Priority	6
Gold Priority	4
Bronze Priority	2

Differential Services	
Network QoS	48
Media Premium QoS	46
Control Premium QoS	40
Gold QoS	26
Bronze QoS	10

Note: If the searched parameter is not located, a notification message is displayed.

3.3.5 Working with Scenarios

The Web interface allows you to create your own "menu" with up to 20 pages selected from the menus in the Navigation tree (i.e., pertaining to the **Configuration**, **Management**, and **Status & Diagnostics** tabs). The "menu" is a set of configuration pages grouped into a logical entity referred to as a *Scenario*. Each page in the Scenario is referred to as a *Step*. For each Step, you can select up to 25 parameters in the page that you want available in the Scenario. Therefore, the Scenario feature is useful in that it allows you quick-and-easy access to commonly used configuration parameters specific to your network environment. When you login to the Web interface, your Scenario is displayed in the Navigation tree, thereby, facilitating your configuration.

Instead of creating a Scenario, you can also load an existing Scenario from a PC to the device (refer to "Loading a Scenario to the Device" on page 39).

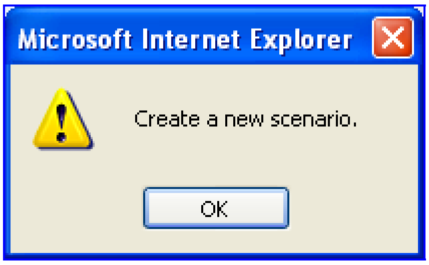
3.3.5.1 Creating a Scenario

The Web interface allows you to create one Scenario with up to 20 configuration pages, as described in the procedure below:

➢ To create a Scenario, take these 10 steps:

1. On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm creation of a Scenario:

Figure 3-14: Scenario Creation Confirm Message Box



Microsoft Internet Explorer

Create a new scenario.

   Note: If a Scenario already exists, the Scenario Loading message box appears.

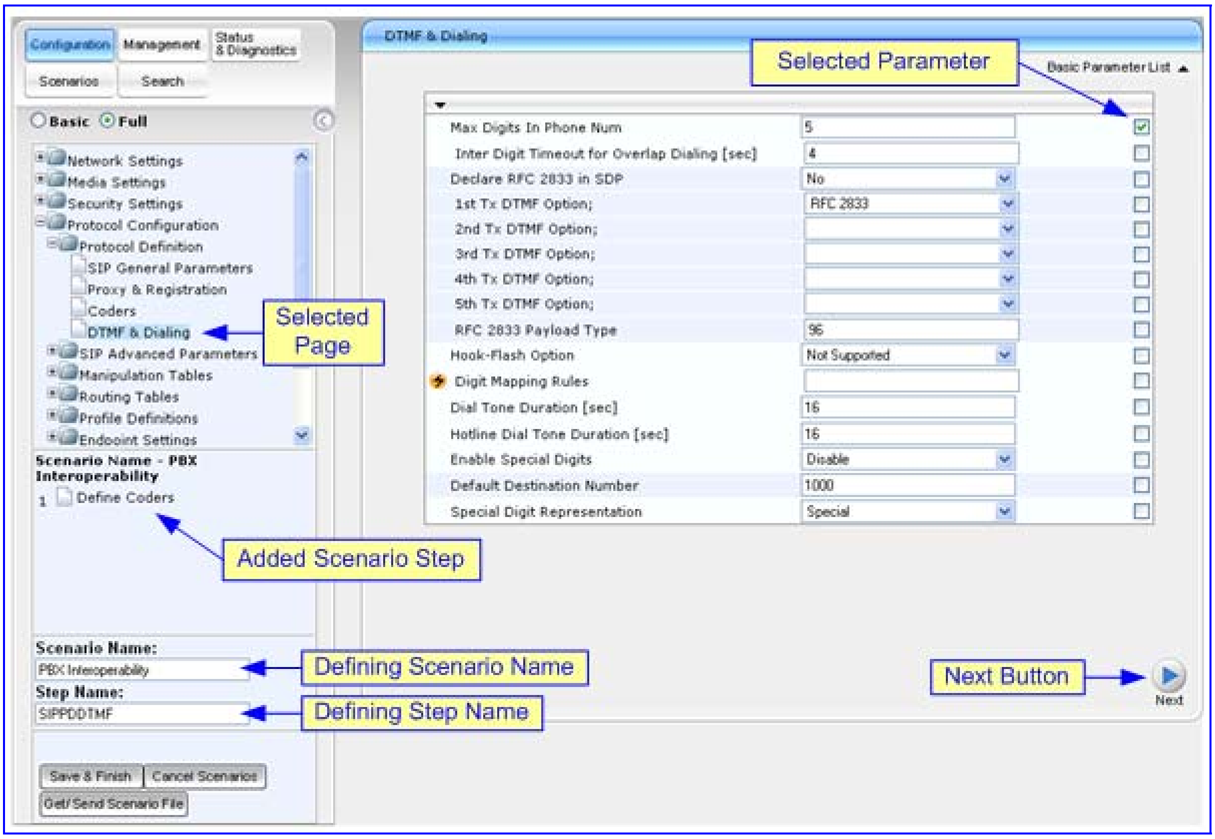
2. Click **OK**; the Scenario mode appears in the Navigation tree as well as the menus of the **Configuration** tab.

   Note: If a Scenario already exists and you wish to create a new one, click the **Create Scenario** button, and then click **OK** in the subsequent message box.

3. In the 'Scenario Name' field, enter an arbitrary name for the Scenario.
4. On the Navigation bar, click the **Configuration** or **Management** tab to display their respective menus in the Navigation tree.
5. In the Navigation tree, select the required page item for the Step, and then in the page itself, select the required parameters by selecting the check boxes corresponding to the parameters.
6. In the 'Step Name' field, enter a name for the Step.

7. Click the **Next** button located at the bottom of the page; the Step is added to the Scenario and appears in the Scenario Step list:

Figure 3-15: Creating a Scenario



Scenario Name - PBX Interoperability
1 Define Coders

Max Digits In Phone Num	5	☑
Inter Digit Timeout for Overlap Dialing [sec]	4	□
Declare RFC 2833 in SDP	No	□
1st Tx DTMF Option;	RFC 2833	□
2nd Tx DTMF Option;		□
3rd Tx DTMF Option;		□
4th Tx DTMF Option;		□
5th Tx DTMF Option;		□
RFC 2833 Payload Type	96	□
Hook-Flash Option	Not Supported	□
Digit Mapping Rules		□
Dial Tone Duration [sec]	16	□
Hotline Dial Tone Duration [sec]	16	□
Enable Special Digits	Disable	□
Default Destination Number	1000	□
Special Digit Representation	Special	□

Scenario Name: PBX Interoperability

Step Name: SIPPDDTMF

Selected Parameter

Selected Page

Added Scenario Step

Defining Scenario Name

Defining Step Name

Next Button

8. Repeat steps 5 through 8 to add additional Steps (i.e., pages).

9. When you have added all the required Steps for your Scenario, click the **Save & Finish** button located at the bottom of the Navigation tree; a message box appears informing you that the Scenario has been successfully created.

10. Click **OK**; the Scenario mode is quit and the menu tree of the **Configuration** tab appears in the Navigation tree.

Notes:

- You can add up to 20 Steps to a Scenario, where each Step can contain up to 25 parameters.
- When in Scenario mode, the Navigation tree is in 'Full' display (i.e., all menus are displayed in the Navigation tree) and the configuration pages are in 'Advanced Parameter List' display (i.e., all parameters are shown in the pages). This ensures accessibility to all parameters when creating a Scenario. For a description on the Navigation tree views, refer to ''Navigation Tree'' on page 23.
- If you previously created a Scenario and you click the **Create Scenario** button, the previously created Scenario is deleted and replaced with the one you are creating.
- Only users with access level of 'Security Administrator' can create a Scenario.

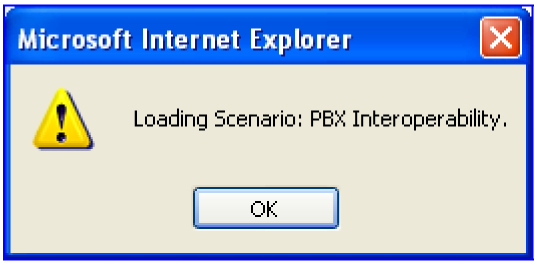
3.3.5.2 Accessing a Scenario

Once you have created the Scenario, you can access it at anytime by following the procedure below:

➢ **To access the Scenario, take these 2 steps:**

1. On the Navigation bar, select the **Scenario** tab; a message box appears, requesting you to confirm the loading of the Scenario.

Figure 3-16: Scenario Loading Message Box

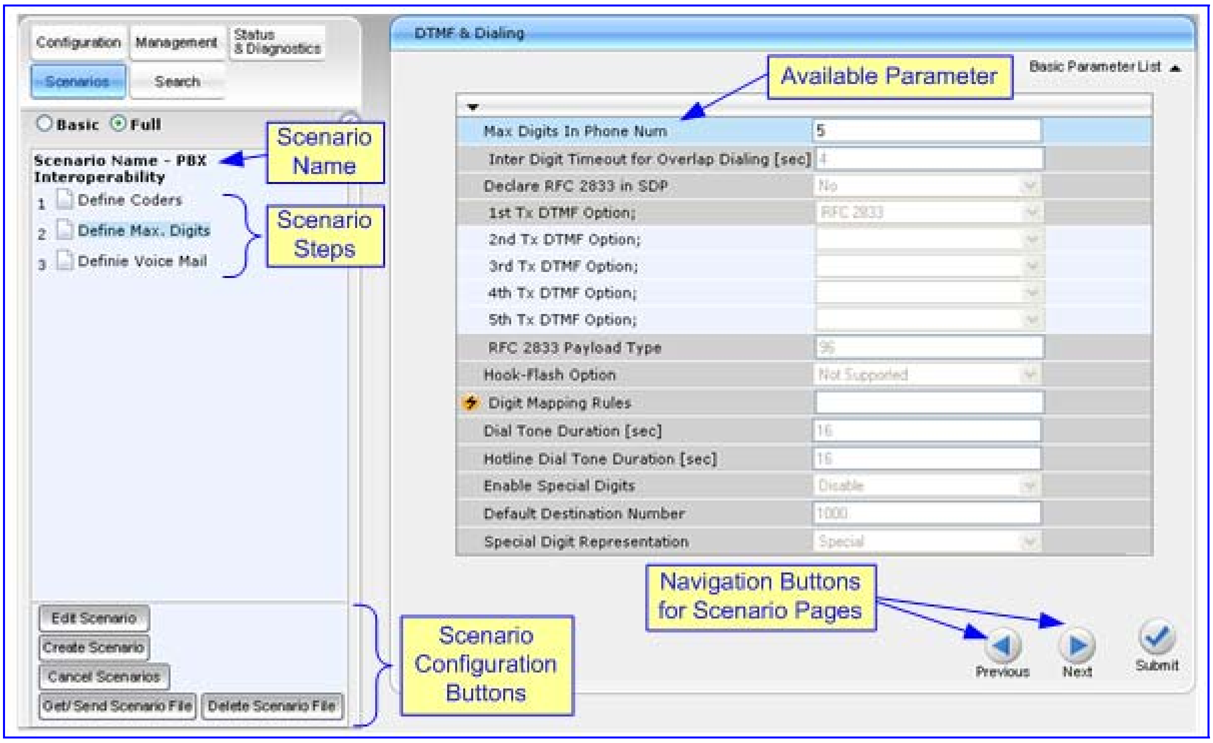


Microsoft Internet Explorer

Loading Scenario: PBX Interoperability.

2. Click **OK**; the Scenario and its Steps appear in the Navigation tree, as shown in the example figure below:

Figure 3-17: Scenario Example



Scenario Name - PBX Interoperability

1 Define Coders
2 Define Max. Digits
3 Definie Voice Mail

DTMF & Dialing

Max Digits In Phone Num	5
Inter Digit Timeout for Overlap Dialing [sec]	4
Declare RFC 2833 in SDP	No
1st Tx DTMF Option;	RFC 2833
2nd Tx DTMF Option;	
3rd Tx DTMF Option;	
4th Tx DTMF Option;	
5th Tx DTMF Option;	
RFC 2833 Payload Type	96
Hook-Flash Option	Not Supported
Digit Mapping Rules	
Dial Tone Duration [sec]	16
Hotline Dial Tone Duration [sec]	16
Enable Special Digits	Disable
Default Destination Number	1000
Special Digit Representation	Special

When you select a Scenario Step, the corresponding page is displayed in the Work pane. In each page, the available parameters are indicated by a dark-blue background; the unavailable parameters are indicated by a gray or light-blue background.

To navigate between Scenario Steps, you can perform one of the following:

- In the Navigation tree, click the required Scenario Step.

- In an opened Scenario Step (i.e., page appears in the Work pane), use the following navigation buttons:
  - ▶ **Next:** opens the next Step listed in the Scenario.
  - ◀ **Previous**: opens the previous Step listed in the Scenario.

Note: If you reset the device while in Scenario mode, after the device resets, you are returned once again to the Scenario mode.

3.3.5.3 Editing a Scenario

You can modify a Scenario anytime by adding or removing Steps (i.e., pages) or parameters, and changing the Scenario name and the Steps' names.

Note: Only users with access level of 'Security Administrator' can edit a Scenario.

➢ To edit a Scenario, take these 6 steps:

1. On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm Scenario loading.
2. Click **OK**; the Scenario appears with its Steps in the Navigation tree.
3. Click the **Edit Scenario** button located at the bottom of the Navigation pane; the 'Scenario Name' and 'Step Name' fields appear.
4. You can perform the following edit operations:
   - **Add Steps:**
     a. On the Navigation bar, select the desired tab (i.e., **Configuration** or **Management**); the tab's menu appears in the Navigation tree.
     b. In the Navigation tree, navigate to the desired page item; the corresponding page opens in the Work pane.
     c. In the page, select the required parameter(s) by marking the corresponding check box(es).
     d. Click **Next**.
   - **Add or Remove Parameters:**
     a. In the Navigation tree, select the required Step; the corresponding page opens in the Work pane.
     b. To add parameters, select the check boxes corresponding to the desired parameters; to remove parameters, clear the check boxes corresponding to the parameters that you want removed.
     c. Click **Next**.

- **Edit the Step Name:**
  a. In the Navigation tree, select the required Step.
  b. In the 'Step Name' field, modify the Step name.
  c. In the page, click **Next**.
- **Edit the Scenario Name:**
  a. In the 'Scenario Name' field, edit the Scenario name.
  b. In the displayed page, click **Next**.
- **Remove a Step:**
  a. In the Navigation tree, select the required Step; the corresponding page opens in the Work pane.
  b. In the page, clear all the check boxes corresponding to the parameters.
  c. Click **Next**.

5. After clicking **Next**, a message box appears notifying you of the change. Click **OK**.
6. Click **Save & Finish**; a message box appears informing you that the Scenario has been successfully modified. The Scenario mode is exited and the menus of the **Configuration** tab appear in the Navigation tree.

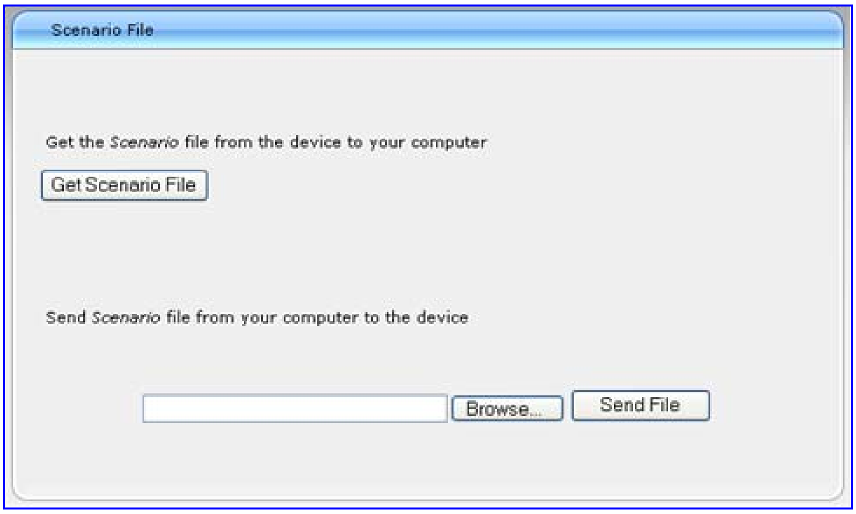
3.3.5.4 Saving a Scenario to a PC

You can save a Scenario to a PC (as a *dat* file). This is especially useful when requiring more than one Scenario to represent different environment setups (e.g., where one includes PBX interoperability and another not). Once you create a Scenario and save it to your PC, you can then keep on saving modifications to it under different Scenario file names. When you require a specific network environment setup, you can simply load the suitable Scenario file from your PC (refer to "Loading a Scenario to the Device" on page 39).

➢ To save a Scenario to a PC, take these 5 steps:

1. On the Navigation bar, click the **Scenarios** tab; the Scenario appears in the Navigation tree.
2. Click the **Get/Send Scenario File** button (located at the bottom of the Navigation tree); the 'Scenario File' page appears, as shown below:

Figure 3-18: Scenario File Page



Scenario File

Get the *Scenario* file from the device to your computer

Send *Scenario* file from your computer to the device

3. Click the **Get Scenario File** button; the 'File Download' window appears.

4. Click **Save**, and then in the 'Save As' window navigate to the folder to where you want to save the Scenario file. When the file is successfully downloaded to your PC, the 'Download Complete' window appears.

5. Click **Close** to close the 'Download Complete' window.

3.3.5.5 Loading a Scenario to the Device

Instead of creating a Scenario, you can load a Scenario file (*data* file) from your PC to the device.

➢ To load a Scenario to the device, take these 4 steps:

1. On the Navigation bar, click the **Scenarios** tab; the Scenario appears in the Navigation tree.

2. Click the **Get/Send Scenario File** button (located at the bottom of the Navigation tree); the 'Scenario File' page appears (refer to ''Saving a Scenario to a PC'' on page 38).

3. Click the **Browse** button, and then navigate to the Scenario file stored on your PC.

4. Click the **Send File** button.

Notes:

- You can only load a Scenario file to a device that has an identical hardware configuration setup to the device in which it was created. For example, if the Scenario was created in a device with FXS interfaces, the Scenario cannot be loaded to a device that does not have FXS interfaces.

- The loaded Scenario replaces any existing Scenario.

- You can also load a Scenario file using BootP, by loading an *ini* file that contains the *ini* file parameter ScenarioFileName (refer to ''Web and Telnet Parameters'' on page 273). The Scenario *dat* file must be located in the same folder as the *ini* file. For a detailed description on BootP, refer to the *Product Reference Manual*.

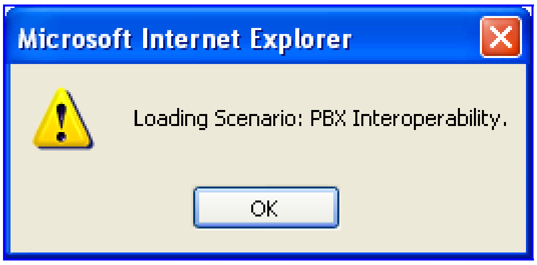
3.3.5.6 Deleting a Scenario

You can delete the Scenario by using the **Delete Scenario File** button, as described in the procedure below:

➢ To delete the Scenario, take these 4 steps:

1. On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm:

Figure 3-19: Scenario Loading Message Box

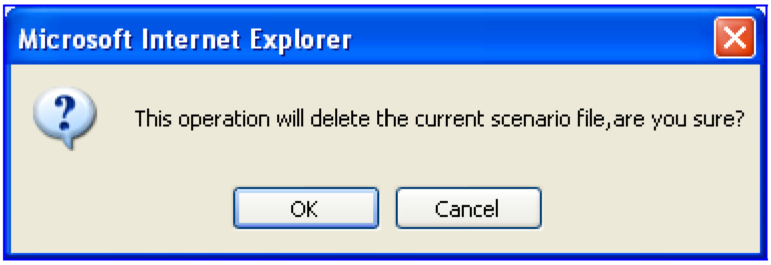


Microsoft Internet Explorer

Loading Scenario: PBX Interoperability.

2. Click **OK**; the Scenario mode appears in the Navigation tree.
3. Click the **Delete Scenario File** button; a message box appears requesting confirmation for deletion.

Figure 3-20: Message Box for Confirming Scenario Deletion



Microsoft Internet Explorer

This operation will delete the current scenario file,are you sure?

4. Click **OK**; the Scenario is deleted and the Scenario mode closes.

Note: You can also delete a Scenario using the following alternative methods:

- Loading an empty *dat* file (refer to "Loading a Scenario to the Device" on page 39).
- Loading an *ini* file with the ScenarioFileName parameter set to no value (i.e., ScenarioFileName = "").

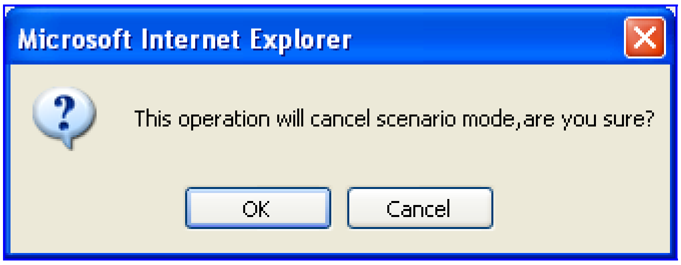
3.3.5.7 Exiting Scenario Mode

When you want to close the Scenario mode after using it for device configuration, follow the procedure below:

➢ To close the Scenario mode, take these 2 steps:

1. Simply click any tab (besides the **Scenarios** tab) on the Navigation bar, or click the **Cancel Scenarios** button located at the bottom of the Navigation tree; a message box appears, requesting you to confirm exiting Scenario mode, as shown below.

Figure 3-21: Confirmation Message Box for Exiting Scenario Mode



Microsoft Internet Explorer

This operation will cancel scenario mode,are you sure?

2. Click **OK** to exit.

3.3.6 Customizing the Web Interface

You can customize the device's Web interface to suit your company preferences. The following Web interface elements can be customized:

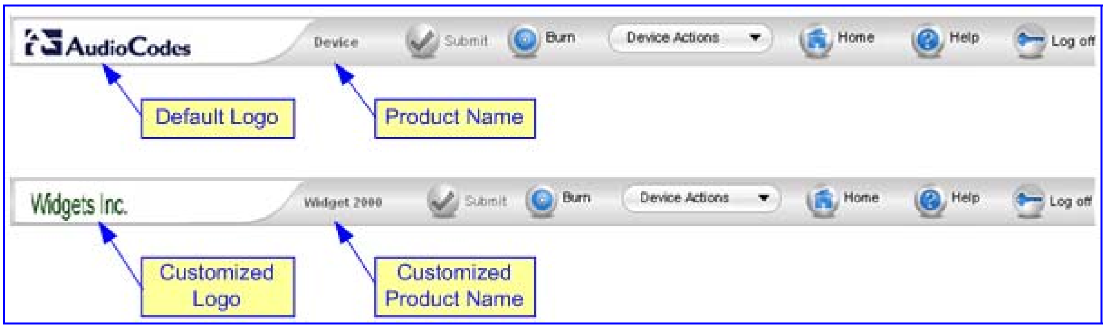
- Corporate logo displayed on the Title bar (refer to "Replacing the Corporate Logo" on page 41)
- Product’s name displayed on the Title bar (refer to "Customizing the Product Name" on page 44)
- Login welcome message (refer to "Creating a Login Welcome Message" on page 44)

3.3.6.1 Replacing the Corporate Logo

The corporate logo that appears in the Title bar can be replaced either with a different logo image (refer to "Replacing the Corporate Logo with an Image" on page 42) or text (refer to "Replacing the Corporate Logo with Text" on page 43).

The figure below shows an example of a customized Title bar. The top image displays the Title bar with AudioCodes logo and product name. The bottom image displays a customized Title bar with a different image logo and product name.

Figure 3-22: Customizing Web Logo and Product Name



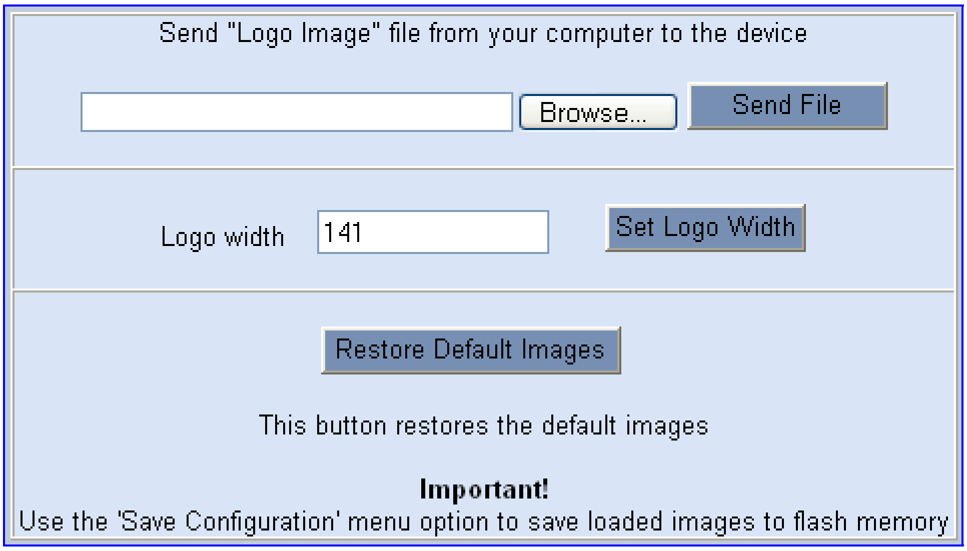
3.3.6.1.1 Replacing the Corporate Logo with an Image

You can replace the logo that appears in the Web interface's Title bar, using either the Web interface or the *ini* file.

➢ **To replace the default logo with a different image via the Web interface, take these 7 steps:**

1. Access the device's Web interface (refer to "Accessing the Web Interface" on page 20).
2. In the URL field, append the case-sensitive suffix ‘AdminPage’ to the IP address (e.g., http://10.1.229.17/AdminPage); the 'Admin' page appears.
3. On the left pane, click **Image Load to Device**; the 'Image Download' page is displayed, as shown in the figure below.

Figure 3-23: Image Download Screen



Send "Logo Image" file from your computer to the device

Logo width: 141

This button restores the default images

Important!
Use the 'Save Configuration' menu option to save loaded images to flash memory

4. Click the **Browse** button, and then navigate to the folder in which the logo image file that you want to use is located.
5. Click the **Send File** button; the image file uploads to the device. When loading is complete, the page is automatically refreshed and the uploaded logo image is displayed in the Web interface's title bar.
6. If you want to modify the width of the image, in the 'Logo Width' field, enter the new width (in pixels) and then click the **Set Logo Width** button.
7. To save the image to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- The logo image must be a GIF, JPG, or JPEG file.
- The logo image must have a fixed height of 30 pixels. The width can be up to 199 pixels, the default being 141 pixels.
- The size of the image file can be up to 64 Kbytes.

Tip: If you encounter any problem during the loading of the file or you want to restore the default image, click the **Restore Default Images** button.

➢ To replace the default logo with a different image using the *ini* file, take these 3 steps:

1. Place your corporate logo image file on the TFTP server in the same folder where the device's *ini* file is located.
2. Configure the *ini* file parameters as described in the table below. (For a description on using the *ini* file, refer to "Modifying an ini File" on page 259.)
3. Load the *ini* file to the device using BootP / TFTP (i.e., not through the Web interface). For detailed information on the BootP/TFTP application, refer to the *Product Reference Manual*.

Table 3-2: ini File Parameters for Changing Logo Image

Parameter	Description
LogoFileName	The name of the image file for your corporate logo. Use a gif, jpg or jpeg image file. The default is AudioCodes' logo file. **Note:** The length of the name of the image file is limited to 48 characters.
LogoWidth	Width (in pixels) of the logo image. The range is 0 - 199. The default value is 141 (which is the width of AudioCodes' displayed logo). **Note:** The optimal setting depends on the screen resolution settings.

3.3.6.1.2 Replacing the Corporate Logo with Text

The corporate logo can be replaced with a text string instead of an image. To replace AudioCodes' default logo with a text string using the *ini* file, configure the *ini* file parameters listed in the table below. (For a description on using the *ini* file, refer to "Modifying an ini File" on page 259.)

Table 3-3: ini File Parameters for Replacing Logo with Text

Parameter	Description
UseWebLogo	▪ **[0]** = Logo image is used (default). ▪ **[1]** = Text string used instead of a logo image.
WebLogoText	Text string that replaces the logo image. The string can be up to 15 characters.

Note: When a text string is used instead of a logo image, the Web browser's title bar displays the string assigned to the WebLogoText parameter.

3.3.6.2 Customizing the Product Name

You can customize the product name (text) that appears in the Title bar, using the *ini* file parameters listed in the table below. (For a description on using the *ini* file, refer to "Modifying an ini File" on page 259.)

Table 3-4: ini File Parameters for Customizing Product Name

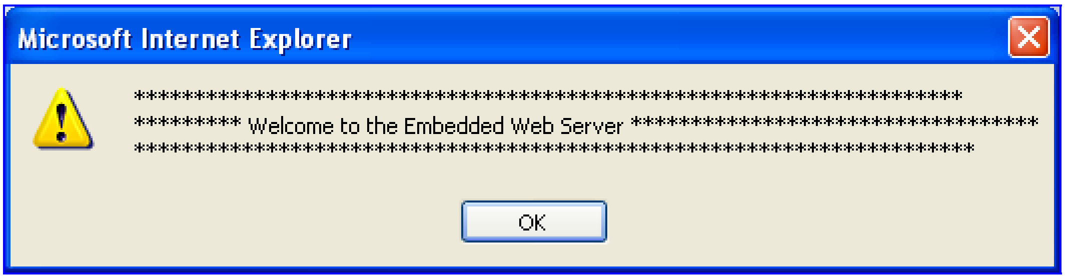
Parameter	Description
UseProductName	Defines whether or not to change the product name: ▪ **[0]** = Don't change the product name (default). ▪ **[1]** = Enable product name change.
UserProductName	The text string that replaces the product name. The default is 'Mediant 2000'. The string can be up to 29 characters.

3.3.6.3 Creating a Login Welcome Message

You can create a Welcome message box (alert message) that appears after each successful login to the device's Web interface. The *ini* file table parameter WelcomeMessage allows you to create the Welcome message. Up to 20 lines of character strings can be defined for the message. If this parameter is not configured, no Welcome message box is displayed after login.

An example of a Welcome message is shown in the figure below:

Figure 3-24: User-Defined Web Welcome Message after Login



****
********* Welcome to the Embedded Web Server **********************************
****

Table 3-5: ini File Parameter for Welcome Login Message

Parameter	Description
WelcomeMessage	Defines the Welcome message that appears after a successful login to the Web interface. The format of this parameter is as follows: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; [\WelcomeMessage] For Example: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "********************************"; WelcomeMessage 2 = "********* This is a Welcome message **"; WelcomeMessage 3 = "********************************"; [\WelcomeMessage] **Note:** Each index represents a line of text in the Welcome message box. Up to 20 indices can be defined.

3.3.7 Getting Help

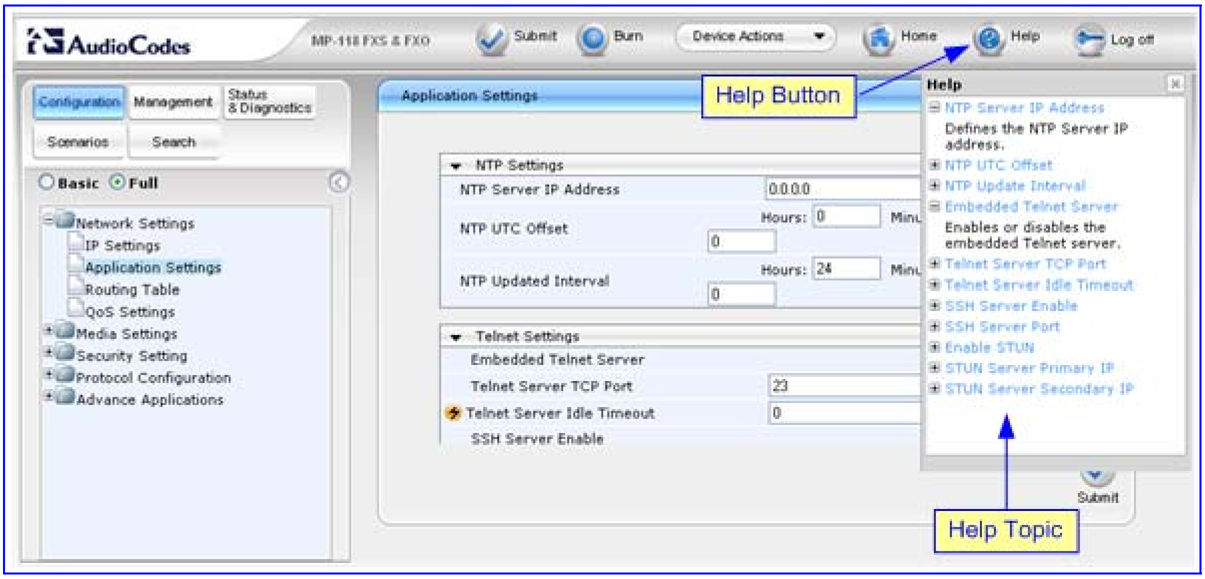
The Web interface provides you with context-sensitive Online Help. The Online Help provides you with brief descriptions of most of the parameters you'll need to successfully configure the device. The Online Help provides descriptions of parameters pertaining to the currently opened page.

➢ To view the Help topic for a currently opened page, take these 4 steps:

1. Using the Navigation tree, open the required page for which you want Help.

2. On the toolbar, click the **Help** button; the Help topic pertaining to the opened page appears, as shown below:

Figure 3-25: Help Topic for Current Page



NTP Server IP Address 0.0.0.0

NTP UTC Offset Hours: 0 Minu 0

NTP Updated Interval Hours: 24 Minu 0

Embedded Telnet Server

Telnet Server TCP Port 23

Telnet Server Idle Timeout 0

SSH Server Enable

⊟ NTP Server IP Address

Defines the NTP Server IP address.

⊞ NTP UTC Offset

⊞ NTP Update Interval

⊟ Embedded Telnet Server

Enables or disables the embedded Telnet server.

⊞ Telnet Server TCP Port

⊞ Telnet Server Idle Timeout

⊞ SSH Server Enable

⊞ SSH Server Port

⊞ Enable STUN

⊞ STUN Server Primary IP

⊞ STUN Server Secondary IP

3. To view a description of a parameter, click the **plus** ⊞ sign to expand the parameter. To collapse the description, click the **minus** ⊟ sign.

4. To close the Help topic, click the **close** ☒ button located on the top-right corner of the Help topic window.

Note: Instead of clicking the **Help** button for each page you open, you can open it once for a page, and then simply leave it open. Each time you open a different page, the Help topic pertaining to that page is automatically displayed.

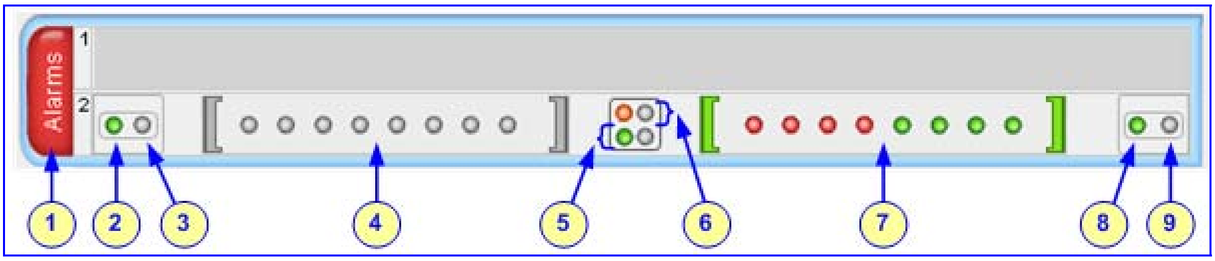
3.3.8 Using the Home Page

The 'Home' page provides you with a graphical display of the device's front panel, displaying color-coded status icons for monitoring the functioning of the device. By default, the 'Home' page is displayed when you access the device's Web interface. When you are configuring the device (in a configuration page), you can always return to the 'Home' page, by simply clicking the **Home** icon on the toolbar. The 'Home' page also displays general device information (in the 'General Information' pane) such as the device's IP address and firmware version.

➢ To access the Home page, take this step:

- On the toolbar, click the **Home** icon; the 'Home' page is displayed:

Figure 3-26: Areas of the Home Page



Note: The number of channels displayed in the 'Home' page depends on the device's hardware configuration.

The table below describes the areas of the 'Home' page.

Table 3-6: Description of the Areas of the Home Page

Item# / Label	Description
1	Displays the highest severity of an active alarm raised (if any) by the device: ▪ Green = No alarms ▪ Red = Critical alarm ▪ Orange = Major alarm ▪ Yellow = Minor alarm You can also view a list of active alarms in the 'Active Alarms' page (refer to “Viewing Active Alarms” on page 245), by clicking the Alarms area.
2	Blade Activity icon: ▪ ● (green): Initialization sequence terminated successfully.
3	Blade Fail icon: ▪ ● (gray): Normal functioning. ▪ ● (red): Blade failure.

Item# / Label	Description
4	T1/E1 Trunk Status icons for trunks 1 through 8. ▪ ● (gray): Disable - Trunk not configured (not in use). ▪ ● (green): Active OK - Trunk synchronized. ▪ ● (yellow): RAI Alarm - Remote Alarm Indication (RAI), also known as the 'Yellow' Alarm. ▪ ● (red): LOS / LOF Alarm - Loss due to LOS (Loss of Signal) or LOF (Loss of Frame). ▪ ● (blue): AIS Alarm - Alarm Indication Signal (AIS), also known as the 'Blue' Alarm ▪ ● (orange): D-Channel Alarm - D-channel alarm You can switch modules (refer to “Switching Between Modules” on page 48), view port settings (refer to “Viewing Trunk Settings” on page 48), and assign a name to a port (refer to “Assigning a Name or Brief Description to a Port” on page 47).
5	Dual Ethernet Link icons: ▪ ● (gray): No link. ▪ ● (green): Active link. You can also view detailed Ethernet port information in the 'Ethernet Port Information' page (refer to “Viewing the Active Alarms Table” on page 245), by clicking this icon.
6	Dual Ethernet activity icons: ▪ ● (gray): No Ethernet activity. ▪ ●(orange): Transmit / receive activity.
7	T1/E1 Trunk Status icons for trunks 9 through 16. Refer to Item #4 for a description.
8	Power status icon: ▪ ● (green): Power received by blade. ▪ ● (red): No power received by blade.
9	Slot status of installed blade in the chassis (SWAP Ready icon).

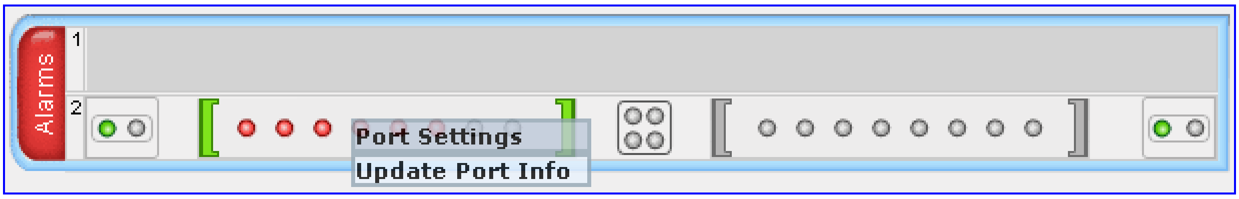
3.3.8.1 Assigning a Name to a Port

The 'Home' page allows you to assign an arbitrary name or a brief description to each port. This description appears as a tooltip when you move your mouse over the port.

➢ To add a port description, take these 3 steps:

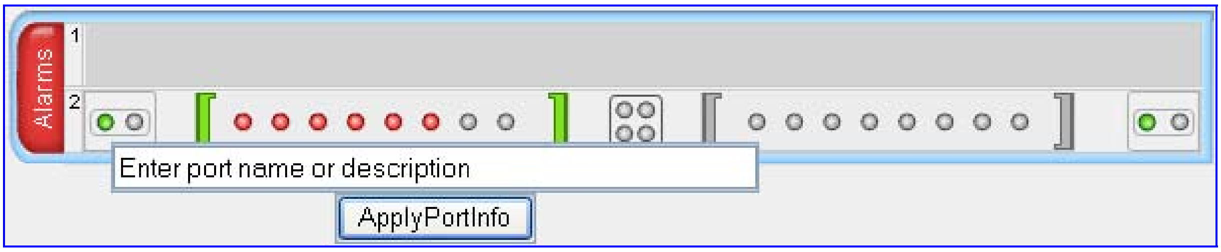
1. Click the required port icon; a shortcut menu appears, as shown below:

Figure 3-27: Shortcut Menu for Assigning a Port Name



2. From the shortcut menu, choose **Update Port Info**; a text box appears.

Figure 3-28: Entering the Port Name



3. Type a brief description for the port, and then click **Apply Port Info**.

3.3.8.2 Viewing Trunk Settings

The 'Home' page allows you to view the settings of a selected port in the 'Trunk Settings' screen. Accessing this screen from the Home page provides an alternative to accessing it from the **Advanced Configuration** menu (refer to "Configuring the Trunk Settings" on page 82).

➢ To view port settings, take these 2 steps:

1. On the 'Home' page, click a desired trunk port LED on the TP-1610 (labeled as items #3 and #5 in the figure in Accessing the Home Page); a shortcut menu appears.
2. From the shortcut menu, choose **Port Settings**; the 'Trunk Settings' screen opens.

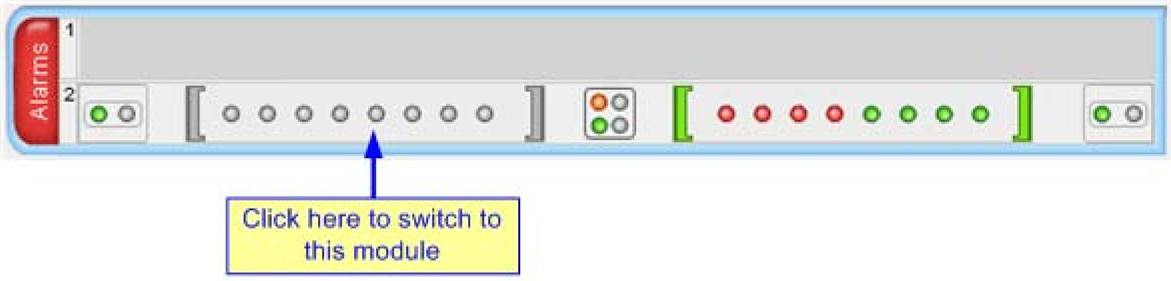
3.3.8.3 Switching Between Modules

The device can house up to two modules, as discussed in previous sections. Since each module is a standalone gateway, the 'Home' page displays only one of the modules to which you are connected. However, you can easily switch to the second module, by having the Web browser connect to the IP address of the other module.

➢ To switch modules, take these 3 steps:

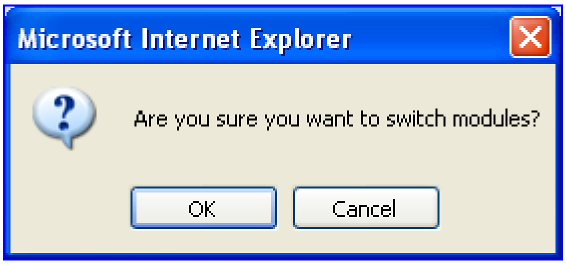
1. In the 'Home' page, click anywhere on the module to which you want to switch, as shown below:

Figure 3-29: Click Module to which you want to Switch



A confirmation message box appears requesting you to confirm switching of modules.

Figure 3-30: Confirmation Message Box for Switching Modules



Are you sure you want to switch modules?

2. Click **OK**; the 'Enter Network Password' screen pertaining to the Web interface of the switched module appears.
3. Enter the login user name and password, and then click **OK**.

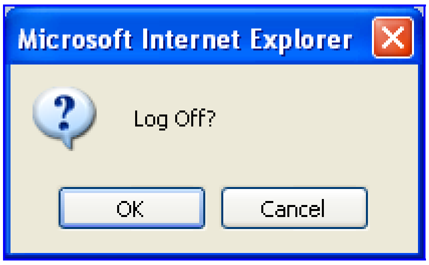
3.3.9 Logging Off the Web Interface

You can log off the Web interface and re-access it with a different user account. For detailed information on the Web User Accounts, refer to User Accounts.

➢ To log off the Web interface, take these 2 steps:

1. On the toolbar, click the **Log Off** button; the 'Log Off' confirmation message box appears:

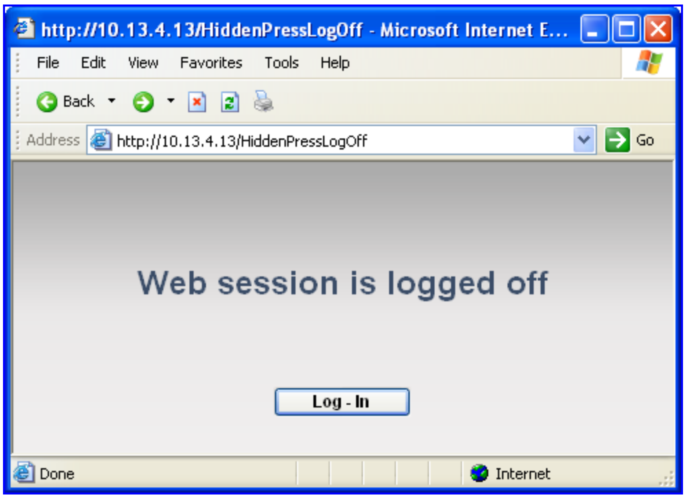
Figure 3-31: Log Off Confirmation Box



Log Off?

2. Click **OK**; the Web session is logged off and the **Log In** button appears.

Figure 3-32: Web Session Logged Off



http://10.13.4.13/HiddenPressLogOff

Web session is logged off

To log in again, simply click the **Log In** button, and then in the 'Enter Network Password' dialog box, enter your user name and password (refer to "Accessing the Web Interface" on page 20).

3.4 Configuration Tab

The **Configuration** tab on the Navigation bar displays all menus related to device configuration. These menus appear in the Navigation tree and include the following:

- Network Settings (refer to "Network Settings" on page 50)
- Media Settings (refer to "Media Settings" on page 65)
- PSTN Settings (refer to “PSTN Settings” on page 82)
- SS7 Configuration (refer to “SS7 Configuration” on page 99)
- Sigtran Configuration (refer to “Sigtran Configuration” on page 99)
- Security Settings (refer to "Security Settings" on page 99)
- Protocol Configuration (refer to "Protocol Configuration" on page 120)
- Advanced Applications (refer to "Advanced Applications" on page 213)
- TDM Configuration (refer to “Configuring the TDM Bus Settings” on page 218)

➢ To access the menus of the Configuration tab, take this step:

- On the Navigation bar, click the **Configuration** tab; the Navigation tree displays the configuration menus pertaining to the **Configuration** tab.

3.4.1 Network Settings

The **Network Settings** menu allows you to configure various networking parameters. This menu contains the following page items:

- IP Settings (refer to "Configuring the IP Settings" on page 50)
- Application Settings (refer to "Configuring the Application Settings" on page 57)
- IP Routing Table (refer to "Configuring the IP Routing Table" on page 62)
- QoS Settings (refer to "Configuring the QoS Settings" on page 63)

3.4.1.1 Configuring the IP Settings

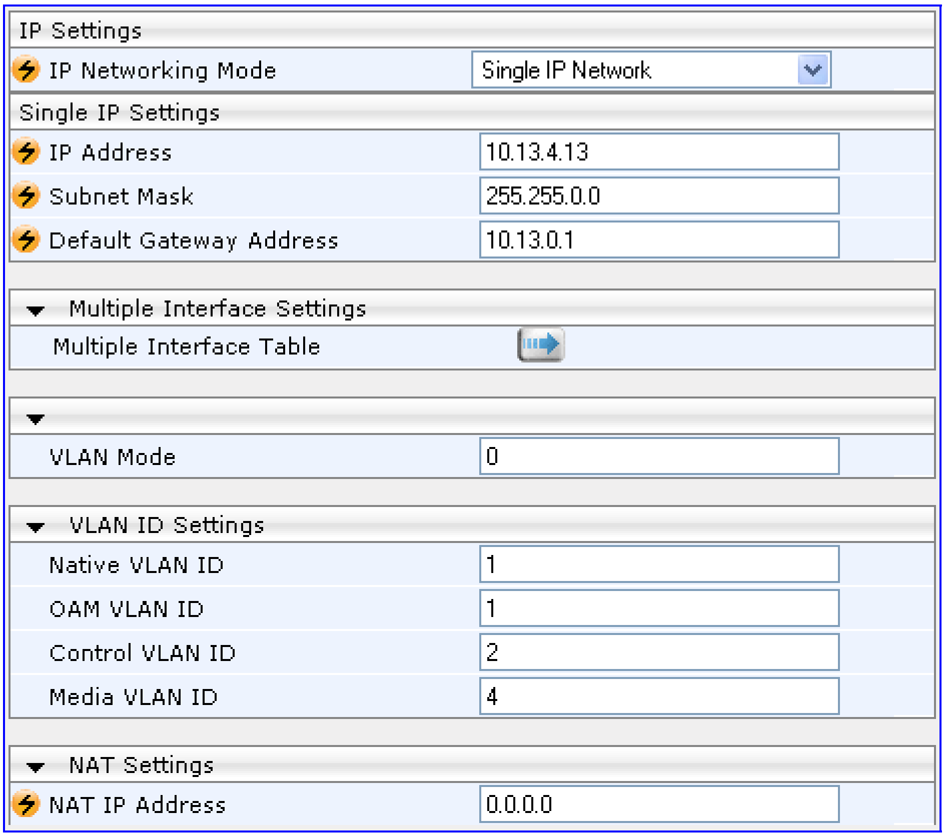
The 'IP Settings' page is used for configuring basic IP networking parameters such as the device's IP address. However, from this page you can also access the 'Multiple Interface Table' page for configuring multiple interfaces.

> **Note:** Once you configure multiple interfaces in the 'Multiple Interface Table' page (accessed by clicking the ➡ button), when clicking the **IP Settings** page item in the Navigation tree, the 'Multiple Interface Table' page is accessed (instead of the 'IP Settings' page).

➢ To configure the IP settings parameters, take these 4 steps:

1. Open the 'IP Settings' page (**Configuration** tab > **Network Settings** menu > **IP Settings** page item).

Figure 3-33: IP Settings Page



IP Settings

IP Networking Mode	Single IP Network

Single IP Settings

IP Address	10.13.4.13
Subnet Mask	255.255.0.0
Default Gateway Address	10.13.0.1

Multiple Interface Settings

Multiple Interface Table	➡
VLAN Mode	0

VLAN ID Settings

Native VLAN ID	1
OAM VLAN ID	1
Control VLAN ID	2
Media VLAN ID	4

NAT Settings

NAT IP Address	0.0.0.0

2. Configure the IP parameters according to the table below.

3. Click the **Submit** button to save your changes.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-7: Network Settings -- IP Settings Parameters

Parameter	Description
IP Settings	
IP Networking Mode **[EnableMultipleIPs]**	Determines the IP network scheme. ▪ **[0]** Single IP Network = Single IP network (default). ▪ **[1]** Multiple IP Networks = Multiple IP networks (OAMP, Media, and Control). ▪ **[1]** Dual IP (Media & Control) = Multiple IP networks. ▪ **[1]** Dual IP (OAM & Control) = Multiple IP networks. ▪ **[1]** Dual IP (OAM & Medial) = Multiple IP networks. **Note:** This parameter is not relevant when using Multiple Interface tables, activated by clicking the **Multiple Interface Table** button ➡ described below (refer to "Configuring the Multiple Interface Table" on

Parameter	Description
	page 53). For detailed information on Multiple IPs, refer to "Multiple IPs" on page 384.
Single IP Settings	
IP Address	IP address of the device. Enter the IP address in dotted-decimal notation, for example, 10.8.201.1. **Notes:** ▪ A warning message is displayed (after clicking **Submit**) if the entered value is incorrect. ▪ After changing the IP address, you must reset the device.
Subnet Mask	Subnet mask of the device. Enter the subnet mask in dotted-decimal notation, for example, 255.255.0.0. **Notes:** ▪ A warning message is displayed (after clicking **Submit**) if the entered value is incorrect. ▪ After changing the subnet mask, you must reset the device.
Default Gateway Address	IP address of the default Gateway used by the device. Enter the IP address in dotted-decimal notation, for example, 10.8.0.1. **Notes:** ▪ A warning message is displayed (after clicking **Submit**) if the entered value is incorrect. ▪ After changing the default Gateway IP address, you must reset the device. ▪ For detailed information on multiple routers support, refer to "Multiple Routers Support" on page 383.
OAM Network Settings (Available only in Multiple IP and Dual IP modes.)	
IP Address **[LocalOAMIPAddress]**	The device's source IP address in the operations, administration, maintenance, and provisioning (OAMP) network. The default value is 0.0.0.0.
Subnet Mask **[LocalOAMSubnetMask]**	The device's subnet mask in the OAMP network. The default subnet mask is 0.0.0.0.
Default Gateway Address **[LocalOAMDefaultGW]**	N/A. Use the IP Routing table instead (refer to "Configuring the IP Routing Table" on page 62).
Control Network Settings (Available only in Multiple IP and Dual IP modes.)	
IP Address **[LocalControlIPAddress]**	The device's source IP address in the Control network. The default value is 0.0.0.0.
Subnet Mask **[LocalControlSubnetMask]**	The device's subnet mask in the Control network. The default subnet mask is 0.0.0.0.
Default Gateway Address **[LocalControlDefaultGW]**	N/A. Use the IP Routing table instead (refer to "Configuring the IP Routing Table" on page 62).
Media Network Settings (Available only in Multiple IP and Dual IP modes.)	
IP Address **[LocalMediaIPAddress]**	The device's source IP address in the Media network. The default value is 0.0.0.0.
Subnet Mask **[LocalMediaSubnetMask]**	The device's subnet mask in the Media network. The default subnet mask is 0.0.0.0.

Parameter	Description
Default Gateway Address **[LocalMediaDefaultGW]**	The device's default Gateway IP address in the Media network. The default value is 0.0.0.0.
Multiple Interface Settings	
Multiple Interface Table	Click the right-pointing arrow ➡ button to open the 'Multiple Interface Table' page. For a description of configuring multiple IP interfaces, refer to "Configuring the Multiple Interface Table" on page 53.
VLAN (For detailed information on the device's VLAN implementation, refer to "VLANS and Multiple IPs" on page 384.)	
VLAN Mode **[VlANMode]**	Enables the VLAN functionality. ▪ **[0]** Disable (default). ▪ **[1]** Enable. **Note:** This parameter cannot be changed on-the-fly and requires a device reset.
VALN ID Settings	
Native VLAN ID **[VLANNativeVlanID]**	Defines the native VLAN identifier (Port VLAN ID - PVID). The valid range is 1 to 4094. The default value is 1.
OAM VLAN ID **[VLANOamVlanID]**	Defines the OAMP VLAN identifier. The valid range is 1 to 4094. The default value is 1.
Control VLAN ID **[VLANControlVlanID]**	Defines the Control VLAN identifier. The valid range is 1 to 4094. The default value is 2.
Media VLAN ID **[VLANMediaVlanID]**	Defines the Media VLAN identifier. The valid range is 1 to 4094. The default value is 3.
NAT Settings	
NAT IP Address **[StaticNatIP]**	Global (public) IP address of the device to enable static Network Address Translation (NAT) between the device and the Internet.

3.4.1.2 Configuring the Multiple Interface Table

The 'Multiple Interface Table' page allows you to configure up to three logical network interfaces, each with its own IP address, unique VLAN ID (if enabled), interface name, and application types (i.e., Control, Media, and/or Operations, Administration, Maintenance and Provisioning - OAMP) permitted on the interface. In addition, this page provides VLAN-related parameters for enabling VLANs, and for defining the 'Native' VLAN ID (VLAN ID to which incoming, untagged packets are assigned). For assigning VLAN priorities and Differentiated Services (DiffServ) for the supported Class of Service (CoS), refer to "Configuring the QoS Settings" on page 63.

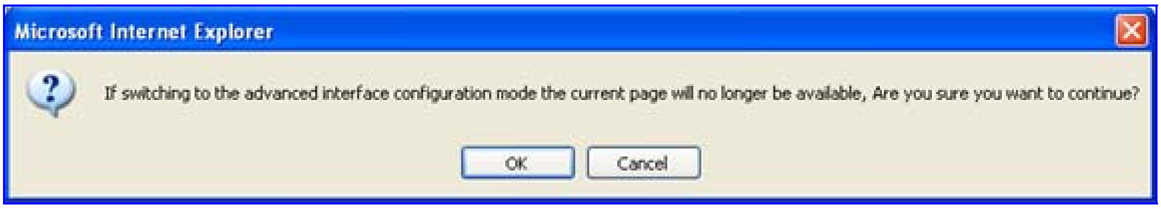
Notes:

- Once you access the 'Multiple Interface Table' page, the 'IP Settings' page is no longer available.
- You can view all added IP interfaces that are currently active, in the 'IP Active Interfaces' page (refer to "Viewing Active IP Interfaces" on page 244).
- You can also configure this table using the *ini* file table parameter InterfaceTable (refer to "Networking Parameters" on page 260).

➢ To configure the multiple IP interface table, take these 7 steps:

1. Open the 'IP Settings' page (refer to "Configuring the IP Settings" on page 50).
2. Under the Multiple Interface Settings group, click the right-arrow ➡ button alongside **Multiple Interface Table**; a confirmation message box appears:

Figure 3-34: Confirmation Message for Accessing the Multiple Interface Table

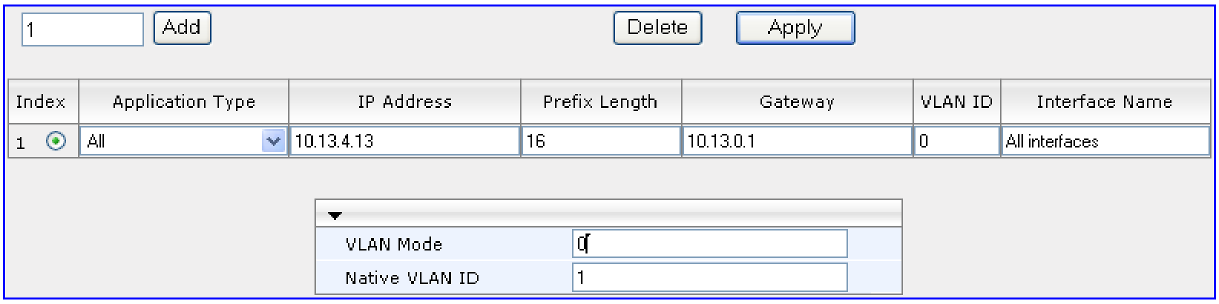


Microsoft Internet Explorer

If switching to the advanced interface configuration mode the current page will no longer be available, Are you sure you want to continue?

3. Click **OK** to confirm; the 'Multiple Interface Table' page appears:

Figure 3-35: Interface Table Page



1

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
1 ●	All	10.13.4.13	16	10.13.0.1	0	All interfaces

VLAN Mode	0
Native VLAN ID	1

4. In the 'Add' field, enter the desired index number for the new interface, and then click **Add**; the index row is added to the table.
5. Configure the interface according to the table below.
6. Click the **Apply** button; the interface is immediately applied to the device.
7. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- When adding more than one interface to the table, ensure that you enable VLANs, using the 'VLAN Mode' (VlANMode) parameter.
- When booting using BootP/DHCP protocols (refer to the *Product Reference Manual*), an IP address is obtained from the server. This address is used as the OAMP address for this session, overriding the IP address you configured in the 'Multiple Interface Table' page. The address specified in this table takes effect only after you save the configuration to the device's flash memory. This enables the device to use a temporary IP address for initial management and configuration, while retaining the address (defined in this table) for deployment.
- For a detailed description on multiple IP interfaces and VLANs, refer to "VLANS and Multiple IPs" on page 384.
- For a description of the Web interface's table command buttons (e.g., **Duplicate** and **Delete**), refer to "Working with Tables" on page 30.

Table 3-8: Multiple Interface Table Parameters Description

Parameter	Description
Table parameters	
Index	Index of each interface. The range is 0-3. **Note:** Each interface index must be unique.
Application Type	Types of applications that are allowed on the specific interface. ▪ **[0]** OAM = Only Operations, Administration, Maintenance and Provisioning (OAMP) applications (e.g., Web, Telnet, SSH, and SNMP) are allowed on the interface. ▪ **[1]** Media = Only Media (i.e., RTP streams of voice/video) is allowed on the interface. ▪ **[2]** Control = Only Call Control applications (e.g., SIP) are allowed on the interface. ▪ **[3]** OAM & Media = Only OAMP and Media (RTP) applications are allowed on the interface. ▪ **[4]** OAM & Control = Only OAMP and Call Control applications are allowed on the interface. ▪ **[5]** Media & Control = Only Media (RTP) and Call Control applications are allowed on the interface. ▪ **[6]** All = All the applications are allowed on the interface. **Notes:** ▪ Only one IPv4 interface of OAM can be configured. ▪ Only one IPv4 interface of Control can be configured. ▪ At least one interface with Media must be configured.
IP Address	The IPv4 IP address in dotted-decimal notation. **Note:** Each interface must be assigned a unique IP address.

Parameter	Description
Prefix Length	This column lists the number of '1' bits in the subnet mask (i.e., replaces the standard dotted-decimal representation of the subnet mask for IPv4 interfaces). For example: A subnet mask of 255.0.0.0 is represented by a prefix length of 8 (i.e., 11111111 00000000 00000000 00000000), and a subnet mask of 255.255.255.252 is represented by a prefix length of 30 (i.e., 11111111 11111111 11111111 11111100). The prefix length is a Classless Inter-Domain Routing (CIDR) style presentation of a dotted-decimal subnet notation. The CIDR-style presentation is the latest method for interpretation of IP addresses. Specifically, instead of using eight-bit address blocks, it uses the variable-length subnet masking technique to allow allocation on arbitrary-length prefixes (refer to http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing for more information). The prefix length values range from 0 to 31.
Gateway	Defines the IP address of the default gateway used by the device. **Notes:** ▪ Only one default gateway can be configured for the device and it must be configured on an interface for Media traffic. All other table entries for this column must have the value 0.0.0.0. ▪ The default gateway's IP address must be in the same subnet as the interface address. ▪ For configuring additional routing rules for other interfaces, refer to "Configuring the IP Routing Table" on page 62.
VLAN ID	Defines the VLAN ID for each interface. When using VLANs, the VLAN ID must be unique for each interface. Incoming traffic tagged with this VLAN ID is routed to the corresponding interface, and outgoing traffic from that interface is tagged with this VLAN ID.
Interface Name	Defines a string (up to 16 characters) to name this interface. This name is displayed in management interfaces (Web, CLI and SNMP) for better readability and has no functional use. **Note:** The interface name is a mandatory parameter and must be unique for each interface.
General Parameters	
VLAN Mode **[VlANMode]**	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
Native VLAN ID **[VLANNativeVlanID]**	Defines the VLAN ID to which untagged incoming traffic is assigned. Outgoing packets sent to this VLAN are sent only with a priority tag (VLAN ID = 0). When this parameter is equal to one of the VLAN IDs in the Interface Table (and VLANs are enabled), untagged incoming traffic is considered as an incoming traffic for that interface. Outgoing traffic sent from this interface is sent with the priority tag (tagged with VLAN ID = 0). When this parameter is different from any value in the 'VLAN ID' column in the Interface Table, untagged incoming traffic is discarded, and all outgoing traffic is tagged. **Note:** If this parameter is not set (i.e., default value is 1), but one of the interfaces has a VLAN ID configured to 1, this interface is still considered the 'Native' VLAN. If you do not wish to have a 'Native' VLAN ID and want to use VLAN ID 1, set this parameter to a value other than any VLAN ID in the table.

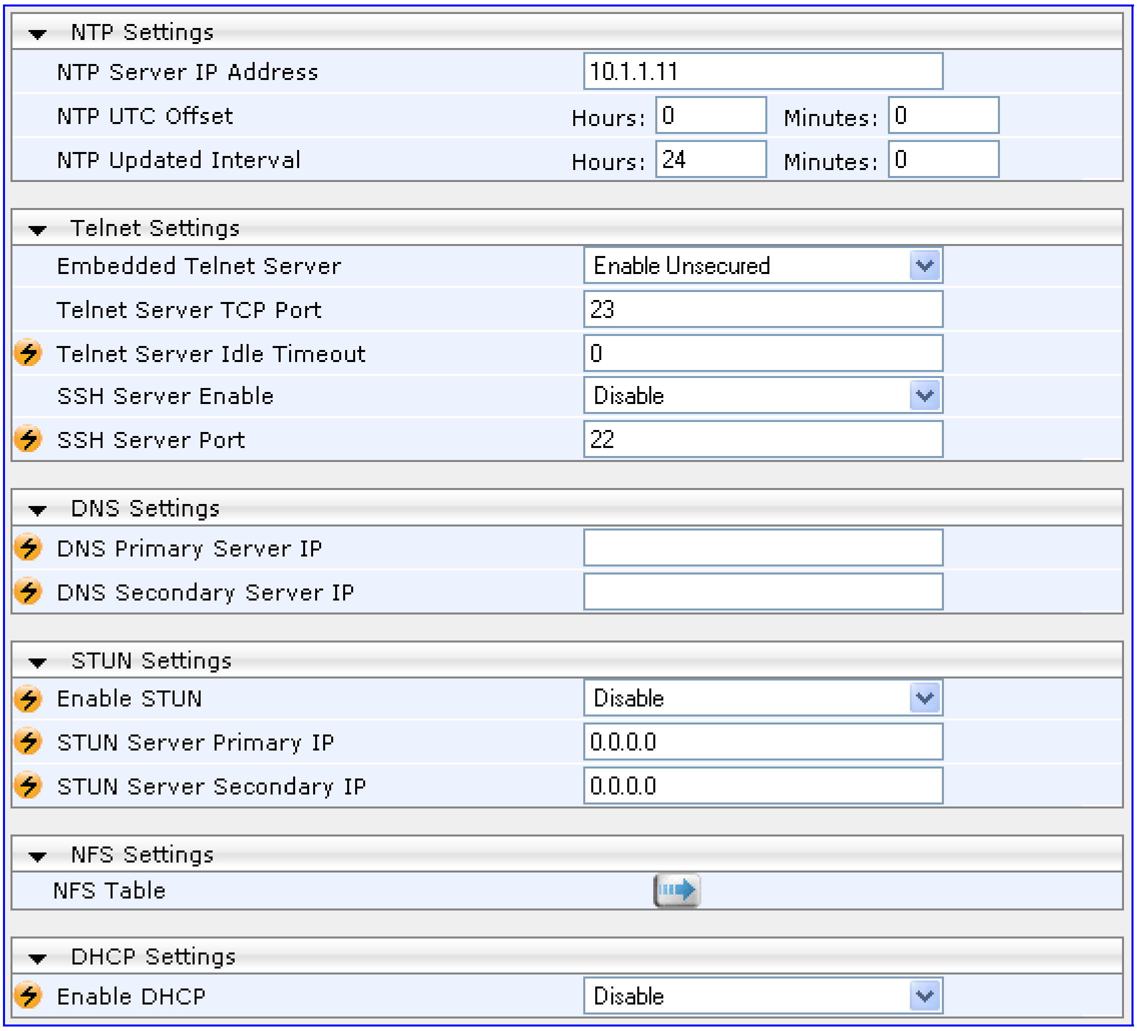
3.4.1.3 Configuring the Application Settings

The 'Application Settings' page is used for configuring various application parameters such as Telnet.

➢ **To configure the Application settings parameters, take these 4 steps:**

1. Open the 'Application Settings' page (**Configuration** tab > **Network Settings** menu > **Application Settings** page item).

Figure 3-36: Application Settings Page



▾ NTP Settings

NTP Server IP Address	10.1.1.11
NTP UTC Offset	Hours: 0 Minutes: 0
NTP Updated Interval	Hours: 24 Minutes: 0

▾ Telnet Settings

Embedded Telnet Server	Enable Unsecured
Telnet Server TCP Port	23
⚡ Telnet Server Idle Timeout	0
SSH Server Enable	Disable
⚡ SSH Server Port	22

▾ DNS Settings

⚡ DNS Primary Server IP	
⚡ DNS Secondary Server IP	

▾ STUN Settings

⚡ Enable STUN	Disable
⚡ STUN Server Primary IP	0.0.0.0
⚡ STUN Server Secondary IP	0.0.0.0

▾ NFS Settings

NFS Table	➡

▾ DHCP Settings

⚡ Enable DHCP	Disable

2. Configure the Applications parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-9: Application Settings Parameters

Parameter	Description
NTP Settings (For detailed information on Network Time Protocol (NTP), refer to "Simple Network Time Protocol Support" on page 383.)	
NTP Server IP Address **[NTPServerIP]**	IP address (in dotted-decimal notation) of the NTP server. The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).
NTP UTC Offset **[NTPServerUTCOffset]**	Defines the Universal Time Coordinate (UTC) offset (in seconds) from the NTP server. The default offset is 0. The offset range is -43200 to 43200.
NTP Update Interval **[NTPUpdateInterval]**	Defines the time interval (in seconds) that the NTP client requests for a time update. The default interval is 86400 (i.e., 24 hours). The range is 0 to 214783647. **Note:** AudioCodes does not recommend setting this parameter to beyond one month (i.e., 2592000 seconds).
Telnet Settings	
Embedded Telnet Server **[TelnetServerEnable]**	Enables or disables the device's embedded Telnet server. Telnet is disabled by default for security reasons. ▪ **[0]** Disable (default) ▪ **[1]** Enable Unsecured ▪ **[2]** Enable Secured (SSL) **Note:** Only the primary Web User Account (which has Security Administration access level) can access the device using Telnet (refer to "Configuring the Web User Accounts" on page 99).
Telnet Server TCP Port **[TelnetServerPort]**	Defines the port number for the embedded Telnet server. The valid range is all valid port numbers. The default port is 23.
Telnet Server Idle Timeout **[TelnetServerIdleDisconnect]**	Defines the timeout (in minutes) for disconnection of an idle Telnet session. When set to zero, idle sessions are not disconnected. The valid range is any value. The default value is 0.
SSH Server Enable **[SSHServerEnable]**	Enables or disables the embedded Secure Shell (SSH) server. ▪ **[0]** Disable (default) ▪ **[1]** Enable
SSH Server Port **[SSHServerPort]**	Defines the port number for the embedded SSH server. Range is any valid port number. The default port is 22.
DNS Settings	
DNS Primary Server IP **[DNSPriServerIP]**	IP address of the primary DNS server. Enter the IP address in dotted-decimal notation, for example, 10.8.2.255. **Note:** To use Fully Qualified Domain Names (FQDN) in the 'Tel to IP Routing' table (or 'Outbound IP Routing' table if EnableSBC is set to 1), you must define this parameter.
DNS Secondary Server IP **[DNSSecServerIP]**	IP address of the second DNS server. Enter the IP address in dotted-decimal notation, for example, 10.8.2.255.

Parameter	Description
STUN Settings	
Enable STUN **[EnableSTUN]**	Determines whether Simple Traversal of UDP through NATs (STUN) is enabled. ▪ **[0]** Disable (default) ▪ **[1]** Enable When enabled, the device functions as a STUN client and communicates with a STUN server located in the public Internet. STUN is used to discover whether the device is located behind a NAT and the type of NAT. In addition, it is used to determine the IP addresses and port numbers that the NAT assigns to outgoing signaling messages (using SIP) and media streams (using RTP, RTCP and T.38). STUN works with many existing NAT types and does not require any special behavior from them. For detailed information on STUN, refer to "STUN" on page 381. **Notes:** ▪ For defining the STUN server domain name, use the *ini* file parameter STUNServerDomainName (refer to "Networking Parameters" on page 260). ▪ This parameter cannot be changed on-the-fly and requires a device reset.
STUN Server Primary IP **[STUNServerPrimaryIP]**	Defines the IP address of the primary STUN server. The valid range is the legal IP addresses. The default value is 0.0.0.0.
STUN Server Secondary IP **[STUNServerSecondaryIP]**	Defines the IP address of the secondary STUN server. The valid range is the legal IP addresses. The default value is 0.0.0.0.
NFS Settings	
NFS Table	For detailed information on configuring the NFS table, refer to "Configuring the NFS Settings" on page 60.
DHCP Settings	
Enable DHCP **[DHCPEnable]**	Determines whether Dynamic Host Control Protocol (DHCP) is enabled. ▪ **[0]** Disable = Disable DHCP support on the device (default). ▪ **[1]** Enable = Enable DHCP support on the device. After the device powers up, it attempts to communicate with a BootP server. If a BootP server does not respond and if DHCP is enabled, then the device attempts to obtain its IP address and other networking parameters from the DHCP server. **Notes:** ▪ After you enable the DHCP server, perform the following procedure: 1. Click the **Submit** button, and then save the configuration (refer to "Saving Configuration" on page 230). 2. Perform a cold reset using the device's hardware reset button (soft reset via Web interface doesn't trigger the BootP/DHCP procedure and this parameter reverts to 'Disable'). ▪ Throughout the DHCP procedure the BootP/TFTP application

Parameter	Description
	must be deactivated, otherwise, the device receives a response from the BootP server instead of from the DHCP server. ▪ For additional information on DHCP, refer to the *Product Reference Manual*. ▪ DHCPEnable is a special 'Hidden' parameter. Once defined and saved in flash memory, its assigned value doesn't revert to its default even if the parameter doesn't appear in the *ini* file.

3.4.1.4 Configuring the NFS Settings

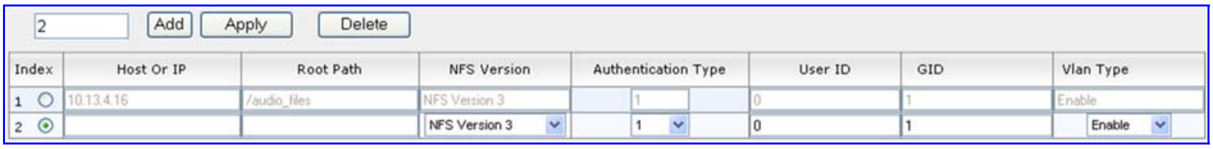
Network File System (NFS) enables the device to access a remote server's shared files and directories, and to handle them as if they're located locally. You can configure up to five different NFS file systems. As a file system, the NFS is independent of machine types, OSs, and network architectures. NFS is used by the device to load the *cmp*, *ini*, and auxiliary files, using the Automatic Update mechanism (refer to Automatic Update Mechanism). Note that an NFS file server can share multiple file systems. There must be a separate row for each remote file system shared by the NFS file server that needs to be accessed by the device.

➢ To add remote NFS file systems, take these 6 steps:

1. Open the 'Application Settings' page (refer to "Configuring the Application Settings" on page 57).

2. Under the NFS Settings group, click the right-arrow button alongside **NFS Table**; the 'NFS Settings' page appears.

Figure 3-37: NFS Settings Page



2 | Add | Apply | Delete

Index		Host Or IP	Root Path	NFS Version	Authentication Type	User ID	GID	Vlan Type
1	○	10.13.4.16	/audio_files	NFS Version 3	1	0	1	Enable
2	●			NFS Version 3	1	0	1	Enable

3. In the 'Add' field, enter the index number of the remote NFS file system, and then click **Add**; an empty entry row appears in the table.

4. Configure the NFS parameters according to the table below.

5. Click the **Apply** button; the remote NFS file system is immediately applied, which can be verified by the appearance of the 'NFS mount was successful' message in the Syslog server.

6. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- To avoid terminating current calls, a row must not be deleted or modified while the device is currently accessing files on that remote NFS file system.
- The combination of 'HostOrIP' and 'RootPath' must be unique for each row in the table. For example, the table must include only one row with a Host / IP of 192.168.1.1 and Root Path of /audio.
- For a description of the web interface's table command buttons (e.g., **Duplicate** and **Delete**), refer to "Working with Tables" on page 30.
- You can also configure the NFS table using the *ini* file table parameter NFSServers (refer to "Networking Parameters" on page 260).

Table 3-10: Network Settings -- NFS Settings Parameters

Parameter	Description
Index	The row index of the remote file system. The valid range is 0 to 4.
Host Or IP	The domain name or IP address of the NFS server. If a domain name is provided, a DNS server must be configured.
Root Path	Path to the root of the remote file system in the format: /[path]. For example, '/audio'.
NFS Version	NFS version used to access the remote file system. ▪ **[2]** NFS Version 2. ▪ **[3]** NFS Version 3 (default).
Authentication Type	Authentication method used for accessing the remote file system. ▪ **[0]** = Auth NULL. ▪ **[1]** = Auth UNIX (default).
UID	User ID used in authentication when using Auth UNIX. The valid range is 0 to 65537. The default is 0.
GID	Group ID used in authentication when using Auth UNIX. The valid range is 0 to 65537. The default is 1.
VLAN Type	The VLAN type for accessing the remote file system. ▪ **[0]** OAMP. ▪ **[1]** Media (default). **Note:** This parameter applies only if VLANs are enabled or if Multiple IPs is configured (refer to "VLANS and Multiple IPs" on page 384).

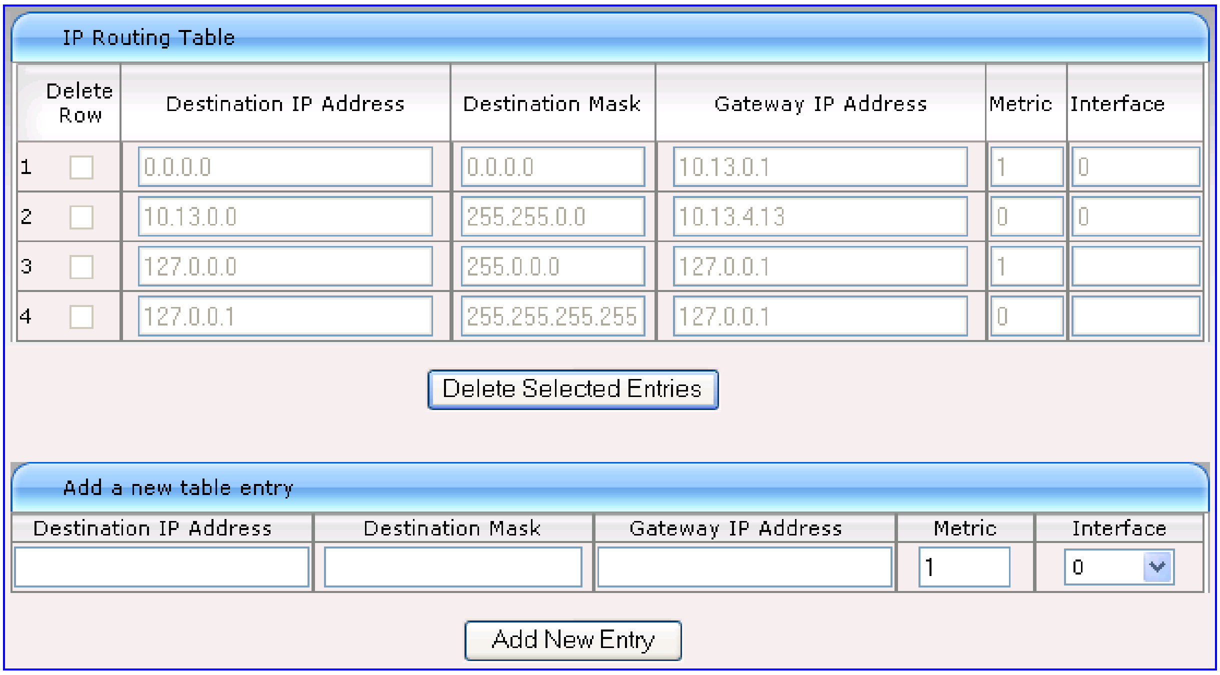
3.4.1.5 Configuring the IP Routing Table

The 'IP Routing Table' page allows you to define up to 50 static IP routing rules for the device. For example, you can define static routing rules for the OAMP and Control networks since a default gateway is supported only for the Media traffic network (refer to "Configuring the Multiple Interface Table" on page 53). Before sending an IP packet, the device searches this table for an entry that matches the requested destination host / network. If such an entry is found, the device sends the packet to the indicated router. If no explicit entry is found, the packet is sent to the default gateway (configured in the 'IP Settings' page-- refer to "Configuring the IP Settings" on page 50).

➢ To configure static IP routing, take these 3 steps:

1. Open the 'IP Routing Table' page (**Configuration** tab > **Network Settings** menu > **IP Routing Table** page item).

Figure 3-38: IP Routing Table Page



IP Routing Table

	Delete Row	Destination IP Address	Destination Mask	Gateway IP Address	Metric	Interface
1	□	0.0.0.0	0.0.0.0	10.13.0.1	1	0
2	□	10.13.0.0	255.255.0.0	10.13.4.13	0	0
3	□	127.0.0.0	255.0.0.0	127.0.0.1	1	
4	□	127.0.0.1	255.255.255.255	127.0.0.1	0	

Add a new table entry

Destination IP Address	Destination Mask	Gateway IP Address	Metric	Interface
			1	0

2. In the 'Add a new table entry' group, add a new static routing rule according to the parameters described in the table below.

3. Click **Add New Entry**; the new routing rule is added to the IP routing table.

To delete a routing rule from the table, select the 'Delete Row' check box that corresponds to the routing rule entry, and then click **Delete Selected Entries**.

Table 3-11: IP Routing Table Description

Parameter	Description
Destination IP Address **[RoutingTableDestinationsColumn]**	Specifies the IP address of the destination host / network.
Destination Mask **[RoutingTableDestinationMasksColumn]**	Specifies the subnet mask of the destination host / network.

Parameter	Description
The address of the host / network you want to reach is determined by an AND operation that is applied to the fields 'Destination IP Address' and 'Destination Mask'. For example, to reach the network 10.8.x.x, enter 10.8.0.0 in the field 'Destination IP Address' and 255.255.0.0 in the field 'Destination Mask'. As a result of the AND operation, the value of the last two octets in the field 'Destination IP Address' is ignored. To reach a specific host, enter its IP address in the field 'Destination IP Address' and 255.255.255.255 in the field 'Destination Mask'.	
Gateway IP Address **[RoutingTableGatewaysColumn]**	The IP address of the router (next hop) to which the packets are sent if their destination matches the rules in the adjacent columns. **Note:** The Gateway address must be in the same subnet on which the address is configured on the 'Multiple Interface Table' page (refer to "Configuring the Multiple Interface Table" on page 53).
Metric **[RoutingTableHopsCountColumn]**	The maximum number of allowed routers (hops) between the device and destination. **Note:** This parameter must be set to 1 for the routing rule to be valid. Routing entries with Hop Count equals 0 are local routes set automatically by the device.
Interface **[RoutingTableInterfacesColumn]**	Specifies the interface (network type) to which the routing rule is applied. ▪ **[0]** = OAMP (default). ▪ **[1]** = Media. ▪ **[2]** = Control. For detailed information on the network types, refer to "Configuring the Multiple Interface Table" on page 53.

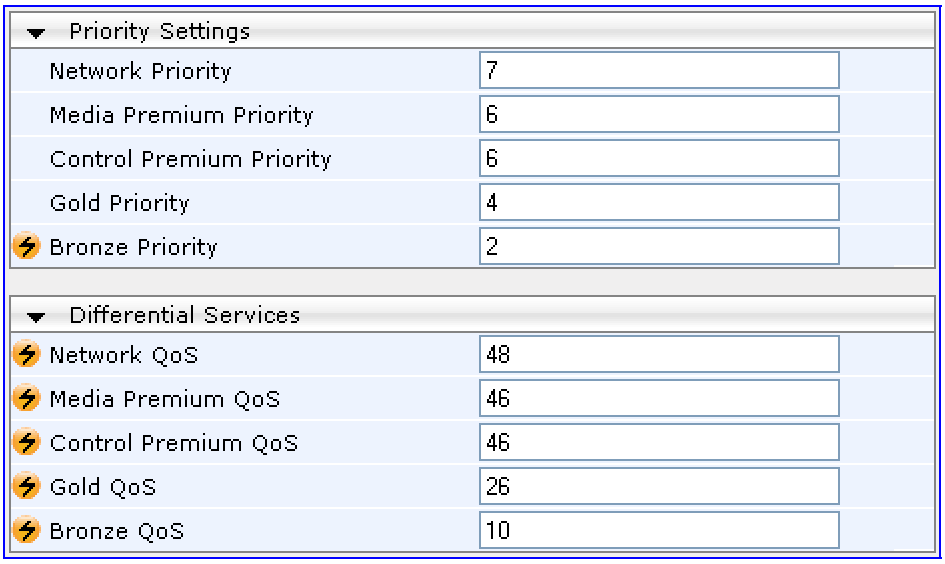
3.4.1.6 Configuring the QoS Settings

The 'QoS Settings' page is used for configuring the Quality of Service (QoS) parameters. This page allows you to assign VLAN priorities (IEEE 802.1p) and Differentiated Services (DiffServ) for the supported Class of Service (CoS).

➢ To configure QoS, take these 4 steps:

1. Open the 'QoS Settings' page (**Configuration** tab > **Network Settings** menu > **QoS Settings** page item).

Figure 3-39: QoS Settings Page



▼ Priority Settings

Network Priority	7
Media Premium Priority	6
Control Premium Priority	6
Gold Priority	4
⚡ Bronze Priority	2

▼ Differential Services

⚡ Network QoS	48
⚡ Media Premium QoS	46
⚡ Control Premium QoS	46
⚡ Gold QoS	26
⚡ Bronze QoS	10

2. Configure the QoS parameters according to the table below.

3. Click the **Submit** button to save your changes.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-12: QoS Settings Parameters

Parameter	Description
Priority Settings	
Network Priority **[VLANNetworkServiceClassPriority]**	Defines the priority for Network Class of Service (CoS) content. The valid range is 0 to 7. The default value is 7.
Media Premium Priority **[VLANPremiumServiceClassMediaPriority]**	Defines the priority for the Premium CoS content and media traffic. The valid range is 0 to 7. The default value is 6.
Control Premium Priority **[VLANPremiumServiceClassControlPriority]**	Defines the priority for the Premium CoS content and control traffic. The valid range is 0 to 7. The default value is 6.
Gold Priority **[VLANGoldServiceClassPriority]**	Defines the priority for the Gold CoS content. The valid range is 0 to 7. The default value is 4.
Bronze Priority **[VLANBronzeServiceClassPriority]**	Defines the priority for the Bronze CoS content. The valid range is 0 to 7. The default value is 2.
Differential Services (For detailed information on IP QoS using Differentiated Services, refer to "IP QoS via Differentiated Services (DiffServ)" on page 384).	
Network QoS **[NetworkServiceClassDiffServ]**	Defines the DiffServ value for Network CoS content. The valid range is 0 to 63. The default value is 48.
Media Premium QoS	Defines the DiffServ value for Premium Media CoS

Parameter	Description
[PremiumServiceClassMediaDiffServ]	content (only if IPDiffServ is not set in the selected IP Profile). The valid range is 0 to 63. The default value is 46. **Note:** The value for the Premium Control DiffServ is determined by the following (according to priority): ▪ IPDiffServ value in the selected IP Profile. ▪ PremiumServiceClassMediaDiffServ.
Control Premium QoS **[PremiumServiceClassControlDiffServ]**	Defines the DiffServ value for Premium Control CoS content (only if ControlIPDiffserv is not set in the selected IP Profile). The valid range is 0 to 63. The default value is 40. **Note:** The value for the Premium Control DiffServ is determined by the following (according to priority): ▪ ControlPDiffserv value in the selected IP Profile. ▪ PremiumServiceClassControlDiffServ.
Gold QoS **[GoldServiceClassDiffServ]**	Defines the DiffServ value for the Gold CoS content. The valid range is 0 to 63. The default value is 26.
Bronze QoS **[BronzeServiceClassDiffServ]**	Defines the DiffServ value for the Bronze CoS content. The valid range is 0 to 63. The default value is 10.

3.4.2 Media Settings

The **Media Settings** menu allows you to configure the device's channel parameters. These parameters are applied to all the device's channels. This menu contains the following page items:

- Voice Settings (refer to "Configuring the Voice Settings" on page 66)
- Fax/Modem/CID Settings (refer to "Configuring the Fax / Modem / CID Settings" on page 67)
- RTP/RTCP Settings (refer to "Configuring the RTP / RTCP Settings" on page 71)
- IPmedia Settings (refer to “Configuring the IPmedia Settings” on page 76)
- General Media Settings (refer to "Configuring the General Media Settings" on page 78)
- DSP Templates (refer to “Configuring the DSP Templates” on page 79)
- Media Security (refer to "Configuring Media Security" on page 80)

Notes:

- Channel parameters can be modified on-the-fly. Changes take effect from the next call.
- Some channel parameters can be configured per channel or call routing, using profiles (refer to "Configuring the Profile Definitions" on page 190).

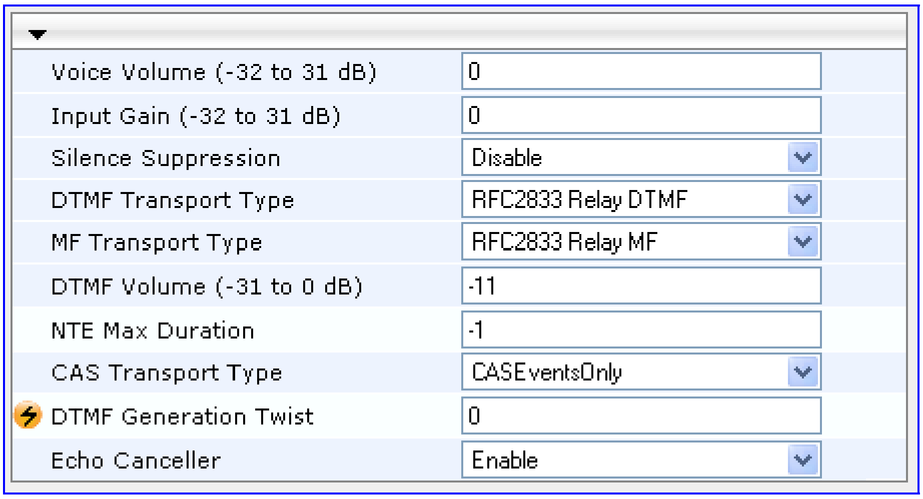
3.4.2.1 Configuring the Voice Settings

The 'Voice Settings' page is used for configuring various voice parameters such as voice volume.

➢ To configure the Voice parameters, take these 4 steps:

1. Open the 'Voice Settings' page (**Configuration** tab > **Media Settings** menu > **Voice Settings** page item).

Figure 3-40: Voice Settings Page



Voice Volume (-32 to 31 dB)	0
Input Gain (-32 to 31 dB)	0
Silence Suppression	Disable
DTMF Transport Type	RFC2833 Relay DTMF
MF Transport Type	RFC2833 Relay MF
DTMF Volume (-31 to 0 dB)	-11
NTE Max Duration	-1
CAS Transport Type	CASEventsOnly
DTMF Generation Twist	0
Echo Canceller	Enable

2. Configure the Voice parameters according to the table below.

3. Click the **Submit** button to save your changes.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-13: Media Settings, Voice Settings Parameters

Parameter	Description
Voice Volume **[VoiceVolume]**	Voice gain control (in decibels). This parameter sets the level for the transmitted (IP-to-PSTN) signal. The valid range is -32 to 31 dB. The default value is 0 dB.
Input Gain **[InputGain]**	Pulse-code modulation (PCM) input gain control (in decibels). This parameter sets the level for the received (PSTN-to-IP) signal. The valid range is -32 to 31 dB. The default value is 0 dB.
Silence Suppression **[EnableSilenceCompression]**	Silence Suppression is a method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. ▪ **[0]** Disable = Silence Suppression is disabled (default). ▪ **[1]** Enable = Silence Suppression is enabled. ▪ **[2]** Enable without Adaptation = A single silence packet is sent during a silence period (applicable only to G.729). **Note:** If the selected coder is G.729, the following rules determine the value of the 'annexb' parameter of the fmtp attribute in the SDP: ▪ If EnableSilenceCompression is 0: 'annexb=no'. ▪ If EnableSilenceCompression is 1: 'annexb=yes'. ▪ If EnableSilenceCompression is 2 and IsCiscoSCEMode is 0: 'annexb=yes'.

Parameter	Description
	▪ If EnableSilenceCompression is 2 and IsCiscoSCEMode is 1: 'annexb=no'.
Echo Canceler **[EnableEchoCanceller]**	Determines whether echo cancellation is enabled and therefore, echo from voice calls is removed. ▪ **[0]** Off = Echo Canceler is disabled. ▪ **[1]** On = Echo Canceler is enabled (default). **Note:** This parameter is used to maintain backward compatibility.
DTMF Transport Type **[DTMFTransportType]**	Determines the DTMF transport type. ▪ **[0]** DTMF Mute = Erases digits from voice stream and doesn't relay to remote. ▪ **[2]** Transparent DTMF = Digits remain in voice stream. ▪ **[3]** RFC 2833 Relay DTMF = Erases digits from voice stream and relays to remote according to RFC 2833 (default). ▪ **[7]** RFC 2833 Relay Rcv Mute = DTMFs are sent according to RFC 2833 and muted when received. **Note:** This parameter is automatically updated if one of the following parameters is configured: TxDTMFOption or RxDTMFOption.
MF Transport Type **[MFTransportType]**	Not Applicable.
DTMF Volume (-31 to 0 dB) **[DTMFVolume]**	DTMF gain control value (in decibels) to the TDM side. The valid range is -31 to 0 dB. The default value is -11 dB.
CAS Transport Type **[CASTransportType]**	Controls the ABCD signaling transport type over IP. ▪ **[0]** CAS Events Only = Disable CAS relay (default). ▪ **[1]** CAS RFC2833 Relay = Enable CAS relay mode using RFC 2833. The CAS relay mode can be used with the TDM tunneling feature to enable tunneling over IP for both voice and CAS signaling bearers.
DTMF Generation Twist **[DTMFGenerationTwist]**	Defines the range (in decibels) between the high and low frequency components in the DTMF signal. Positive decibel values cause the higher frequency component to be stronger than the lower one. Negative values cause the opposite effect. For any parameter value, both components change so that their average is constant. The valid range is -10 to 10 dB. The default value is 0 dB.

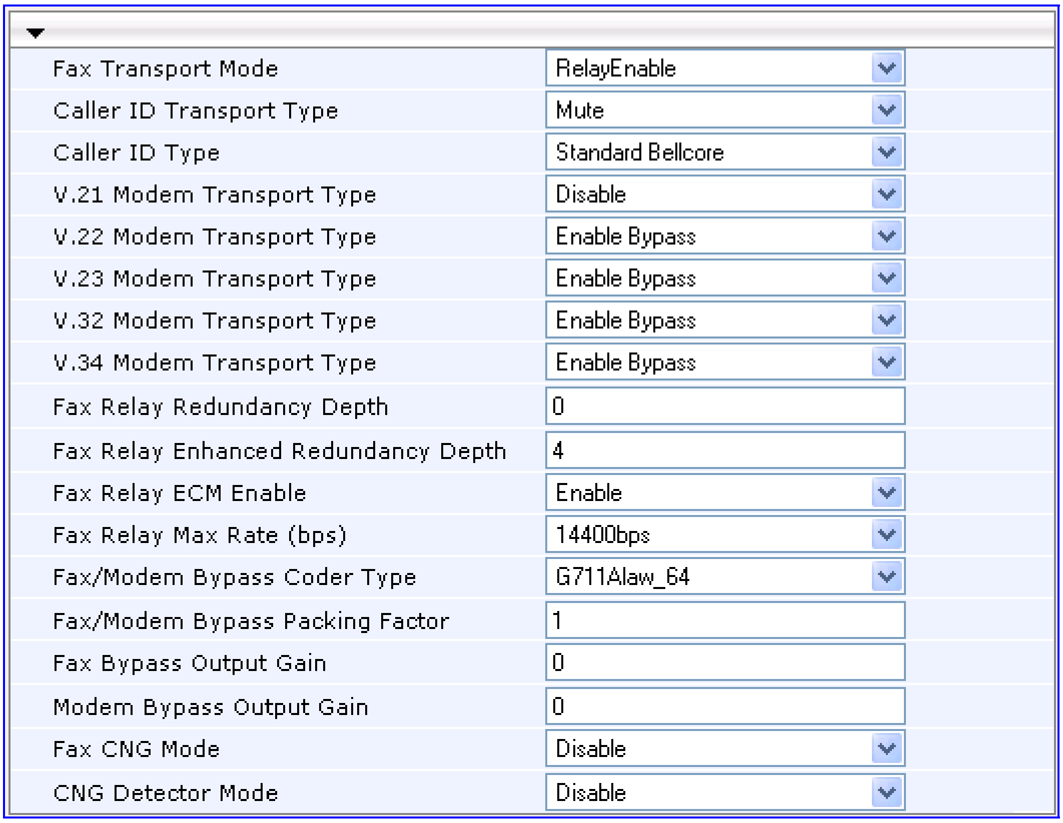
3.4.2.2 Configuring the Fax / Modem / CID Settings

The 'Fax/Modem/CID Settings' page is used for configuring fax, modem, and Caller ID (CID) parameters.

- **To configure the fax, modem, and CID parameters, take these 4 steps:**

1. Open the 'Fax/Modem/CID Settings' page (**Configuration** tab > **Media Settings** menu > **Fax/Modem/CID Settings** page item).

Figure 3-41: Fax/Modem/CID Settings Page



Fax Transport Mode	RelayEnable
Caller ID Transport Type	Mute
Caller ID Type	Standard Bellcore
V.21 Modem Transport Type	Disable
V.22 Modem Transport Type	Enable Bypass
V.23 Modem Transport Type	Enable Bypass
V.32 Modem Transport Type	Enable Bypass
V.34 Modem Transport Type	Enable Bypass
Fax Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable
Fax Relay Max Rate (bps)	14400bps
Fax/Modem Bypass Coder Type	G711Alaw_64
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0
Modem Bypass Output Gain	0
Fax CNG Mode	Disable
CNG Detector Mode	Disable

2. Configure the fax, Modem, and CID parameters according to the table below.

3. Click the **Submit** button to save your changes.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-14: Media Settings -- Fax/Modem/CID Parameters

Parameter	Description
Fax Transport Mode **[FaxTransportMode]**	Fax transport mode used by the device. - **[0]** Disable = transparent mode. - **[1]** T.38 Relay = (default). - **[2]** Bypass. - **[3]** Events Only. **Note:** This parameter is overridden by the parameter IsFaxUsed (refer to "SIP General Parameters" on page

Parameter	Description
	121). If the parameter IsFaxUsed is set to 1 (T.38 Relay) or 3 (Fax Fallback), then FaxTransportMode is always set to 1 (T.38 relay).
Caller ID Transport Type **[CallerIDTransportType]**	Determines the device's behavior for Caller ID detection. ▪ **[0]** Disable = Caller ID is not detected - DTMF digits remain in the voice stream. ▪ **[1]** Relay = Caller ID is detected - DTMF digits are erased from the voice stream. ▪ **[3]** Mute = Caller ID is detected - DTMF digits are erased from the voice stream (default).
V.21 Modem Transport Type **[V21ModemTransportType]**	V.21 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) -- default ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass. ▪ **[3]** Events Only = Transparent with Events.
V.22 Modem Transport Type **[V22ModemTransportType]**	V.22 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events
V.23 Modem Transport Type **[V23ModemTransportType]**	V.23 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events
V.32 Modem Transport Type **[V32ModemTransportType]**	V.32 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events **Note:** This option applies to V.32 and V.32bis modems.
V.34 Modem Transport Type **[V34ModemTransportType]**	V.90 / V.34 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events

Parameter	Description
Fax Relay Redundancy Depth **[FaxRelayRedundancyDepth]**	Number of times that each fax relay payload is retransmitted to the network. ▪ **[0]** = No redundancy (default). ▪ **[1]** = One packet redundancy. ▪ **[2]** = Two packet redundancy. **Note:** This parameter is applicable only to non-V.21 packets.
Fax Relay Enhanced Redundancy Depth **[FaxRelayEnhancedRedundancyDepth]**	Number of times that control packets are retransmitted when using the T.38 standard. The valid range is 0 to 4. The default value is 0.
Fax Relay ECM Enable **[FaxRelayECMEnable]**	Determines whether the Error Correction Mode (ECM) mode is used during fax relay. ▪ **[0]** Disable = ECM mode is not used during fax relay. ▪ **[1]** Enable = ECM mode is used during fax relay (default).
Fax Relay Max Rate (bps) **[FaxRelayMaxRate]**	Maximum rate (in bps), at which fax relay messages are transmitted (outgoing calls). ▪ **[0]** 2400 = 2.4 kbps. ▪ **[1]** 4800 = 4.8 kbps. ▪ **[2]** 7200 = 7.2 kbps. ▪ **[3]** 9600 = 9.6 kbps. ▪ **[4]** 12000 = 12.0 kbps. ▪ **[5]** 14400 = 14.4 kbps (default). **Note:** The rate is negotiated between the sides (i.e., the device adapts to the capabilities of the remote side).
Fax/Modem Bypass Coder Type **[FaxModemBypassCoderType]**	Coder used by the device when performing fax/modem bypass. Usually, high-bit-rate coders such as G.711 should be used. ▪ **[0]** G.711Alaw= G.711 A-law 64 (default). ▪ **[1]** G.711Mulaw = G.711 µ-law.
Fax/Modem Bypass Packing Factor **[FaxModemBypassM]**	Number of (20 msec) coder payloads that are used to generate a fax/modem bypass packet. The valid range is 1, 2, or 3 coder payloads. The default value is 1 coder payload.
Fax Bypass Output Gain **[FaxBypassOutputGain]**	Defines the fax bypass output gain control. The range is -31 to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).
Modem Bypass Output Gain **[ModemBypassOutputGain]**	Defines the modem bypass output gain control. The range is -31 dB to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).

Parameter	Description
Fax CNG Mode **[FaxCNGMode]**	Determines the device's behavior upon detection of a CNG tone. - **[0]** = Does not send a SIP Re-INVITE upon detection of a fax CNG tone when CNGDetectorMode is set to 1 (default). - **[1]** = Sends a SIP Re-INVITE upon detection of a fax CNG tone when CNGDetectorMode is set to 1.
CNG Detector Mode **[CNGDetectorMode]**	Determines whether the device detects the fax Calling tone (CNG). - **[0]** Disable = The originating device doesn't detect CNG; the CNG signal passes transparently to the remote side (default). - **[1]** Relay = CNG is detected on the originating side. CNG packets are sent to the remote side according to T.38 (if IsFaxUsed = 1) and the fax session is started. A Re-INVITE message isn't sent and the fax session starts by the terminating device. This option is useful, for example, when the originating device is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network (i.e., originating device). To also send a SIP Re-INVITE message upon detection of a fax CNG tone in this mode, set the parameter FaxCNGMode to 1. - **[2]** Events Only = CNG is detected on the originating side and a fax session is started by the originating side using the Re-INVITE message. Usually, T.38 fax session starts when the 'preamble' signal is detected by the answering side. Some SIP devices don't support the detection of this fax signal on the answering side and thus, in these cases it is possible to configure the device to start the T.38 fax session when the CNG tone is detected by the originating side. However, this mode is not recommended.
T.38 Max Datagram Size **[T38MaxDatagram]**	Defines the maximum size of a T.38 datagram that the device can receive. This value is included in the outgoing SDP when T.38 is in use. The valid range is 122 to 1,024. The default value is 122.

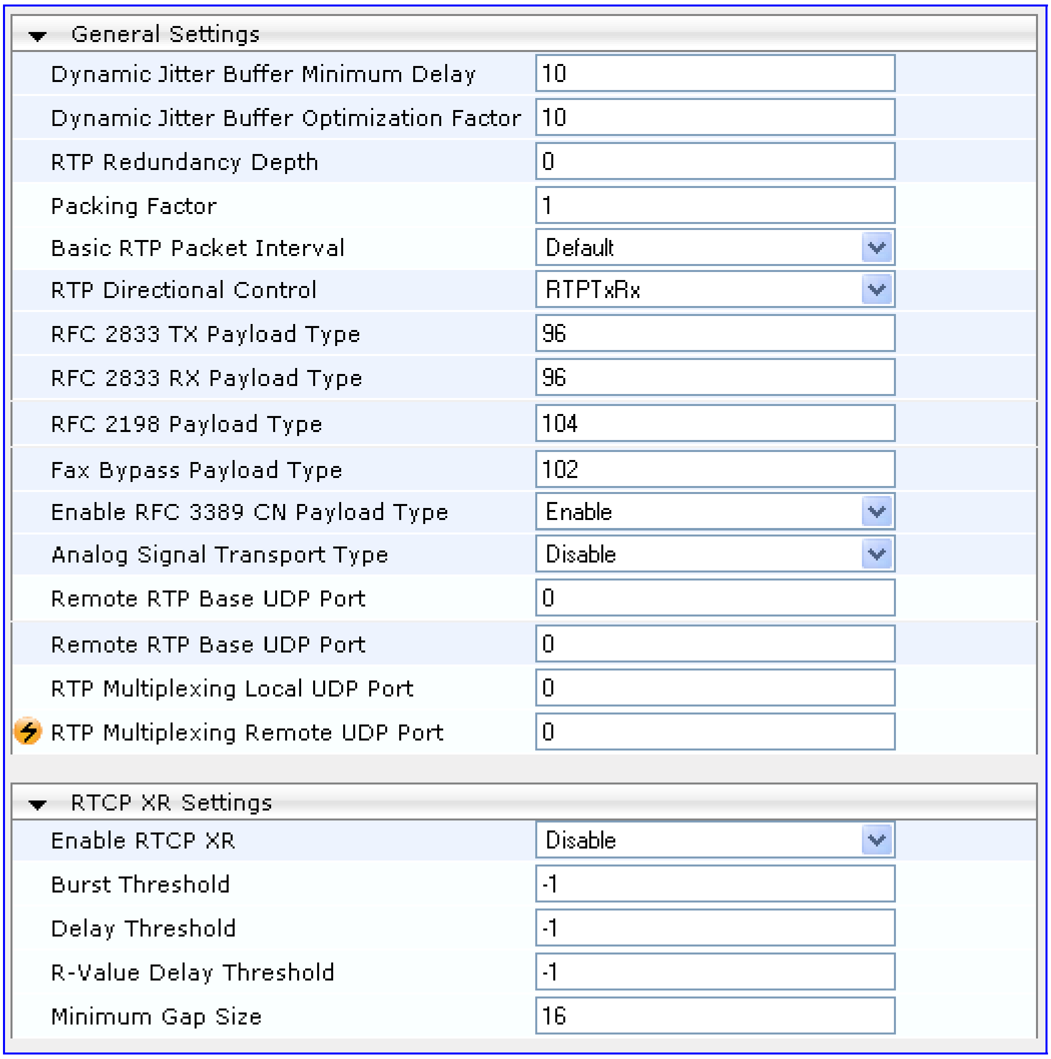
3.4.2.3 Configuring the RTP / RTCP Settings

The 'RTP/RTCP Settings' page allows you to configure the Real-Time Transport Protocol (RTP) and Real-Time Transport (RTP) Control Protocol (RTCP) parameters.

➢ To configure the RTP / RTCP parameters, take these 4 steps:

1. Open the 'RTP/RTCP Settings' page (**Configuration** tab > **Media Settings** menu > **RTP / RTCP Settings** page item).

Figure 3-42: RTP / RTCP Settings Page



▼ General Settings

Dynamic Jitter Buffer Minimum Delay	10
Dynamic Jitter Buffer Optimization Factor	10
RTP Redundancy Depth	0
Packing Factor	1
Basic RTP Packet Interval	Default
RTP Directional Control	RTPTxRx
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
Fax Bypass Payload Type	102
Enable RFC 3389 CN Payload Type	Enable
Analog Signal Transport Type	Disable
Remote RTP Base UDP Port	0
Remote RTP Base UDP Port	0
RTP Multiplexing Local UDP Port	0
⚡ RTP Multiplexing Remote UDP Port	0

▼ RTCP XR Settings

Enable RTCP XR	Disable
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
Minimum Gap Size	16

2. Configure the RTP / RTCP parameters according to the table below.

3. Click the **Submit** button to save your changes.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-15: Media Settings, RTP / RTCP Parameters

Parameter	Description
Dynamic Jitter Buffer Minimum Delay **[DJBufMinDelay]**	Minimum delay (in msec) for the Dynamic Jitter Buffer. The valid range is 0 to 150. The default delay is 10. **Note:** For more information on Jitter Buffer, refer to "Dynamic Jitter Buffer Operation" on page 360.
Dynamic Jitter Buffer Optimization Factor **[DJBufOptFactor]**	Dynamic Jitter Buffer frame error / delay optimization factor. The valid range is 0 to 13. The default factor is 10. **Notes:** ▪ Set to 13 for data (fax and modem) calls. ▪ For more information on Jitter Buffer, refer to "Dynamic Jitter Buffer Operation" on page 360.
RTP Redundancy Depth **[RTPRedundancyDepth]**	Determines whether the device generates redundant packets. ▪ **[0]** 0 = Disable the generation of redundant packets (default). ▪ **[1]** 1 = Enable the generation of RFC 2198 redundancy packets.
Packing Factor **[RTPPackingFactor]**	N/A. Controlled internally by the device according to the selected coder.
Basic RTP Packet Interval **[BasicRTPPacketInterval]**	N/A. Controlled internally by the device according to the selected coder.
RTP Directional Control **[RTPDirectionControl]**	N/A. Controlled internally by the device according to the selected coder.
RFC 2833 TX Payload Type **[RFC2833TxPayloadType]**	N/A. Use the *ini* file parameter RFC2833PayloadType instead.
RFC 2833 RX Payload Type **[RFC2833RxPayloadType]**	N/A. Use the *ini* file parameter RFC2833PayloadType instead.
RFC 2198 Payload Type **[RFC2198PayloadType]**	RTP redundancy packet payload type, according to RFC 2198. The range is 96-127. The default is 104. **Note:** This parameter is applicable only if RTP Redundancy Depth = 1.
Fax Bypass Payload Type **[FaxBypassPayloadType]**	Determines the fax bypass RTP dynamic payload type. The valid range is 96 to 120. The default value is 102.
Enable RFC 3389 CN Payload Type **[EnableStandardSIDPayloadType]**	Determines whether Silence Indicator (SID) packets are sent according to RFC 3389. ▪ **[0]** Disable = G.711 SID packets are sent in a proprietary method (default). ▪ **[1]** Enable = SID (comfort noise) packets are sent with the RTP SID payload type according to RFC 3389. Applicable to G.711 and G.726 coders.
Comfort Noise Generation Negotiation **[ComfortNoiseNegotiation]**	Enables negotiation and usage of Comfort Noise (CN). ▪ **[0]** Disable = Disable (default). ▪ **[1]** Enable = Enable. The use of CN is indicated by including a payload type for CN

Parameter	Description
	on the media description line of the SDP. The device can use CN with a codec whose RTP timestamp clock rate is 8,000 Hz (G.711/G.726). The static payload type 13 is used. The use of CN is negotiated between sides. Therefore, if the remote side doesn't support CN, it is not used. **Note:** Silence Suppression must be enabled to generate CN.
RTP Base UDP Port **[BaseUDPPort]**	Lower boundary of UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). The upper boundary is the Base UDP Port + 10 * (number of device's channels). The range of possible UDP ports is 6,000 to 64,000. The default base UDP port is 6000. For example: If the Base UDP Port is set to 6000 (default) then: 1) The first channel uses the following ports RTP 6000, RTCP 6001, and T.38 6002, 2) the second channel uses RTP 6010, RTCP 6011, and T.38 6012, etc. **Note:** If RTP Base UDP Port is not a factor of 10, the following message is generated: 'invalid local RTP port'. For detailed information on the default RTP/RTCP/T.38 port allocation, refer to the *Product Reference Manual*.
Remote RTP Base UDP Port **[RemoteBaseUDPPort]**	Determines the lower boundary of UDP ports used for RTP, RTCP and T.38 by a remote device. If this parameter is set to a non-zero value, ThroughPacket™ (RTP multiplexing) is enabled. The device uses this parameter (and BaseUDPPort) to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels. The valid range is the range of possible UDP ports: 6,000 to 64,000. The default value is 0 (i.e., RTP multiplexing is disabled). For detailed information on RTP multiplexing, refer to RTP Multiplexing (ThroughPacket) on page 360. **Notes:** ▪ The value of this parameter on the local device must equal the value of BaseUDPPort on the remote device. ▪ To enable RTP multiplexing, the parameters L1L1ComplexTxUDPPort and L1L1ComplexRxUDPPort must be set to a non-zero value. ▪ When VLANs are implemented, RTP multiplexing is not supported.
RTP Multiplexing Local UDP Port **[L1L1ComplexTxUDPPort]**	Determines the local UDP port used for outgoing multiplexed RTP packets (applies to RTP multiplexing). The valid range is the range of possible UDP ports: 6,000 to 64,000. The default value is 0 (i.e., RTP multiplexing is disabled). This parameter cannot be changed on-the-fly and requires a device reset.
RTP Multiplexing Remote UDP Port **[L1L1ComplexRxUDPPort]**	Determines the remote UDP port to where the multiplexed RTP packets are sent, and the local UDP port used for incoming multiplexed RTP packets (applies to RTP multiplexing). The valid range is the range of possible UDP ports: 6,000 to 64,000. The default value is 0 (i.e., RTP multiplexing is disabled).

Parameter	Description
	This parameter cannot be changed on-the-fly and requires a device reset. **Note:** All devices that participate in the same RTP multiplexing session must use this same port.
RTCP XR Settings (**Note:** For a detailed description of RTCP XR reports, refer to the *Product Reference Manual*.)	
Enable RTCP XR **[VQMonEnable]**	Enables voice quality monitoring and RTCP Extended Reports (RTCP XR). ▪ **[0]** Disable = Disable (default) ▪ **[1]** Enable = Enables
Burst Threshold **[VQMonBurstHR]**	Voice quality monitoring - excessive burst alert threshold. if set to -1 (default), no alerts are issued.
Delay Threshold **[VQMonDelayTHR]**	Voice quality monitoring - excessive delay alert threshold. if set to -1 (default), no alerts are issued.
R-Value Delay Threshold **[VQMonEOCRValTHR]**	Voice quality monitoring - end of call low quality alert threshold. if set to -1 (default), no alerts are issued.
Minimum Gap Size **[VQMonGMin]**	Voice quality monitoring - minimum gap size (number of frames). The default is 16.
RTCP XR Report Mode **[RTCPXRReportMode]**	Determines whether RTCP XR reports are sent to the Event State Compositor (ESC), and if so, defines the interval in which they are sent. ▪ **[0]** Disable = RTCP XR reports are not sent to the ESC (default). ▪ **[1]** End Call = RTCP XR reports are sent to the ESC at the end of each call. ▪ **[2]** End Call & Periodic = RTCP XR reports are sent to the ESC at the end of each call and periodically according to the parameter RTCPInterval.
RTCP XR Packet Interval **[RTCPInterval]**	Defines the time interval (in msec) between adjacent RTCP reports. The interval range is 0 to 65,535. The default interval is 5,000.
Disable RTCP XR Interval Randomization **[DisableRTCPRandomize]**	Controls whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval. ▪ **[0]** Disable = Randomize (default) ▪ **[1]** Enable = No Randomize
RTCP XR Collection Server **[RTCPXREscIP]**	IP address of the Event State Compositor (ESC). The device sends RTCP XR reports to this server, using PUBLISH messages. The address can be configured as a numerical IP address or as a domain name.

3.4.2.4 Configuring the IPmedia Settings

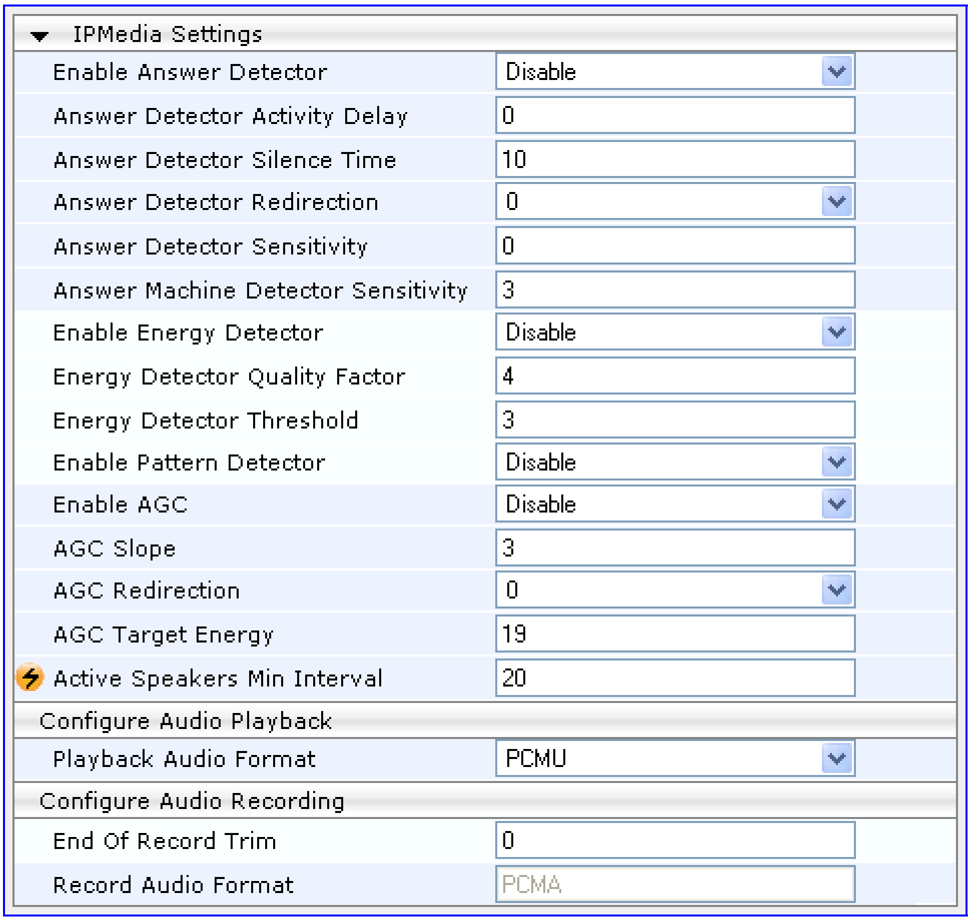
The 'IPMedia Settings' page allows you to configure the IP media parameters. This includes Automatic Gain Control (AGC) parameters. AGC equalizes the energy of the output signal to a required level. It estimates the energy of the incoming signal, calculates the essential gain and performs amplification. Feedback ensures that the output signal is not clipped. You can define the required Gain Slope in decibels/sec and the required energy threshold.

When the AGC first detects a signal in the input, it begins operating in Fast Mode. This means that the Gain Slope is 8 dB/sec for the first 1.5 seconds. After this period, the Gain Slope is changed to the user-defined value. You can disable or enable the feature by using the *ini* file parameter AGCDisableFastAdaptation. After Fast Mode is used, the signal should be off for two minutes in order to have the feature turned on again. (This feature is designed so that AGC can fast-adapt when a conversation is started).

➢ To configure the IP media parameters, take these 4 steps:

1. Open the 'IPMedia Settings' page (**Configuration** tab > **Media Settings** menu > **IPmedia Settings** page item).

Figure 3-43: IPMedia Settings Page



▼ IPMedia Settings

Enable Answer Detector	Disable
Answer Detector Activity Delay	0
Answer Detector Silence Time	10
Answer Detector Redirection	0
Answer Detector Sensitivity	0
Answer Machine Detector Sensitivity	3
Enable Energy Detector	Disable
Energy Detector Quality Factor	4
Energy Detector Threshold	3
Enable Pattern Detector	Disable
Enable AGC	Disable
AGC Slope	3
AGC Redirection	0
AGC Target Energy	19
⚡ Active Speakers Min Interval	20

Configure Audio Playback

Playback Audio Format	PCMU

Configure Audio Recording

End Of Record Trim	0
Record Audio Format	PCMA

2. Configure the IP media parameters according to the table below.

3. Click the **Submit** button to save your changes.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-16: IPMedia Parameters

Parameter	Description
Enable Answer Detector **[EnableAnswerDetector]**	N/A.
Answer Detector Activity Delay **[AnswerDetectorActivityDelay]**	N/A.
Answer Detector Silence Time **[AnswerDetectorSilenceTime]**	N/A.
Answer Detector Redirection **[AnswerDetectorRedirection]**	N/A.
Answer Detector Sensitivity **[AnswerDetectorSensitivity]**	Determines the Answer Detector sensitivity. The range is 0 (most sensitive) to 2 (least sensitive). The default is 0.
Answer Machine Detector Sensitivity **[AMDDetectionSensitivity]**	Determines the Answer Machine Detector (AMD) detection sensitivity. AMD can be useful in automatic dialing applications. In some of these applications, it is important to detect if a human voice or an answering machine is answering the call. AMD can be activated and de-activated only after a channel is already open. The direction of the detection (PSTN or IP) can also be configured. The range is 0 to 7, where 0 is the best detection of an answering machine and 7 is the best detection of a live call (i.e., voice detected). The default is 3. For a detailed description on AMD, refer to Answer Machine Detector (AMD) on page 343. **Note:** To enable the AMD feature, set the ini file parameter EnableDSPIPMDetectors to 1.
Enable AGC **[EnableAGC]**	Activates the Automatic Gain Control (AGC) mechanism. The AGC mechanism adjusts the level of the received signal to maintain a steady (configurable) volume level. ▪ **[0]** Disable (default). ▪ **[1]** Enable. **Note:** For a description on AGC, refer to "Automatic Gain Control (AGC)" on page 401.
AGC Slope **[AGCGainSlope]**	Determines the AGC convergence rate: ▪ 0 = 0.25 dB/sec ▪ 1 = 0.50 dB/sec ▪ 2 = 0.75 dB/sec ▪ 3 = 1.00 dB/sec (default) ▪ 4 = 1.25 dB/sec ▪ 5 = 1.50 dB/sec ▪ 6 = 1.75 dB/sec ▪ 7 = 2.00 dB/sec ▪ 8 = 2.50 dB/sec ▪ 9 = 3.00 dB/sec ▪ 10 = 3.50 dB/sec

Parameter	Description
	▪ 11 = 4.00 dB/sec ▪ 12 = 4.50 dB/sec ▪ 13 = 5.00 dB/sec ▪ 14= 5.50 dB/sec ▪ 15 = 6.00 dB/sec ▪ 16 = 7.00 dB/sec ▪ 17 = 8.00 dB/sec ▪ 18 = 9.00 dB/sec ▪ 19 = 10.00 dB/sec ▪ 20 = 11.00 dB/sec ▪ 21 = 12.00 dB/sec ▪ 22 = 13.00 dB/sec ▪ 23 = 14.00 dB/sec ▪ 24 = 15.00 dB/sec ▪ 25 = 20.00 dB/sec ▪ 26 = 25.00 dB/sec ▪ 27 = 30.00 dB/sec ▪ 28 = 35.00 dB/sec ▪ 29 = 40.00 dB/sec ▪ 30 = 50.00 dB/sec ▪ 31 = 70.00 dB/sec
AGC Redirection **[AGCRedirection]**	Determines the AGC direction. ▪ **[0]** 0 = AGC works on signals from the TDM side (default). ▪ **[1]** 1 = AGC works on signals from the IP side.
AGC Target Energy **[AGCTargetEnergy]**	Determines the signal energy value (dBm) that the AGC attempts to attain. The valid range is 0 to -63 dBm. The default value is -19 dBm.
Enable Energy Detector **[EnableEnergyDetector]**	N/A
Energy Detector Quality Factor **[EnergyDetectorQualityFactor]**	N/A
Energy Detector Threshold **[EnergyDetectorThreshold]**	N/A
Enable Pattern Detector **[EnablePatternDetector]**	Enables or disables the activation of the Pattern Detector (PD). Valid options include: ▪ **[0]** Disable = Disable (default) ▪ **[1]** Enable = Enable

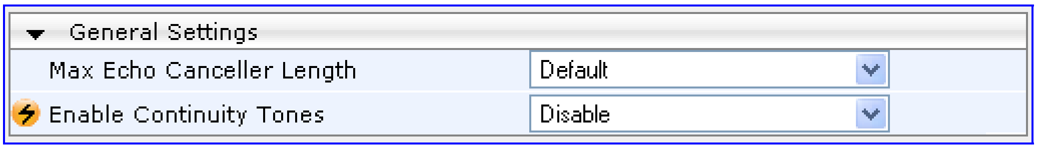
3.4.2.5 Configuring the General Media Settings

The 'General Media Settings' page allows you to configure various media parameters.

➢ **To configure general media parameters, take these 4 steps:**

1. Open the 'General Media Settings' page (**Configuration** tab > **Media Settings** menu > **General Media Settings** page item).

Figure 3-44: General Media Settings Page



▼ General Settings

Max Echo Canceller Length	Default
Enable Continuity Tones	Disable

2. Configure the general media parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-17: Media Settings Parameters

Parameter	Description
Max Echo Canceller Length **[MaxEchoCancellerLength]**	Determines the maximum Echo Canceler Length (in msec), which is the maximum echo path delay (tail length) for which the echo canceller is designed to operate: ▪ **[0]** Default = based on various internal device settings to attain maximum channel capacity (default) ▪ **[11]** 64 msec ▪ **[22]** 128 msec **Notes:** ▪ Using 128 msec reduces the channel capacity to 200 channels. ▪ Reset the device after modifying this parameter. ▪ It isn't necessary to configure the parameter EchoCancellerLength as it automatically acquires its value from this parameter.
Enable Continuity Tones	N/A.

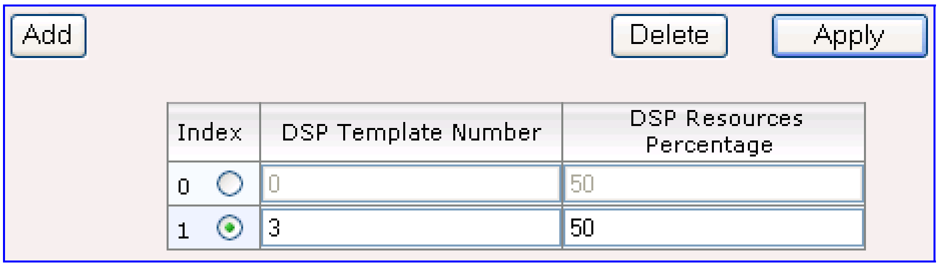
3.4.2.6 Configuring the DSP Templates

The 'DSP Templates' page allows you to assign up to two DSP templates to the device. In addition, you can define the percentage of DSP resources allocated per DSP template.

➢ To select DSP templates, take these 5 steps:

1. Open the 'DSP Templates' page (**Configuration** tab > **Media Settings** menu > **DSP Templates** page item).

Figure 3-45: DSP Templates Page



Index	DSP Template Number	DSP Resources Percentage
0 ○	0	50
1 ●	3	50

2. Select an index row by clicking the corresponding 'Index' radio button.
3. Click **Edit**, and then in the 'DSP Template Number' field, enter the desired DSP template number.
4. Click **Apply** to save your settings.
5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- If you delete all the table entries, the device uses the default DSP template.
- For a description of the Web interface's table command buttons (e.g., **Duplicate** and **Delete**), refer to "Working with Tables" on page 30.

Table 3-18: DSP Templates Parameters

Parameter	Description
DSP Template Number **[DSPVersionTemplateNumber]**	Determines the number of the DSP template load. Each load has a different coder list, channel capacity, and supported features. For the list of supported DSP template numbers (coders and channel capacity), refer to the device's *Release Notes*. The default is 0.
DSP Resources Percentage	Resource percentage used for the specified template.

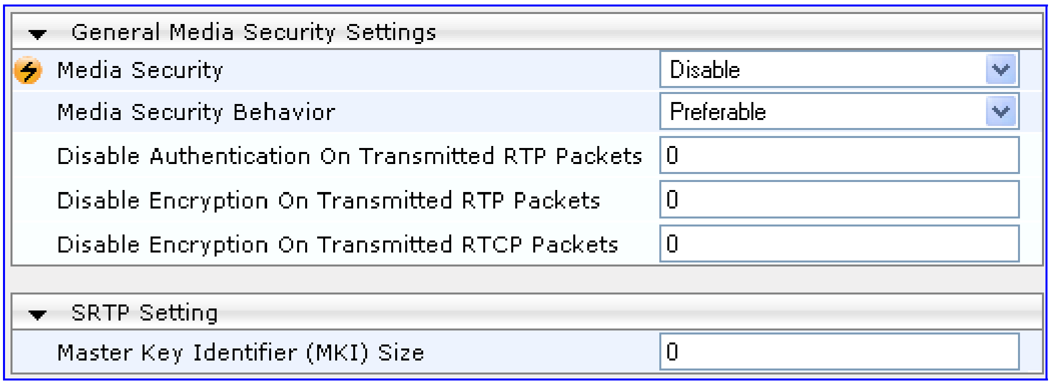
3.4.2.7 Configuring Media Security

The 'Media Security' page allows you to configure media security.

➢ To configure media security, take these 4 steps:

1. Open the 'Media Security' page (**Configuration** tab > **Media Settings** menu > **Media Security** page item).

Figure 3-46: Media Security Page



General Media Security Settings

Media Security	Disable
Media Security Behavior	Preferable
Disable Authentication On Transmitted RTP Packets	0
Disable Encryption On Transmitted RTP Packets	0
Disable Encryption On Transmitted RTCP Packets	0

SRTP Setting

Master Key Identifier (MKI) Size	0

2. Configure the media security parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-19: Media Security Parameters

Parameter	Description
Media Security **[EnableMediaSecurity]**	Enables Secure Real-Time Transport Protocol (SRTP). ▪ **[0]** Disable = SRTP is disabled (default). ▪ **[1]** Enable = SRTP is enabled.
Media Security Behavior **[MediaSecurityBehaviour]**	Determines the device's mode of operation when SRTP is used (EnableMediaSecurity = 1). ▪ **[0]** Preferable = The device initiates encrypted calls. If negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted. ▪ **[1]** Mandatory = The device initiates encrypted calls, but if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected (default).
Disable Authentication On Transmitted RTP Packets **[RTPAuthenticationDisableTx]**	On a secured RTP session, this parameter determines whether to enable Authentication on transmitted RTP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable

Parameter	Description
Disable Encryption On Transmitted RTP Packets **[RTPEncryptionDisableTx]**	On a secured RTP session, this parameter determines whether to enable Encryption on transmitted RTP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable
Disable Encryption On Transmitted RTCP Packets **[RTCPEncryptionDisableTx]**	On a secured RTP session, this parameter determines whether to enable Encryption on transmitted RTCP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable
SRTP Settings	
Master Key Identifier (MKI) Size **[SRTPTxPacketMKISize]**	Determines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets. The range is 0 to 4. The default value is 0.

3.4.3 PSTN Settings

The **PSTN Settings** menu allows you to configure various PSTN settings and includes the following page items:

- Trunk Settings (refer to "Configuring the Trunk Settings" on page 82)
- CAS State Machines (refer to "Configuring the CAS State Machines" on page 97)

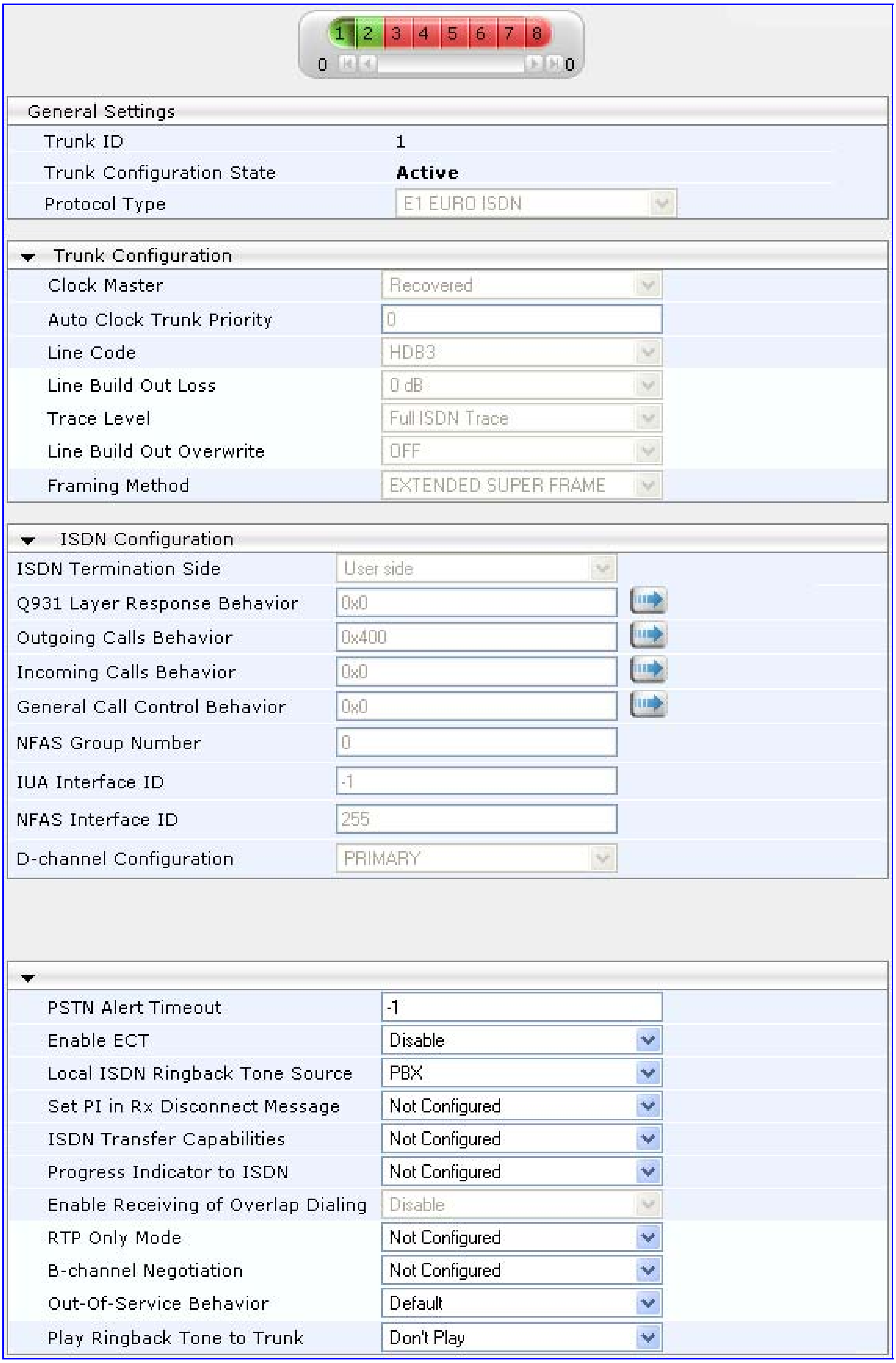
3.4.3.1 Configuring the Trunk Settings

The 'Trunk Settings' page allows you to configure the device's trunks. For configuring the trunks using the *ini* file parameters, refer to "PSTN Parameters" on page 303.

➢ To configure the Trunks, take these 7 steps:

1. Open the ‘Trunk Settings’ page (**Configuration** tab > **PSTN Settings** menu > **Trunk Settings** page item).

Figure 3-47: Trunk Settings Page



General Settings

Trunk ID	1
Trunk Configuration State	**Active**
Protocol Type	E1 EURO ISDN

Trunk Configuration

Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	HDB3
Line Build Out Loss	0 dB
Trace Level	Full ISDN Trace
Line Build Out Overwrite	OFF
Framing Method	EXTENDED SUPER FRAME

ISDN Configuration

ISDN Termination Side	User side
Q931 Layer Response Behavior	0x0
Outgoing Calls Behavior	0x400
Incoming Calls Behavior	0x0
General Call Control Behavior	0x0
NFAS Group Number	0
IUA Interface ID	-1
NFAS Interface ID	255
D-channel Configuration	PRIMARY

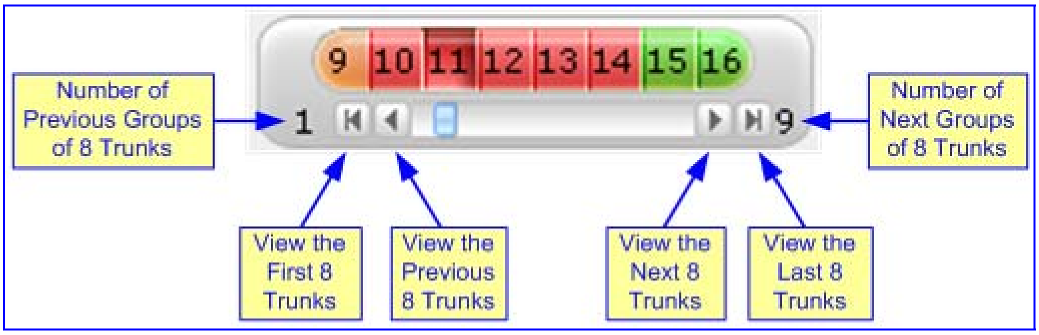
PSTN Alert Timeout	-1
Enable ECT	Disable
Local ISDN Ringback Tone Source	PBX
Set PI in Rx Disconnect Message	Not Configured
ISDN Transfer Capabilities	Not Configured
Progress Indicator to ISDN	Not Configured
Enable Receiving of Overlap Dialing	Disable
RTP Only Mode	Not Configured
B-channel Negotiation	Not Configured
Out-Of-Service Behavior	Default
Play Ringback Tone to Trunk	Don't Play

On the top of the page, a bar with Trunk number icons displays the status of each trunk, according to the following color codes:

- Grey: Disabled
- Green: Active
- Yellow: RAI alarm
- Red: LOS / LOF alarm
- Blue: AIS alarm
- Orange: D-channel alarm (ISDN only)

2. Select the trunk that you want to configure, by clicking the desired Trunk number icon. The bar initially displays the first eight trunk number icons (i.e., trunks 1 through 8). To scroll through the trunk number icons (i.e., view the next/last or previous/first group of eight trunks), refer to the figure below:

Figure 3-48: Trunk Scroll Bar


9
10
11
12
13
14
15
16
1
9
Number of Previous Groups of 8 Trunks
Number of Next Groups of 8 Trunks
View the First 8 Trunks
View the Previous 8 Trunks
View the Next 8 Trunks
View the Last 8 Trunks

Note: If the Trunk scroll bar displays all the available trunks, the scroll bar buttons are unavailable.

After you have selected a trunk, the following is displayed:

- The read-only 'Trunk ID' field displays the selected trunk number.
- The read-only ‘Trunk Configuration State’ displays the state of the trunk (e.g., 'Active' or 'Inactive').
- The parameters displayed in the page pertain to the selected trunk only.

1. Click the **Stop Trunk** ■ button (located at the bottom of the page) to de-activate the trunk so that you can configure currently grayed out (unavailable) parameters.(Skip this step if you want to configure parameters that are also available when the trunk is active). The stopped trunk is indicated by the following:
   - The ‘Trunk Configuration State’ field displays ‘Inactive’.
   - The **Stop Trunk** button is replaced by the **Apply Trunk Settings** ✓ button.

     (When all trunks are stopped, the **Apply to All Trunks** ✓ button also appears.)
   - All the parameters are available and can be modified.
2. Configure the desired trunk parameters, as described in the table below.

3. Click the **Apply Trunk Settings** button to apply the changes to the selected trunk (or click **Apply to All Trunks** to apply the changes to all trunks); the **Stop Trunk** button replaces **Apply Trunk Settings** and the 'Trunk Configuration State' displays 'Active'.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.
5. To reset the device, refer to "Resetting the Device" on page 228.

Notes:

- If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the device.
- The displayed parameters on the page depend on the protocol selected in the 'Protocol Type' field.
- All trunks must be of the same line type (i.e., either E1 or T1). However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the device's Release Notes).
- If the trunk protocol type is CAS, you can assign or modify a dial plan (in the 'Dial Plan' field) and perform this without stopping the trunk.
- If the trunk can't be stopped because it provides the device's clock (assuming the device is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the device's clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' page (refer to "Configuring the TDM Bus Settings" on page 218).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to 'None'.

Table 3-20: Trunk (E1/T1/J1) Configuration Parameters

***ini* File Field Name** **Web Parameter Name**	**Valid Range and Description**
General Settings	
Protocol Type **[ProtocolType]**	Defines the PSTN protocol for the trunk: ▪ **[0]** = NONE ▪ **[1]** E1 EURO ISDN ▪ **[2]** T1 CAS ▪ **[3]** T1 RAW CAS ▪ **[4]** T1 TRANSPARENT ▪ **[5]** E1 TRANSPARENT 31 ▪ **[6]** E1 TRANSPARENT 30 ▪ **[7]** E1 MFCR2 ▪ **[8]** E1 CAS ▪ **[9]** E1 RAW CAS ▪ **[10]** T1 NI2 ISDN ▪ **[11]** T1 4ESS ISDN ▪ **[12]** T1 5ESS 9 ISDN

ini File Field Name Web Parameter Name	Valid Range and Description
	▪ **[13]** T1 5ESS 10 ISDN ▪ **[14]** T1 DMS100 ISDN ▪ **[15]** J1 TRANSPARENT ▪ **[16]** T1 NTT ISDN = Japan - Nippon Telegraph ▪ **[17]** E1 AUSTEL ISDN = Australian Telecom ▪ **[18]** T1 HKT ISDN = Hong Kong - HKT ▪ **[19]** E1 KOR ISDN = Korean operator ▪ **[20]** T1 HKT ISDN = Hong Kong - HKT over T1 ▪ **[21]** E1 QSIG ▪ **[23]** T1 QSIG ▪ **[30]** E1 FRENCH VN6 ISDN ▪ **[31]** E1 FRENCH VN3 ISDN ▪ **[35]** T1 DMS100 Meridian ISDN ▪ **[40]** E1 NI2 ISDN ▪ **[41]** E1 CAS R15 **Note:** The device simultaneously supports different variants of CAS and PRI protocols on different E1/T1 spans (no more than four simultaneous PRI variants). The device simultaneously supports different BRI variants
Trunk Configuration	
Clock Master **[ClockMaster]**	Determines the Tx clock source of the E1/T1 line. ▪ **[0]** Recovered = Generate the clock according to the Rx of the E1/T1 line (default). ▪ **[1]** Generated = Generate the clock according to the internal TDM bus. **Notes:** ▪ The source of the internal TDM bus clock is determined by the parameter TDMBusClockSource. ▪ For detailed information on configuring the device's clock settings, refer to "Clock Settings" on page 393.
Auto Clock Trunk Priority **[AutoClockTrunkPriority]**	Defines the trunk priority for auto-clock fallback (per trunk parameter). ▪ 0 to 99 = priority (0 is the highest = default). ▪ 100 = the SW never performs a fallback to that trunk (usually used to mark untrusted source of clock). **Note:** Fallback is enabled when the TDMBusPSTNAutoClockEnable parameter is set to 1.
Line Code **[LineCode]**	Use to select B8ZS or AMI for T1 spans, and HDB3 or AMI for E1 spans. ▪ **[0]** B8ZS = use B8ZS line code (for T1 trunks only) default. ▪ **[1]** AMI = use AMI line code. ▪ **[2]** HDB3 = use HDB3 line code (for E1 trunks only).
Line Build Out Loss	Defines the line build out loss for the selected T1 trunk.

ini File Field Name Web Parameter Name	Valid Range and Description
[LineBuildOut.Loss]	▪ **[0]** 0 dB (default) ▪ **[1]** -7.5 dB ▪ **[2]** -15 dB ▪ **[3]** -22.5 dB **Note:** This parameter is not applicable for PRI E1 trunks.
Trace Level **[TraceLevel]**	Defines the trace level: ▪ **[0]** No Trace (default) ▪ **[1]** Full ISDN Trace ▪ **[2]** Layer 3 ISDN Trace ▪ **[3]** Only ISDN Q.931 Messages Trace ▪ **[4]** Layer 3 ISDN No Duplication Trace
Framing Method **[FramingMethod]**	Determines the physical framing method for the trunk. ▪ **[0]** = default according to protocol type E1 or T1. E1 default is E1 CRC4 MultiFrame Format extended G.706B (as c); T1 default is T1 Extended SuperFrame with CRC6 (as D). ▪ **[1]** = T1 SuperFrame Format (as B). ▪ **[a]** = E1 DoubleFrame Format ▪ **[b]** = E1 CRC4 MultiFrame Format ▪ **[c]** = E1 CRC4 MultiFrame Format extended G.706B ▪ **[A]** = T1 4-Frame multiframe. ▪ **[B]** = T1 12-Frame multiframe (D4). ▪ **[C]** = T1 Extended SuperFrame without CRC6 ▪ **[D]** = T1 Extended SuperFrame with CRC6 ▪ **[E]** = T1 72-Frame multiframe (SLC96) ▪ **[F]** = J1 Extended SuperFrame with CRC6 (Japan)
ISDN Configuration Parameters	
ISDN Termination Side **[TerminationSide]**	Selects the ISDN termination side. Applicable only to ISDN protocols. ▪ **[0]** User side = ISDN User Termination Equipment (TE) side (default) ▪ **[1]** Network side = ISDN Network Termination (NT) side **Note:** Select 'User side' when the PSTN or PBX side is configured as 'Network side' and vice versa. If you don't know the device's ISDN termination side, choose 'User side'. If the D-channel alarm is indicated, choose 'Network Side'.
NFAS Group Number **[NFASGroupNumber_x]**	Indicates the NFAS group number (NFAS member) for the selected trunk. 'x' identifies the Trunk ID. ▪ 0 = Non NFAS trunk (default) ▪ 1 to 9 = NFAS group number Trunks that belong to the same NFAS group have the same number. With ISDN Non-Facility Associated Signaling you can use single D-

ini File Field Name Web Parameter Name	Valid Range and Description
	channel to control multiple PRI interfaces. **Notes:** ▪ This parameter is applicable only to T1 ISDN protocols. ▪ For a detailed description on NFAS, refer to "ISDN Non-Facility Associated Signaling (NFAS)" on page 398.
NFAS Interface ID **[ISDNNFASInterfaceID_x]**	Defines a different Interface ID for each T1 trunk. The valid range is 0 to 100. The default interface ID equals to the trunk's ID. 'x' identifies the trunk ID. **Notes:** ▪ To set the NFAS interface ID, configure ISDNIBehavior_x to include '512' feature per T1 trunk. ▪ For a detailed description on NFAS, refer to "ISDN Non-Facility Associated Signaling (NFAS)" on page 398.
D-channel Configuration **[DChConfig_x]**	Defines primary, backup (optional), and B-channels only. The *ini* file parameter *x* represents the Trunk ID. ▪ **[0]** PRIMARY= Primary Trunk (default) - contains a D-channel that is used for signaling. ▪ **[1]** BACKUP = Backup Trunk - contains a backup D-channel that is used if the primary D-channel fails. ▪ **[2]** NFAS = NFAS Trunk - contains only 24 B-channels, without a signaling D-channel. **Note:** This parameter is applicable only to T1 ISDN protocols.
Enable Receiving of Overlap Dialing **[ISDNRxOverlap_x]**	Enables Rx ISDN overlap per trunk ID. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enabled. **Notes:** ▪ If enabled, the device receives ISDN called number that is sent in the 'Overlap' mode. ▪ The SETUP message to IP is sent only after the number (including the Sending Complete IE) is fully received (via SETUP and/or subsequent INFO Q.931 messages). ▪ The MaxDigits parameter can be used to limit the length of the collected number for device ISDN overlap dialing (if sending complete is not received). ▪ If a digit map pattern is defined (DigitMapping), the device collects digits until a match is found (e.g., for closed numbering schemes) or until a timer expires (e.g., for open numbering schemes). If a match is found (or the timer expires), the digit collection process is terminated even if Sending Complete wasn't received.
Local ISDN Ringback Tone Source **[LocalISDNRBSource_ID]**	Determines whether Ringback tone is played to the ISDN by the PBX / PSTN or by the device. ▪ **[0]** PBX = PBX / PSTN (default). ▪ **[1]** Gateway. This parameter is applicable to ISDN protocols. It is used

ini File Field Name Web Parameter Name	Valid Range and Description
	simultaneously with the parameter PlayRBTone2Trunk. The *ID* in the *ini* file parameter depicts the trunk number, where 0 is the first trunk.
Progress Indicator to ISDN **[ProgressIndicator2ISDN_ID]**	Progress Indicator (PI) to ISDN. The *ID* in the *ini* file parameter depicts the trunk number, where 0 is the first trunk. ▪ **[-1]** Not Configured = The PI in ISDN messages is set according to the parameter PlayRBTone2Tel (default). ▪ **[0]** No PI = PI is not sent to ISDN. ▪ **[1]** PI = 1; **[8]** PI = 8: The PI value is sent to PSTN in Q.931/Proceeding and Alerting messages. Typically, the PSTN/PBX cuts through the audio channel without playing local Ringback tone, enabling the originating party to hear remote Call Progress Tones or network announcements.
Set PI in Rx Disconnect Message **[PIForDisconnectMsg_ID]**	Defines the device's behavior when a Disconnect message is received from the ISDN before a Connect message is received. The *ID* in the *ini* file parameter depicts the trunk number, where 0 is the first trunk. ▪ **[-1]** Not Configured = Sends a 183 SIP response according to the received progress indicator (PI) in the ISDN Disconnect message. If PI = 1 or 8, the device sends a 183 response, enabling the PSTN to play a voice announcement to the IP side. If there isn't a PI in the Disconnect message, the call is released (default). ▪ **[0]** No PI = Doesn't send a 183 response to IP. The call is released. ▪ **[1]** PI = 1; **[8]** PI = 8: Sends a 183 response to IP.
ISDN Transfer Capabilities **[ISDNTransferCapability_ID]**	Defines the IP-to-ISDN Transfer Capability of the Bearer Capability IE in ISDN SETUP messages. The *ID* in the *ini* file parameter depicts the trunk number. ▪ **[-1]** Not Configured ▪ **[0]** Audio 3.1 = Audio (default). ▪ **[1]** Speech = Speech. ▪ **[2]** Data = Data. ▪ Audio 7 = Currently not supported. **Note:** If this parameter isn't configured or equals to '-1', Audio 3.1 capability is used.
ISDN Flexible Behavior Parameters ISDN protocol is implemented in different Switches / PBXs by different vendors. Several implementations vary a little from the specification. Therefore, to provide a flexible interface that supports these ISDN variants, the ISDN behavior parameters are used. To configure the different behavior bits in the Web interface, you can either enter the exact hexadecimal bits value in the field to the right of the relevant parameter, or directly configure each bit field by completing the following steps: 1. Click the arrow ➡ button to the right of the relevant parameter; the relevant behavior page appears. 2. Modify each bit field according to your requirements. 3. Click the **Submit** button to save your changes.	
Q.931 Layer Response Behavior	Bit-field used to determine several behavior options that influence the behaviour of the Q.931 protocol. To select the options, click the arrow

ini File Field Name Web Parameter Name	Valid Range and Description
[ISDNIBehavior]	button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable). ▪ **[1]** NO STATUS ON UNKNOWN IE = Q.931 Status message isn't sent if Q.931 received message contains an unknown/unrecognized IE(s). By default, the Status message is sent. **Note:** Applicable only to PRI variants in which sending of Status message is optional. ▪ **[2]** NO STATUS ON INV OP IE = Q.931 Status message isn't sent if an optional IE with invalid content is received. By default, the Status message is sent. **Note:** Applicable only to PRI variants in which sending of Status message is optional. ▪ **[4]** ACCEPT UNKNOWN FAC IE = Accepts unknown/unrecognized Facility IE. Otherwise, the Q.931 message that contains the unknown Facility IE is rejected (default). **Note:** Applicable only to PRI variants where a complete ASN1 decoding is performed on Facility IE. ▪ **[128]** SEND USER CONNECT ACK = Connect ACK message is sent in response to received Q.931 Connect. Otherwise, the Connect ACK is not sent (default). **Note:** Applicable only to Euro ISDN User side outgoing calls. ▪ **[512]** EXPLICIT INTERFACE ID = Enables to configure T1 NFAS Interface ID (refer to the parameter ISDNNFASInterfaceID_x). **Note:** Applicable to 4/5ESS, DMS, NI-2 and HKT variants. ▪ **[2048]** ALWAYS EXPLICIT = Always set the Channel Identification IE to explicit Interface ID, even if the B-channel is on the same trunk as the D-channel. **Note:** Applicable to 4/5ESS, DMS and NI-2 variants. ▪ **[32768]** ACCEPT MU LAW =Mu-Law is also accepted in ETSI. ▪ **[65536]** EXPLICIT PRES SCREENING = The calling party number (octet 3a) is always present even when presentation and screening are at their default. **Note:** Applicable only to ETSI, NI-2, and 5ESS. ▪ **[131072]** STATUS INCOMPATIBLE STATE = Clears the call on receipt of Q.931 Status with incompatible state. Otherwise, no action is taken (default). ▪ **[262144]** STATUS ERROR CAUSE = Clear call on receipt of STATUS according to cause value. ▪ **[524288]** ACCEPT A LAW =A-Law is also accepted in 5ESS. ▪ **[2097152]** RESTART INDICATION =acEV_PSTN_RESTART_CONFIRM is generated on receipt of a RESTART message. ▪ **[4194304]** FORCED RESTART = On data link (re)initialization, send RESTART if there is no call. ▪ **[1073741824]** NS QSI ENCODE INTEGER = If this bit is set, INTEGER ASN.1 type is used in operator coding (compliant to new ECMA standards); otherwise, OBJECT IDENTIFIER ASN.1 type is used. **Note:** Only applicable only to QSIG.

ini File Field Name Web Parameter Name	Valid Range and Description
	▪ **[2147483648]** NS 5ESS NATIONAL = Use the National mode of AT&T 5ESS for B-channel maintenance. **Note:** To configure the device to support several ISDNIBehavior features, add the individual feature values. For example, to support both [512] and [2048] features, set ISDNIBehavior = 2560 (i.e., 512 + 2048).
Outgoing Calls Behavior **[ISDNOutCallsBehavior]**	This parameter determines several behaviour options that influence the behaviour of the ISDN Stack outgoing calls. To select options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable). ▪ **[2]** USER SENDING COMPLETE =When this bit is set, the device doesn't automatically generate the information element Sending-Complete IE in the SETUP message. If this bit is not set, the device generates it automatically in the SETUP message only. ▪ **[16]** USE MU LAW = When set, the device sends G.711-m-Law in outgoing voice calls. When disabled, the device sends G.711-A-Law in outgoing voice calls. (Applicable only to the Korean variant.) ▪ **[128]** DIAL WITH KEYPAD = When enabled, the device uses the Keypad IE to store the called number digits instead of the CALLED_NB IE. (Only applicable to the KOR variant (Korean network). Useful for Korean switches that don't accept the CALLED_NB IE.) ▪ **[256]** STORE CHAN ID IN SETUP =When this bit is set, the device forces the sending of a Channel-Id IE in an outgoing SETUP message even if it's not required by the standard (i.e., optional), and no Channel-Id has been specified in the establishment request. This is useful for improving required compatibility with switches. On PRI lines, it indicates an unused channel ID, preferred only. ▪ **[572]** USE A LAW = When set, the device sends G.711 A-Law in outgoing voice calls. When disabled, the device sends the default G.711-Law in outgoing voice calls. Applicable to E10 variant. ▪ **[1024]** = Numbering plan / type for T1 IP-to-Tel calling numbers are defined according to the manipulation tables or according to the RPID header (default). Otherwise, the plan / type for T1 calls are set according to the length of the calling number. ▪ **[2048]** = When this bit is set, the device accepts any IA5 character in the called_nb and calling_nb strings and sends any IA5 character in the called_nb, and is not restricted to extended digits only (i.e., 0-9,*,#). ▪ **[16384]** DLCI REVERSED OPTION = Behavior bit used in the IUA interface groups to indicate that the reversed format of the DLCI field must be used. **Note:** When using the *ini* file to configure the device to support several ISDNOutCallsBehavior features, add the individual feature values. For example, to support both [2] and [16] features, set ISDNOutCallsBehavior = 18 (i.e., 2 + 16).

ini File Field Name Web Parameter Name	Valid Range and Description
Incoming Calls Behavior **[ISDNInCallsBehavior]**	This is the bit-field used to determine several behavior options that influence how the ISDN Stack INCOMING calls behave. To select the options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable). ▪ **[32]** DATA CONN RS = Sends a CONNECT (answer) message on NOT incoming Tel calls. ▪ **[64]** VOICE CONN RS = device sends a CONNECT (answer) message on incoming Tel calls. ▪ **[2048]** CHAN ID IN FIRST RS = Sends Channel ID in the first response to an incoming Q.931 Call Setup message. Otherwise, the Channel ID is sent only if the device requires changing the proposed Channel ID (default). ▪ **[8192]** CHAN ID IN CALL PROC = Sends Channel ID in a Q.931 Call Proceeding message. ▪ **[65536]** PROGR IND IN SETUP ACK = Includes Progress Indicator (PI=8) in Setup ACK message if an empty called number is received in an incoming SETUP message. Applicable to overlap dialing mode. The parameter also directs the device to play a dial tone (for TimeForDialTone), until the next called number digits are received. ▪ **[262144]** = NI-2 second redirect number. You can select and use (in INVITE messages) the NI-2 second redirect number if two redirect numbers are received in Q.931 Setup for incoming Tel-to-IP calls. **Note:** When using the *ini* file to configure the device to support several ISDNInCallsBehavior features, add the individual feature values. For example, to support both [2048] and [65536] features, set ISDNInCallsBehavior = 67584 (i.e., 2048 + 65536).
General Call Control Behavior **[ISDNGeneralCCBehavior]**	Bit-field used to determine several general CC behavior options. To select the options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable). ▪ **[2]** = data calls with interworking indication use 64 kbps B-channels (physical only). ▪ **[8]** REVERSE CHAN ALLOC ALGO = Channel ID allocation algorithm. ▪ **[16]** = The device clears down the call if it receives a NOTIFY message specifying 'User-Suspended'. A NOTIFY (User-Suspended) message is used by some networks (e.g., in Italy or Denmark) to indicate that the remote user has cleared the call, especially in the case of a long distance voice call. ▪ **[32]** CHAN ID 16 ALLOWED = Applies only to ETSI E1 lines (30B+D). Enables handling the differences between the newer QSIG standard (ETS 300-172) and other ETSI-based standards (ETS 300-102 and ETS 300-403) in the conversion of B-channel ID values into timeslot values: 1) In 'regular ETSI' standards, the timeslot is identical to the B-channel ID value, and the range for both is 1 to 15 and 17 to 31. The D-channel is identified as channel-id #16 and carried into the timeslot #16. 2) In newer QSIG standards, the channel-id range is 1 to 30, but the timeslot range is still 1 to 15 and 17 to 31. The D-channel is

ini File Field Name Web Parameter Name	Valid Range and Description
	not identified as channel-id #16, but is still carried into the timeslot #16. When this bit is set, the channel ID #16 is considered as a valid B-channel ID, but timeslot values are converted to reflect the range 1 to 15 and 17 to 31. This is the new QSIG mode of operation. When this bit is not set (default), the channel_id #16 is not allowed, as for all ETSI-like standards. ▪ **[64]** USE T1 PRI = PRI interface type is forced to T1. ▪ **[128]** USE E1 PRI = PRI interface type is forced to E1. ▪ **[256]** START WITH B CHAN OOS = B-channels start in the Out-Of-Service state (OOS). ▪ **[512]** CHAN ALLOC LOWEST = CC allocates B-channels starting from the lowest available B-channel id. ▪ **[1024]** CHAN ALLOC HIGHEST = CC allocates B-channels starting from the highest available B-channel id. **Note:** When using the *ini* file to configure the device to support several ISDNGeneralCCBehavior features, add the individual feature values. For example, to support both [16] and [32] features, set ISDNGeneralCCBehavior = 48 (i.e., 16 + 32).
CAS Configuration (These parameters only appear if the protocol Type is	

CAS Table
[CASTableIndex_x]
	Defines CAS protocol for each trunk ID from a list of CAS protocols defined by the parameter CASFileName_Y.
	For example:
	CASFileName_0 = 'E_M_WinkTable.dat'
	CASFileName_1 = 'E_M_ImmediateTable.dat'
	CASTableIndex_0 = 0
	CASTableIndex_1 = 0
	CASTableIndex_2 = 1
	CASTableIndex_3 = 1
	Trunks 0 and 1 use the E&M Winkstart CAS protocol, while trunks 2 and 3 use the E&M Immediate Start CAS protocol.
	Note: For additional CAS table *ini* file parameters (CASFileName_0, CASFileName_1, CASFileName_7, and CASTablesNum), refer to "E1/T1 Configuration Parameters" on page 303.

Dial Plan **[CasTrunkDialPlanName]**	The Dial Plan name that is used on a specific trunk. The range is up to 11 character strings.
Miscellaneous	
PSTN Alert Timeout **[TrunkPSTNAlertTimeout_ID]**	Alert Timeout (ISDN T301 timer) in seconds for outgoing calls to PSTN. This timer is used between the time that a SETUP message is sent to the Tel side (IP-to-Tel call establishment) and a CONNECT message is received. If ALERT is received, the timer is restarted. In the *ini* file parameter, *ID* depicts the trunk number, where 0 is the first trunk. The range is 1 to 600. The default is 180.
Digital Out-Of-Service Behavior **[DigitalOOSBehaviorForTrunk_ID]**	Determines the method for setting digital trunks to Out-Of-Service state per trunk. ▪ **[-1]** Not Configured = Use the settings of the DigitalOOSBehavio parameter for per device (default).

ini File Field Name Web Parameter Name	Valid Range and Description
	▪ **[0]** Default = Uses default behavior for each trunk (see note below). ▪ **[1]** Service = Sends ISDN In or Out of Service (only for ISDN protocols that support Service message). ▪ **[2]** D-Channel = Takes D-Channel down or up (ISDN only). ▪ **[3]** Alarm = Sends or cleans PSTN AIS Alarm (ISDN and CAS). ▪ **[4]** Block = Blocks trunk (CAS only). **Notes:** ▪ The default behavior (value 0) is as follows: - ISDN: Use Service messages on supporting variants and use Alarm on non-supporting variants. - CAS: Use Alarm. ▪ When updating this parameter value at run-time, you must stop the trunk and then restart it for the update to take effect. ▪ To determine the method for setting Out-Of-Service state for all trunks (i.e., per device), use the DigitalOOSBehavior parameter (refer to ''Configuring the Digital Gateway Parameters'' on page 207). ▪ The *ID* in the *ini* file parameter name represents the trunk number, where 0 is the first trunk.
Play Ringback Tone to Trunk **[PlayRBTone2Trunk_ID]**	Determines the method for playing a ringback tone (RBT) to the Trunk side. In the *ini* file parameter, *ID* depicts the Trunk number, where 0 is the first trunk. ▪ **[-1]** = Not configured - use the value of the parameter PlayRBTone2Tel. ▪ **[0]** Don't Play = The device configured with ISDN / CAS protocol type, doesn't play an RBT. No PI is sent to the ISDN unless the parameter ProgressIndicator2ISDN_ID is configured differently. ▪ **[1]** Play on Local = The device configured with CAS protocol type, plays a local RBT to PSTN upon receipt of a 180 Ringing response (with or without SDP). **Note:** Receipt of a 183 response doesn't cause the device configured with CAS to play an RBT (unless SIP183Behaviour = 1). The device configured with ISDN protocol type operates according to the parameter LocalISDNRBSource: 1) If the device receives a 180 Ringing response (with or without SDP) and LocalISDNRBSource = 1, it plays an RBT and sends an Alert with PI = 8 (unless the parameter ProgressIndicator2ISDN_ID is configured differently). 2) If LocalISDNRBSource = 0, the device doesn't play an RBT and an Alert message (without PI) is sent to the ISDN. In this case, the PBX / PSTN should play the RBT to the originating terminal by itself. **Note:** Receipt of a 183 response doesn't cause the device with ISDN protocol type to play an RBT; the device issues a Progress message (unless SIP183Behaviour = 1). If SIP183Behaviour = 1, the 183 response is treated the same way as a 180 Ringing response. ▪ **[2]** Prefer IP = Play according to 'Early Media' (default). If a 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the

ini File Field Name Web Parameter Name	Valid Range and Description
	current 180 response), the device with ISDN / CAS protocol type doesn't play the RBT; PI = 8 is sent in an ISDN Alert message (unless the parameter ProgressIndicator2ISDN_ID is configured differently). If a 180 response is received, but the 'early media' voice channel is not opened, the device with CAS protocol type plays an RBT to the PSTN. The device with ISDN protocol type operates according to the parameter LocalISDNRBSource: 1) If LocalISDNRBSource = 1, the device plays an RBT and sends an ISDN Alert with PI = 8 to the ISDN (unless the parameter ProgressIndicator2ISDN_ID is configured differently). 2) If LocalISDNRBSource = 0, the device doesn't play an RBT. No PI is sent in the ISDN Alert message (unless the parameter ProgressIndicator2ISDN_ID is configured differently). In this case, the PBX / PSTN should play an RBT tone to the originating terminal by itself. **Note:** Receipt of a 183 response results in an ISDN Progress message (unless SIP183Behaviour = 1). If SIP183Behaviour = 1 (183 is handled the same way as a 180 + SDP), the device sends an Alert message with PI = 8, without playing an RBT.
B-Channel Negotiation **[BChannelNegotiationForTrunk_ID]**	Determines the ISDN B-Channel negotiation mode. ▪ **[-1]** Not Configured = use per device configuration of BChannelNegotiation parameter (default). ▪ **[0]** Preferred = Preferred. ▪ **[1]** Exclusive = Exclusive. ▪ **[2]** Any = Any. **Notes:** ▪ Applicable to ISDN protocols. ▪ The option ‘Any’ is only applicable if TerminationSide is set to 0 (i.e., User side). ▪ The *ID* in the *ini* file parameter name represents the trunk number, where 0 is the first trunk.
RTP Only Mode **[RTPOnlyModeForTrunk_ID]**	Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a Control session. The remote IP address is determined according to the 'Tel to IP Routing' table (or 'Outbound IP Routing' table if EnableSBC is set to 1). The port is the same port as the local RTP port (configured by the parameter BaseUDPPort and the channel on which the call is received). ▪ **[-1]** Not Configured = Use the per device parameter (RTPOnlyMode) value (default). ▪ **[0]** Disable = Disabled. ▪ **[1]** Transmit & Receive = send and receive RTP packets. ▪ **[2]** Transmit Only = send RTP packets only. ▪ **[3]** Receive Only = receive RTP packets only. **Note:** The *ID* in the *ini* file parameter depicts the trunk number, where 0 is the first trunk.

ini File Field Name Web Parameter Name	Valid Range and Description
Digital Out-Of-Service Behavior **[DigitalOOSBehavior]**	Determines the method for setting digital trunks to Out-Of-Service state per device. ▪ **[0]** Default = Uses default behavior for each trunk - see note below (default) ▪ **[1]** Service = Sends ISDN In or Out of Service (only for ISDN protocols that support Service message). ▪ **[2]** D-Channel = Takes D-Channel down or up (ISDN only). ▪ **[3]** Alarm = Sends or clears PSTN AIS Alarm (ISDN and CAS). ▪ **[4]** Block = Blocks trunk (CAS only). **Notes:** ▪ The default behavior (value 0) is as follows: - ISDN: Use Service messages on supporting variants and use Alarm on non-supporting variants. - CAS: Use Alarm. ▪ When updating this parameter value at run-time, you must stop the trunk and then restart it for the update to take effect. ▪ To determine the method for setting Out-Of-Service state per trunk, use the DigitalOOSBehaviorFor Trunk_ID parameter (refer to "Trunk Settings" on page 82).
Transfer Mode **[TrunkTransferMode]**	Enables the trunk Transfer Mode. Refer to TrunkTransferMode (0, 1, or 3) in "ISDN and CAS Interworking-Related Parameters" on page 307. **Note:** This parameter is only available for Protocol Type T1 CAS.
Enable TBCT **[TrunkTransferMode]**	Enables the Two B Channel Transfer (TBCT) trunk transfer mode. Refer to TrunkTransferMode (0 and 2) in "ISDN and CAS Interworking-Related Parameters" on page 307. **Note:** This parameter is only available for Protocol Type T1 N12 ISDN.
Enable RLT **[TrunkTransferMode]**	Enables the Release Link Trunk (RLT) trunk transfer mode. Refer to TrunkTransferMode (0 and 2) in "ISDN and CAS Interworking-Related Parameters" on page 307. **Note:** This parameter is only available for Protocol Type T1 DMS100 ISDN.
Enable Single Step Transfer **[TrunkTransferMode]**	Enables the Single Step Transfer Trunk transfer mode. Refer to TrunkTransferMode (0 and 4) in "ISDN and CAS Interworking-Related Parameters" on page 307.
Enable ECT **[TrunkTransferMode]**	Enables the Explicit Call Transfer (ECT) trunk transfer mode. Refer to TrunkTransferMode (0 and 2) in "ISDN and CAS Interworking-Related Parameters" on page 307. **Note:** This parameter is only available for Protocol Type E1 EURO ISDN.

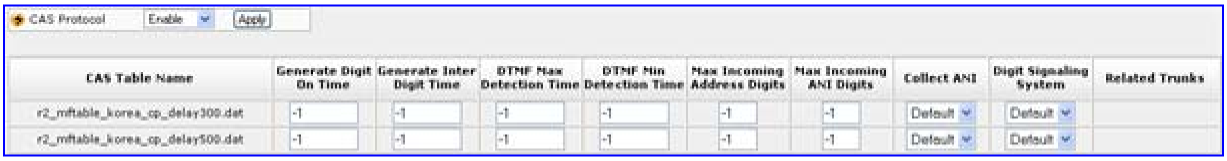
3.4.3.2 Configuring the CAS State Machines

The 'CAS State Machine' page allows you to modify various timers and other basic parameters to define the initialization of the CAS state machine without changing the state machine itself (no compilation is required). The change doesn't affect the state machine itself, but rather the configuration.

➢ To modify the CAS state machine parameters, take these 6 steps:

1. Open the ‘CAS State Machine' page (**Configuration** tab > **PSTN Settings** menu > **CAS State Machines** page item).

Figure 3-49: CAS State Machine Page



CAS Protocol: Enable

CAS Table Name	Generate Digit On Time	Generate Inter Digit Time	DTMF Max Detection Time	DTMF Min Detection Time	Max Incoming Address Digits	Max Incoming ANI Digits	Collect ANI	Digit Signaling System	Related Trunks
r2_mftable_korea_cp_delay300.dat	-1	-1	-1	-1	-1	-1	Default	Default	
r2_mftable_korea_cp_delay500.dat	-1	-1	-1	-1	-1	-1	Default	Default	

2. Ensure that the trunk is inactive. The trunk number displayed in the 'Related Trunks' field must be green. If it is red (indicating that the trunk is active), click the trunk number to open the 'Trunk Settings' page (refer to "Configuring the Trunk Settings" on page 82), select the required Trunk number icon, and then click **Stop Trunk**.

3. In the 'CAS State Machine' page, modify the required parameters according to the table below.

4. Once you have completed the configuration, activate the trunk if required in the 'Trunk Settings' page, by clicking the trunk number in the 'Related Trunks' field, and in the 'Trunk Settings' page, select the required Trunk number icon, and then click **Apply Trunk Settings**.

5. Click **Submit**.

6. Reset the device (refer to "Resetting the Device" on page 228).

Notes:

- It's strongly recommended that you don't modify the default values unless you fully understand the implications of the changes and know the default values. Every change affects the configuration of the state machine parameters and the call process related to the trunk you are using with this state machine.
- You can modify CAS state machine parameters only if the following conditions are met:
  1) Trunks are inactive (stopped), i.e., the 'Related Trunks' field displays the trunk number in green.
  2) State machine is not in use or is in reset, or when it is not related to any trunk. If it is related to a trunk, you must delete the trunk or de-activate (*Stop*) the trunk.
- Field values displaying '-1' indicate CAS default values. In other words, CAS state machine values are used.
- The modification of the CAS state machine occurs at the CAS application initialization only for non-default values (-1).
- For a detailed description of the CAS Protocol table, refer to the *Product Reference Manual*.

Table 3-21: CAS State Machine Parameters Description

Parameter	Description
Generate Digit On Time **[CasStateMachineGenerateDigitOnTime]**	Generates digit on-time (in msec). The value must be a positive value. The default value is -1.
Generate Inter Digit Time **[CasStateMachineGenerateInterDigitTime]**	Generates digit off-time (in msec). The value must be a positive value. The default value is -1.
DTMF Max Detection Time **[CasStateMachineDTMFMaxOnDetectionTime]**	Detects digit maximum on time (according to DSP detection information event) in msec units. The value must be a positive value. The default value is -1.
DTMF Min Detection Time **[CasStateMachineDTMFMinOnDetectionTime]**	Detects digit minimum on time (according to DSP detection information event) in msec units. The digit time length must be longer than this value to receive a detection. Any number may be used, but the value must be less than CasStateMachineDTMFMaxOnDetectionTime. The value must be a positive value. The default value is -1.
MAX Incoming Address Digits **[CasStateMachineMaxNumOfIncomingAddressDigits]**	Defines the limitation for the maximum address digits that need to be collected. After reaching this number of digits, the collection of address digits is stopped. The value must be an integer. The default value is -1.
MAX Incoming ANI Digits **[CasStateMachineMaxNumOfIncomingANIDigits]**	Defines the limitation for the maximum ANI digits that need to be collected. After reaching this number of digits, the collection of ANI digits is stopped. The value must be an integer. The default value is -1.
Collet ANI **[CasStateMachineCollectANI]**	In some cases, when the state machine handles the ANI collection (not related to MFCR2), you can control the state machine to collect ANI or discard ANI. ▪ **[0]** No = Don't collect ANI. ▪ **[1]** Yes = Collect ANI. ▪ **[-1]** Default = Default value.
Digit Signaling System **[CasStateMachineDigitSignalingSystem]**	Defines which Signaling System to use in both directions (detection\generation). ▪ **[0]** DTMF = Uses DTMF signaling. ▪ **[1]** MF = Uses MF signaling (default). ▪ **[-1]** Default = Default value.

3.4.4 SS7 Configuration

The SS7 Configuration menu allows you to configure the Signaling System #7 (SS7) protocol parameters. For a detailed description of SS7 configuration, refer to the *Product Reference Manual*.

3.4.5 Sigtran Configuration

The Sigtran Configuration menu allows you to configure the SIGTRAN parameters. For a detailed description of SIGTRAN configuration, refer to the *Product Reference Manual*.

3.4.6 Security Settings

The **Security Settings** menu allows you to configure various security settings. This menu contains the following page items:

- Web User Accounts (refer to "Configuring the Web User Accounts" on page 99)
- Web & Telnet Access List (refer to "Configuring the Web and Telnet Access List" on page 102)
- Firewall Settings (refer to "Configuring the Firewall Settings" on page 103)
- Certificates (refer to "Configuring the Certificates" on page 105)
- General Security Settings (refer to "Configuring the General Security Settings" on page 109)
- IPSec Table (refer to "Configuring the IPSec Table" on page 114)
- IKE Table (refer to "Configuring the IKE Table" on page 117)

3.4.6.1 Configuring the Web User Accounts

To prevent unauthorized access to the Web interface, two Web user accounts are available (primary and secondary) with assigned user name, password, and access level. When you login to the Web interface, you are requested to provide the user name and password of one of these Web user accounts. If the Web session is idle (i.e., no actions are performed) for more than five minutes, the Web session expires and you are once again requested to login with your user name and password. Up to five Web users can simultaneously open (log in to) a session on the device's Web interface.

Each Web user account is composed of three attributes:

- **User name and password:** enables access (login) to the Web interface.
- **Access level:** determines the extent of the access (i.e., availability of pages and read / write privileges). The available access levels and their corresponding privileges are listed in the table below:

Table 3-22: Web User Accounts Access Levels and Privileges

Access Level	Numeric Representation*	Privileges
Security Administrator	200	Read / write privileges for all pages.
Administrator	100	read / write privileges for all pages except security-related pages, which are read-only.
User Monitor	50	No access to security-related and file-loading pages; read-only access to the other pages. This read-only access level is typically applied to the secondary Web user account.
No Access	0	No access to any page.
* The numeric representation of the access level is used only to define accounts in a RADIUS server (the access level ranges from 1 to 255).		

The default attributes for the two Web user accounts are shown in the following table:

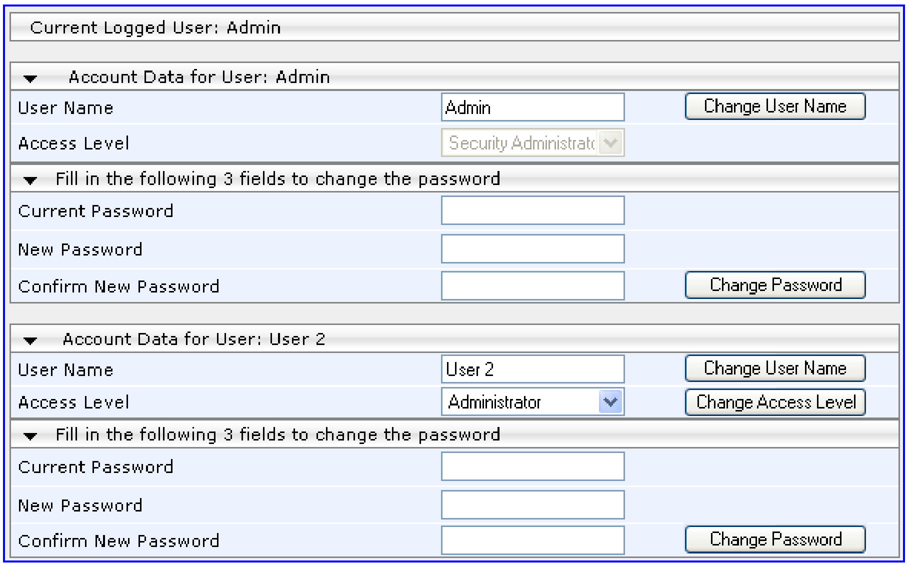
Table 3-23: Default Attributes for the Web User Accounts

Account / Attribute	User Name (Case-Sensitive)	Password (Case-Sensitive)	Access Level
Primary Account	Admin	Admin	Security Administrator **Note:** The Access Level cannot be changed for this account type.
Secondary Account	User	User	User Monitor

➢ To change the Web user accounts attributes, take these 4 steps:

1. Open the 'Web User Accounts' page (**Configuration** tab > **Security Settings** menu > **Web User Accounts** page item).

Figure 3-50: Web User Accounts Page (for Users with 'Security Administrator' Privileges)



Current Logged User: Admin

Account Data for User: Admin

User Name: Admin

Access Level: Security Administrator

Fill in the following 3 fields to change the password

Current Password

New Password

Confirm New Password

Account Data for User: User 2

User Name: User 2

Access Level: Administrator

Fill in the following 3 fields to change the password

Current Password

New Password

Confirm New Password

Note: If you are logged into the Web interface as the Security Administrator, both Web user accounts are displayed on the 'Web User Accounts' page (as shown above). If you are logged in with the secondary user account, only the details of the secondary account are displayed on the page.

2. To change the access level of the secondary account:
   a. From the 'Access Level' drop-down list, select the new access level.
   b. Click **Change Access Level**; the new access level is applied immediately.

Notes:

- The access level of the primary Web user account is 'Security Administrator', which cannot be modified.
- The access level of the secondary account can only be modified by the primary account user or a secondary account user with 'Security Administrator' access level.

3. To change the user name of an account, perform the following:
   a. In the field 'User Name', enter the new user name (maximum of 19 case-sensitive characters).
   b. Click **Change User Name**; if you are currently logged into the Web interface with this account, the 'Enter Network Password' dialog box appears, requesting you to enter the new user name.
4. To change the password of an account, perform the following:
   a. In the field 'Current Password', enter the current password.
   b. In the fields 'New Password' and 'Confirm New Password', enter the new password (maximum of 19 case-sensitive characters).
   c. Click **Change Password**; if you are currently logged into the Web interface with this account, the 'Enter Network Password' dialog box appears, requesting you to enter the new password.

Notes:

- For security, it's recommended that you change the default user name and password.
- A Web user with access level 'Security Administrator' can change all attributes of all the Web user accounts. Web users with an access level other than 'Security Administrator' can only change their own password and user name.
- To reset the two Web user accounts' user names and passwords to default, set the *ini* file parameter ResetWebPassword to 1.
- To access the Web interface with a different account, click the **Log off** button located on the toolbar, click any button or page item, and then re-access the Web interface with a different user name and password.
- You can set the entire Web interface to read-only (regardless of Web user account's access level), by using the *ini* file parameter DisableWebConfig (refer to ''Web and Telnet Parameters'' on page 273).
- Access to the Web interface can be disabled, by setting the *ini* file parameter DisableWebTask to 1. By default, access is enabled.
- You can define additional Web user accounts using a RADIUS server (refer to the *Product Reference Manual*).
- For secured HTTP connection (HTTPS) (refer to the *Product Reference Manual*).

3.4.6.2 Configuring the Web and Telnet Access List

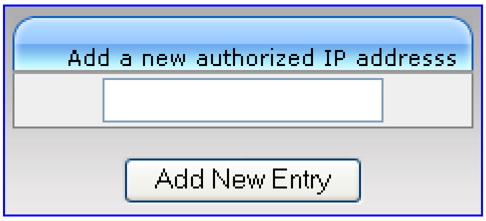
The 'Web & Telnet Access List' page is used to define up to ten IP addresses that are permitted to access the device's Web and Telnet interfaces. Access from an undefined IP address is denied. If no IP addresses are defined, this security feature is inactive and the device can be accessed from any IP address.

The Web and Telnet Access List can also be defined using the *ini* file parameter WebAccessList_x (refer to "Web and Telnet Parameters" on page 273).

- **To add authorized IP addresses for Web and Telnet interfaces access, take these 4 steps:**

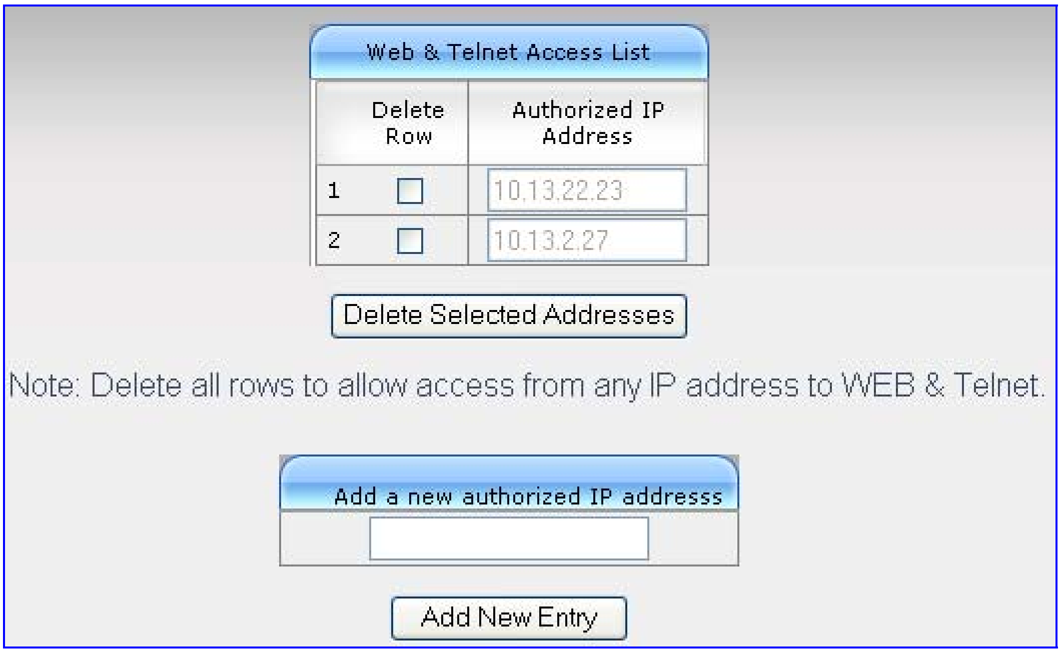
1. Open the 'Web & Telnet Access List' page (**Configuration** tab > **Security Settings** menu > **Web & Telnet Access List** page item).

Figure 3-51: Web & Telnet Access List Page - Add New Entry



2. To add an authorized IP address, in the 'Add a New Authorized IP Address' field, enter the required IP address, and then click **Add New Address**; the IP address you entered is added as a new entry to the 'Web & Telnet Access List' table.

Figure 3-52: Web & Telnet Access List Table



	Delete Row	Authorized IP Address
1	□	10.13.22.23
2	□	10.13.2.27

Note: Delete all rows to allow access from any IP address to WEB & Telnet.

3. To delete authorized IP addresses, select the Delete Row check boxes corresponding to the IP addresses that you want to delete, and then click **Delete Selected Addresses**; the IP addresses are removed from the table and these IP addresses can no longer access the Web and Telnet interfaces.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- The first authorized IP address in the list must be your PC's (terminal) IP address; otherwise, access from your PC is denied.
- Only delete your PC's IP address last from the 'Web & Telnet Access List' page. If it's deleted before the last, access from your PC is denied after it's deleted.

3.4.6.3 Configuring the Firewall Settings

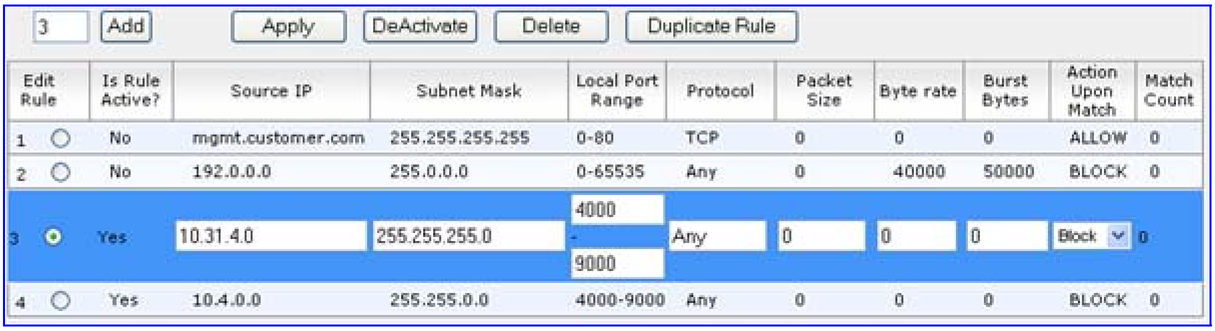
The device provides an internal firewall, allowing you (the security administrator) to define network traffic filtering rules. You can add up to 50 ordered firewall rules. For each packet received on the network interface, the table is scanned from the top down until a matching rule is found. This rule can either deny (*block*) or permit (*allow*) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. For detailed information on the internal firewall, refer to the *Product Reference Manual*.

Note: You can also configure the firewall settings using the *ini* file table parameter AccessList (refer to "Security Parameters" on page 276).

➢ To add firewall rules, take these 5 steps:

1. Open the 'Firewall Settings' page (**Configuration** tab > **Security Settings** menu > **Firewall Settings** page item).

Figure 3-53: Firewall Settings Page



Edit Rule		Is Rule Active?	Source IP	Subnet Mask	Local Port Range	Protocol	Packet Size	Byte rate	Burst Bytes	Action Upon Match	Match Count
1	○	No	mgmt.customer.com	255.255.255.255	0-80	TCP	0	0	0	ALLOW	0
2	○	No	192.0.0.0	255.0.0.0	0-65535	Any	0	40000	50000	BLOCK	0
3	●	Yes	10.31.4.0	255.255.255.0	4000 - 9000	Any	0	0	0	Block	0
4	○	Yes	10.4.0.0	255.255.0.0	4000-9000	Any	0	0	0	BLOCK	0

2. In the 'Add' field, enter the index of the access rule that you want to add, and then click **Add**; a new firewall rule index appears in the table.
3. Configure the firewall rule's parameters according to the table below.
4. Click one of the following buttons:
   - **Apply:** saves the new rule (without activating it).
   - **Duplicate Rule:** adds a new rule by copying a selected rule.
   - **Activate:** saves the new rule and activates it.
   - **Delete:** deletes the selected rule.
5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

➢ To edit a rule, take these 4 steps:

1. In the 'Edit Rule' column, select the rule that you want to edit.
2. Modify the fields as desired.
3. Click the **Apply** button to save the changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

➢ To activate a de-activated rule, take these 2 steps:

1. In the 'Edit Rule' column, select the de-activated rule that you want to activate.
2. Click the **Activate** button; the rule is activated.

➢ To de-activate an activated rule, take these 2 steps:

1. In the 'Edit Rule' column, select the activated rule that you want to de-activate..
2. Click the **DeActivate** button; the rule is de-activated.

➢ To delete a rule, take these 3 steps:

1. Select the radio button of the entry you want to activate.
2. Click the **Delete Rule** button; the rule is deleted.
3. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-24: Internal Firewall Parameters

Parameter	Description
Is Rule Active	A read-only field indicating whether the rule is active or not. **Note:** After device reset, all rules are active.
Source IP **[AccessList_Source_IP]**	IP address (or DNS name) of source network, or a specific host.
Subnet Mask **[AccessList_Net_Mask]**	IP network mask - 255.255.255.255 for a single host or the appropriate value for the source IP addresses. The IP address of the sender of the incoming packet is bitwise ANDed with this mask and then compared to the field 'Source IP'.
Local Port Range **[AccessList_Start_Port]** **[AccessList_End_Port]**	The destination UDP/TCP ports (on this device) to which packets are sent. The valid range is 0 to 65535. **Note:** When the protocol type isn't TCP or UDP, the entire range must be provided.
Protocol **[AccessList_Protocol]**	The protocol type (e.g., UDP, TCP, ICMP, ESP or 'Any'), or the IANA protocol number (in the range of 0 (Any) to 255). **Note:** This field also accepts the abbreviated strings 'SIP' and 'HTTP'. Specifying these strings implies selection of the TCP or UDP protocols, and the appropriate port numbers as defined on the device.

Parameter	Description
Packet Size **[AccessList_Packet_Size]**	Maximum allowed packet size. The valid range is 0 to 65535. **Note:** When filtering fragmented IP packets, this field relates to the overall (re-assembled) packet size, and not to the size of each fragment.
Byte Rate **[AccessList_Byte_Rate]**	Expected traffic rate (bytes per second).
Burst Bytes **[AccessList_Byte_Burst]**	Tolerance of traffic rate limit (number of bytes).
Action Upon Match **[AccessList_Allow_Type]**	Action upon match (i.e., 'Allow' or 'Block').
Match Count **[AccessList_MatchCount]**	A read-only field providing the number of packets accepted / rejected by the specific rule.

3.4.6.4 Configuring the Certificates

The 'Certificates' page is used for the following:

- Replacing the server certificate (refer to "Server Certificate Replacement" on page 105)
- Replacing the client certificates (refer to "Client Certificates" on page 108)
- Regenerating Self-Signed Certificates (refer to "Self-Signed Certificates" on page 109)
- Updating the private key (using HTTPSPkeyFileName, as described in the *Product Reference Manual*).

3.4.6.4.1 Server Certificate Replacement

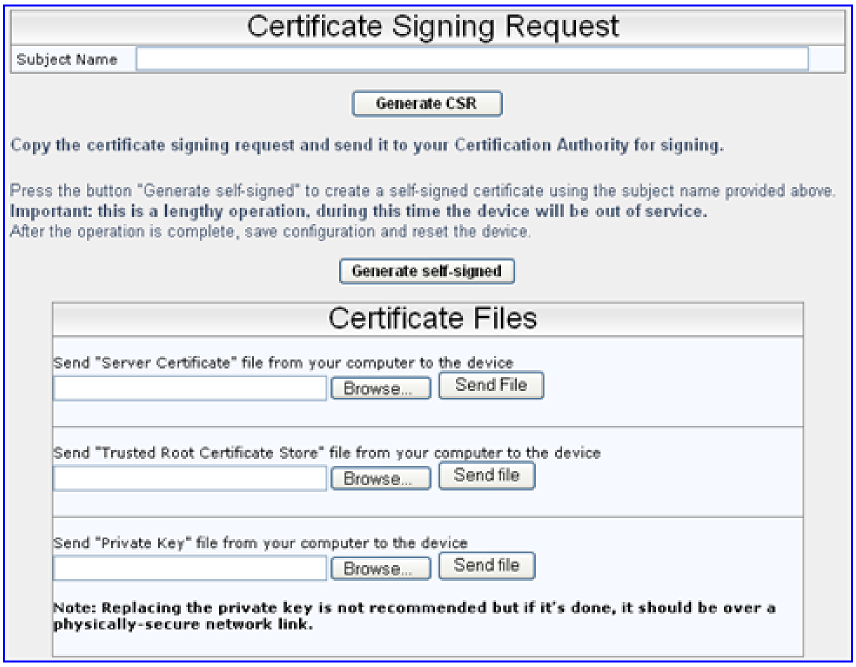
The device is supplied with a working Secure Socket Layer (SSL) configuration consisting of a unique self-signed server certificate. If an organizational Public Key Infrastructure (PKI) is used, you may wish to replace this certificate with one provided by your security administrator.

➢ To replace the device's self-signed certificate, take these 8 steps:

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns_name.corp.customer.com). This DNS name is used to access the device and should therefore, be listed in the server certificate.

2. Open the 'Certificates Signing Request' page (**Configuration** tab > **Security Settings** menu > **Certificates** page item).

Figure 3-54: Certificates Signing Request Page



Certificate Signing Request

Subject Name

Copy the certificate signing request and send it to your Certification Authority for signing.

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.
Important: this is a lengthy operation, during this time the device will be out of service.
After the operation is complete, save configuration and reset the device.

Certificate Files

Send "Server Certificate" file from your computer to the device

Send "Trusted Root Certificate Store" file from your computer to the device

Send "Private Key" file from your computer to the device

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

3. In the 'Subject Name' field, enter the DNS name, and then click **Generate CSR**. A textual certificate signing request that contains the SSL device identifier is displayed.

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 then sends you a server certificate for the device.

5. Save the certificate to a file (e.g., cert.txt). Ensure that the file is a plain-text file containing the 'BEGIN CERTIFICATE' header, as shown in the example of a Base64-Encoded X.509 Certificate below:

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUj
ETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBTZXJ2ZXVy
MB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRlIxEz
ARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCC
ASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkon
WnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7
JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJ
gHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END CERTIFICATE-----
```

6. Set the parameter 'Secured Web Connection (HTTPS)' to 'HTTPS Only' (0) (refer to "Configuring the General Security Settings" on page 109) to ensure you have a method of accessing the device in case the new certificate doesn't work. Restore the previous setting after testing the configuration.

7. In the 'Certificates Files' group, click the **Browse** button corresponding to 'Send Server Certificate...', navigate to the cert.txt file, and then click **Send File**.

8. When the loading of the certificate is complete, save the configuration (refer to "Saving Configuration" on page 230) and restart the device; the Web interface uses the provided certificate.

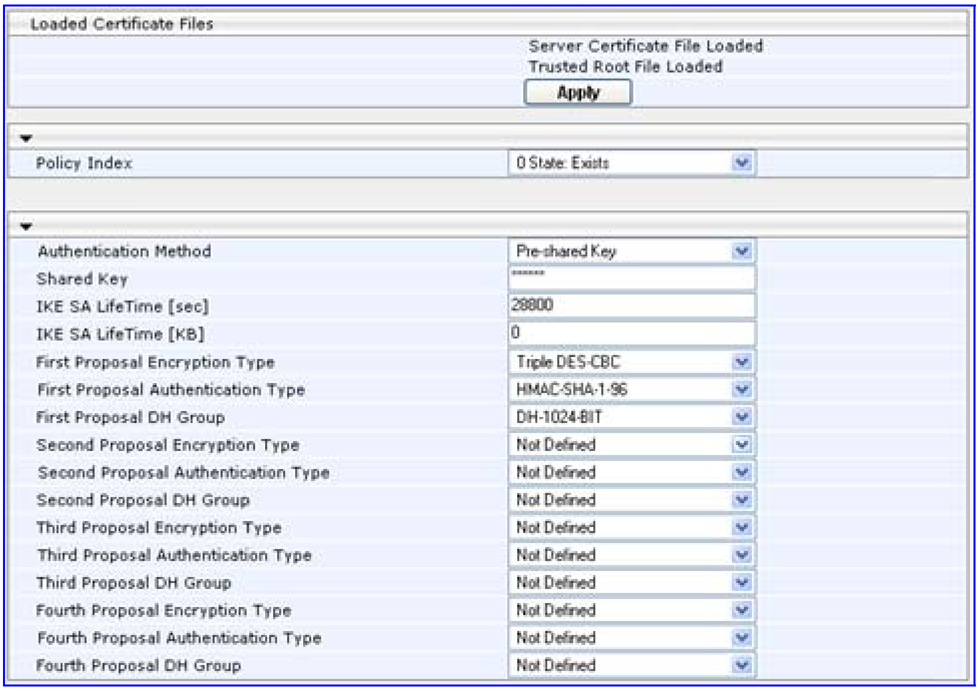
Notes:

- The certificate replacement process can be repeated when necessary (e.g., the new certificate expires).
- It is possible to use the IP address of the device (e.g., 10.3.3.1) instead of a qualified DNS name in the Subject Name. This is not recommended since the IP address is subject to changes and may not uniquely identify the device.
- The server certificate can also be loaded via *ini* file using the parameter HTTPSCertFileName.

➢ To apply the loaded certificate for IPsec negotiations, take these 2 steps:

1. Open the 'IKE Table' page (refer to "Configuring the IKE Table" on page 117); the 'Loaded Certificates Files' group lists the newly uploaded certificates, as shown below:

Figure 3-55: IKE Table Listing Loaded Certificate Files



Loaded Certificate Files

Server Certificate File Loaded
Trusted Root File Loaded

Policy Index	0 State: Exists
Authentication Method	Pre-shared Key
Shared Key	******
IKE SA LifeTime [sec]	28800
IKE SA LifeTime [KB]	0
First Proposal Encryption Type	Triple DES-CBC
First Proposal Authentication Type	HMAC-SHA-1-96
First Proposal DH Group	DH-1024-BIT
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Second Proposal DH Group	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Third Proposal DH Group	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined
Fourth Proposal DH Group	Not Defined

2. Click the **Apply** button to load the certificates; future IKE negotiations are now performed using the new certificates.

3.4.6.4.2 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 used, 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 managing PC, and loading the same certificate (in base64-encoded X.509 format) to the device'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 device must be configured to use NTP (refer to "Simple Network Time Protocol Support" on page 383) to obtain the current date and time. Without the correct date and time, client certificates cannot work.

➢ To enable two-way client certificates, take these 5 steps:

1. Set the parameter 'Secured Web Connection (HTTPS)' to 'HTTPS Only' (0) in "Configuring the General Security Settings" on page 109 to ensure you have a method of accessing the device in case the client certificate doesn’t work. Restore the previous setting after testing the configuration.
2. Open the ‘Certificates Signing Request' page (refer to "Server Certificate Replacement" on page 105).
3. In the 'Certificates Files' group, click the **Browse** button corresponding to 'Send "Trusted Root Certificate Store" file ...', navigate to the file, and then click **Send File**.
4. When the operation is complete, set the *ini* file parameter HTTPSRequireClientCertificates to 1.
5. Save the configuration (refer to "Saving Configuration" on page 230), and then restart the device.

When a user connects to the secured Web server:

- If the user has a client certificate from a CA that is 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 doesn’t have a client certificate from a listed CA, or doesn’t have a client certificate at all, the connection is rejected.

Notes:

- 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.
- The root certificate can also be loaded via *ini* file using the parameter HTTPSRootFileName.
- You can enable Online Certificate Status Protocol (OCSP) on the device to check whether a peer's certificate has been revoked by an OCSP server. For further information, refer to the *Product Reference Manual*.

3.4.6.4.3 Self-Signed Certificates

The device is shipped with an operational, self-signed server certificate. The subject name for this default certificate is 'ACL_nnnnnnn', where *nnnnnnn* denotes the serial number of the device. However, this subject name may not be appropriate for production and can be changed while still using self-signed certificates.

➢ To change the subject name and regenerate the self-signed certificate, take these 4 steps:

1. Before you begin, ensure the following:
   - You have a unique DNS name for the device (e.g., dns_name.corp.customer.com). This name is used to access the device and should therefore, be listed in the server certificate.
   - No traffic is running on the device. The certificate generation process is disruptive to traffic and should be executed during maintenance time.
2. Open the ‘Certificates’ page (refer to "Server Certificate Replacement" on page 105).
3. In the 'Subject Name' field, enter the fully-qualified DNS name (FQDN) as the certificate subject, and then click **Generate Self-signed**; after a few seconds, a message appears displaying the new subject name.
4. Save configuration (refer to "Saving Configuration" on page 230), and then restart the device for the new certificate to take effect.

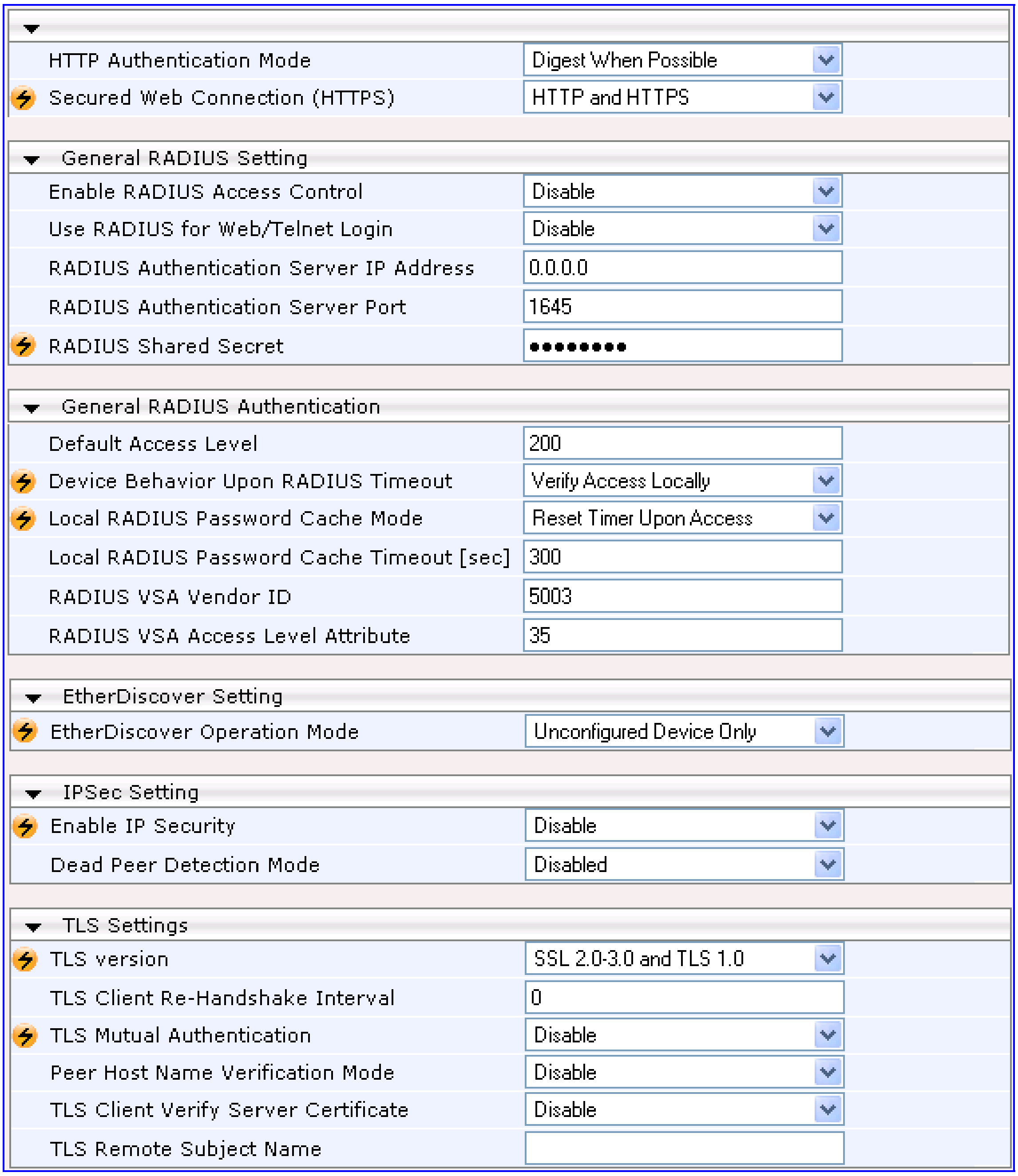
3.4.6.5 Configuring the General Security Settings

The 'General Security Settings' page is used to configure various security features.

➢ To configure the general security parameters, take these 4 steps:

1. Open the 'General Security Settings' page (**Configuration** tab > **Security Settings** menu > **General Security Settings** page item).

Figure 3-56: General Security Settings Page



HTTP Authentication Mode	Digest When Possible
⚡ Secured Web Connection (HTTPS)	HTTP and HTTPS

General RADIUS Setting

Enable RADIUS Access Control	Disable
Use RADIUS for Web/Telnet Login	Disable
RADIUS Authentication Server IP Address	0.0.0.0
RADIUS Authentication Server Port	1645
⚡ RADIUS Shared Secret	●●●●●●●●●

General RADIUS Authentication

Default Access Level	200
⚡ Device Behavior Upon RADIUS Timeout	Verify Access Locally
⚡ Local RADIUS Password Cache Mode	Reset Timer Upon Access
Local RADIUS Password Cache Timeout [sec]	300
RADIUS VSA Vendor ID	5003
RADIUS VSA Access Level Attribute	35

EtherDiscover Setting

⚡ EtherDiscover Operation Mode	Unconfigured Device Only

IPSec Setting

⚡ Enable IP Security	Disable
Dead Peer Detection Mode	Disabled

TLS Settings

⚡ TLS version	SSL 2.0-3.0 and TLS 1.0
TLS Client Re-Handshake Interval	0
⚡ TLS Mutual Authentication	Disable
Peer Host Name Verification Mode	Disable
TLS Client Verify Server Certificate	Disable
TLS Remote Subject Name	

2. Configure the General Security parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-25: General Security Parameters

Parameter	Description
HTTP Authentication Mode **[WebAuthMode]**	Determines the authentication mode for the Web interface. ▪ **[0]** Basic Mode = Basic authentication (clear text) is used (default). ▪ **[1]** Digest When Possible = Digest authentication (MD5) is used. ▪ **[2]** Basic if HTTPS, Digest if HTTP = Digest authentication (MD5) is used for HTTP, and basic authentication is used for HTTPS. **Note:** When RADIUS login is enabled (i.e., the parameter WebRADIUSLogin is set to 1), basic authentication is forced.
Secured Web Connection (HTTPS) **[HTTPSOnly]**	Determines the protocol types used to access the Web interface. ▪ **[0]** Disable = HTTP and HTTPS (default). ▪ **[1]** Enable = Unencrypted HTTP packets are blocked.
General RADIUS Settings	
Enable RADIUS Access Control **[EnableRADIUS]**	Determines whether the RADIUS application is enabled. ▪ **[0]** Disable = RADIUS application is disabled (default). ▪ **[1]** Enable = RADIUS application is enabled.
Use RADIUS for Web/Telnet Login **[WebRADIUSLogin]**	Uses RADIUS queries for Web and Telnet interface authentication. ▪ **[0]** Disable (default). ▪ **[1]** Enable. When enabled, logging in to the device's Web and Telnet embedded servers is performed via a RADIUS server. The device contacts a predefined server and verifies the given user name and password pair against a remote database, in a secure manner. **Notes:** ▪ The parameter EnableRADIUS must be set to 1. ▪ RADIUS authentication requires HTTP basic authentication, meaning the user name and password are transmitted in clear text over the network. Therefore, it's recommended to set the parameter HttpsOnly to 1 to force the use of HTTPS, since the transport is encrypted. ▪ If using RADIUS authentication when logging in to the CLI, only the primary Web User Account (which has Security Administration access level) can access the device's CLI (refer to "Configuring the Web User Accounts" on page 99).
RADIUS Authentication Server IP Address **[RADIUSAuthServerIP]**	IP address of the RADIUS authentication server.
RADIUS Authentication Server Port **[RADIUSAuthPort]**	Port number of the RADIUS authentication server. The default value is 1645.

Parameter	Description
RADIUS Shared Secret **[SharedSecret]**	'Secret' used to authenticate the device to the RADIUS server. Should be a cryptographically strong password.
General RADIUS Authentication	
Default Access Level **[DefaultAccessLevel]**	Defines the default access level for the device when the RADIUS (authentication) response doesn't include an access level attribute. The valid range is 0 to 255. The default value is 200 (Security Administrator').
Device Behavior Upon RADIUS Timeout **[BehaviorUponRadiusTimeout]**	Defines device behavior upon a RADIUS timeout. ▪ **[0]** Deny Access = Denies access. ▪ **[1]** Verify Access Locally = Checks password locally (default).
Local RADIUS Password Cache Mode **[RadiusLocalCacheMode]**	Defines the device's mode of operation regarding the timer (configured by the parameter RadiusLocalCacheTimeout) that determines the validity of the user name and password (verified by the RADIUS server). ▪ **[0]** Absolute Expiry Timer = when you access a Web page, the timeout doesn't reset but instead, continues decreasing. ▪ **[1]** Reset Timer Upon Access = upon each access to a Web page, the timeout always resets (reverts to the initial value configured by RadiusLocalCacheTimeout).
Local RADIUS Password Cache Timeout **[RadiusLocalCacheTimeout]**	Defines the time (in seconds) the locally stored user name and password (verified by the RADIUS server) are valid. When this time expires, the user name and password become invalid and a must be re-verified with the RADIUS server. The valid range is 1 to 0xFFFFFF. The default value is 300 (5 minutes). ▪ **[-1]** = Never expires. ▪ **[0]** = Each request requires RADIUS authentication.
RADIUS VSA Vendor ID **[RadiusVSAVendorID]**	Defines the vendor ID that the device accepts when parsing a RADIUS response packet. The valid range is 0 to 0xFFFFFFFF. The default value is 5003.
RADIUS VSA Access Level Attribute **[RadiusVSAAccessAttribute]**	Defines the code that indicates the access level attribute in the Vendor Specific Attributes (VSA) section of the received RADIUS packet. The valid range is 0 to 255. The default value is 35.
EtherDiscover Setting	
EtherDiscover Operation Mode	N/A.
IPSec Setting	
Enable IP Security **[EnableIPSec]**	Enables / disables the Internet Protocol security (IPSec) on the device. ▪ **[0]** Disable = IPSec is disabled (default). ▪ **[1]** Enable = IPSec is enabled.
Dead Peer Detection Mode **[IPSecDPDMode]**	Enables the Dead Peer Detection (DPD) 'keep-alive' mechanism (according to RFC 3706) to detect loss of peer connectivity.

Parameter	Description
	▪ **[0]** Disabled (default). ▪ **[1]** Periodic = message exchanges at regular intervals. ▪ **[2]** On Demand = message exchanges as needed (i.e., before sending data to the peer). If the liveliness of the peer is questionable, the device sends a DPD message to query the status of the peer. If the device has no traffic to send, it never sends a DPD message. For detailed information on DPD, refer to the *Product Reference Manual*.
TLS Settings	
TLS version **[TLSVersion]**	Defines the supported versions of SSL/TLS (Secure Socket Layer/Transport Layer Security. ▪ **[0]** SSL 2.0-3.0 and TLS 1.0 = SSL 2.0, SSL 3.0, and TLS 1.0 are supported (default). ▪ **[1]** TLS 1.0 Only = only TLS 1.0 is used. When set to 0, SSL/TLS handshakes always start with SSL 2.0 and switch to TLS 1.0 if both peers support it. When set to 1, TLS 1.0 is the only version supported; clients attempting to contact the device using SSL 2.0 are rejected.
TLS Client Re-Handshake Interval **[TLSReHandshakeInterval]**	Defines the time interval (in minutes) between TLS Re-Handshakes initiated by the device. The interval range is 0 to 1,500 minutes. The default is 0 (i.e., no TLS Re-Handshake).
TLS Mutual Authentication **[SIPSRequireClientCertificate]**	Determines the device's behavior when acting as a server for TLS connections. ▪ **[0]** Disable = The device does not request the client certificate (default). ▪ **[1]** Enable = The device requires receipt and verification of the client certificate to establish the TLS connection. **Notes:** ▪ The SIPS certificate files can be changed using the parameters HTTPSCertFileName and HTTPSRootFileName. ▪ This parameter cannot be changed on-the-fly and requires a device reset.
Peer Host Name Verification Mode **[PeerHostNameVerificationMode]**	Determines whether the device verifies the Subject Name of a remote certificate when establishing TLS connections. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Server Only = Verify Subject Name only when acting as a server for the TLS connection. ▪ **[2]** Server & Client = Verify Subject Name when acting as a server or client for the TLS connection. When a remote certificate is received and this parameter is not disabled, the SubjectAltName value is compared with the list of available Proxies. If a match is found for any of the configured Proxies, the TLS connection is established. The comparison is performed if the SubjectAltName is either a

Parameter	Description
	DNS name (DNSName) or an IP address. If no match is found and the SubjectAltName is marked as 'critical', the TLS connection is not established. If DNSName is used, the certificate can also use wildcards ('*') to replace parts of the domain name. If the SubjectAltName is not marked as 'critical' and there is no match, the CN value of the SubjectName field is compared with the parameter TLSRemoteSubjectName. If a match is found, the connection is established. Otherwise, the connection is terminated.
TLS Client Verify Server Certificate **[VerifyServerCertificate]**	Determines whether the device, when acting as client for TLS connections, verifies the Server certificate. The certificate is verified with the Root CA information. ▪ **[0]** Disable (default). ▪ **[1]** Enable. **Note:** If Subject Name verification is necessary, the parameter PeerHostNameVerificationMode must be used as well.
TLS Remote Subject Name **[TLSRemoteSubjectName]**	Defines the Subject Name that is compared with the name defined in the remote side certificate when establishing TLS connections. If the SubjectAltName of the received certificate is not equal to any of the defined Proxies Host names/IP addresses and is not marked as 'critical', the Common Name (CN) of the Subject field is compared with this value. If not equal, the TLS connection is not established. If the CN uses a domain name, the certificate can also use wildcards ('*') to replace parts of the domain name. The valid range is a string of up to 49 characters. **Note:** This parameter is applicable only if the parameter PeerHostNameVerificationMode is set to 1 or 2.

3.4.6.6 Configuring the IPSec Table

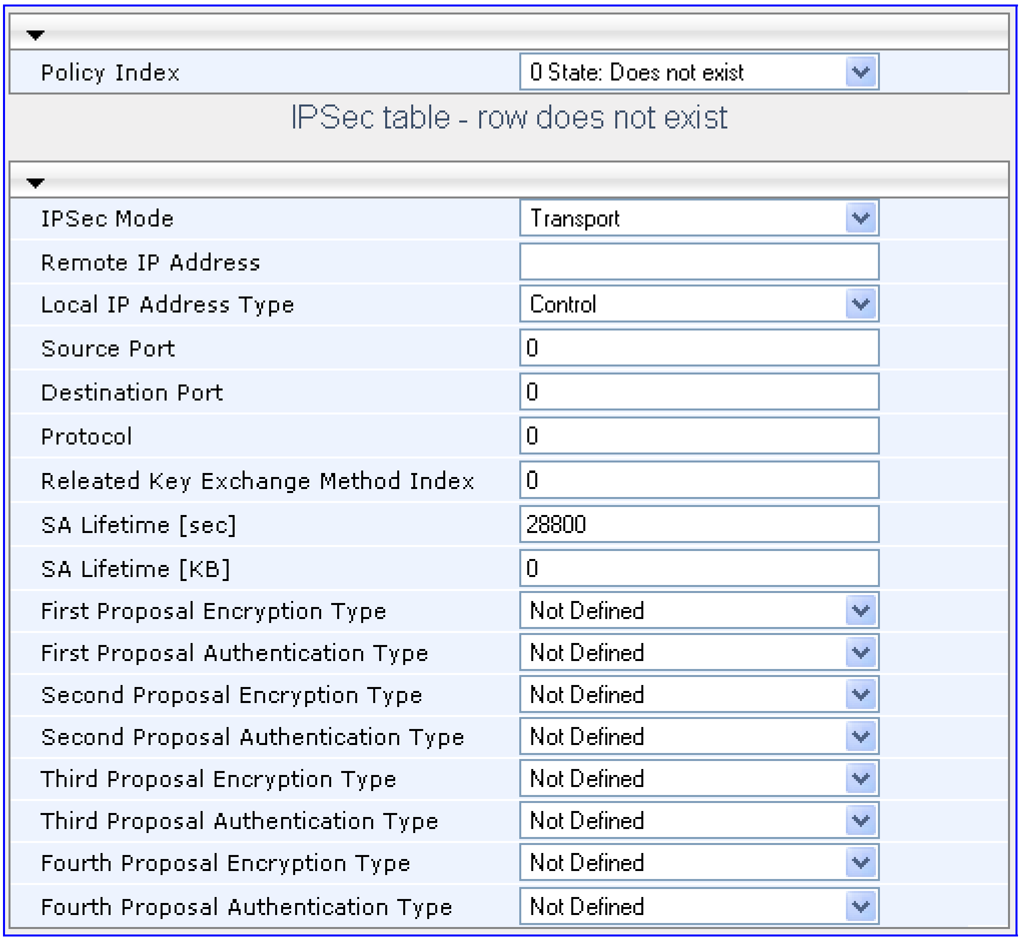
The 'IPSec Table' page allows you to configure the Security Policy Database (SPD) parameters for IP security (IPSec).

Note: You can also configure the IPSec table using the *ini* file table parameter IPSEC_SPD_TABLE (refer to "Security Parameters" on page 276).

➢ To configure the IPSec SPD table, take these 5 steps:

1. Open the 'IPSec Table' page (**Configuration** tab > **Security Settings** menu > **IPSec Table** page item).

Figure 3-57: IPSec Table Page



Policy Index	0 State: Does not exist

IPSec table - row does not exist

IPSec Mode	Transport
Remote IP Address	
Local IP Address Type	Control
Source Port	0
Destination Port	0
Protocol	0
Releated Key Exchange Method Index	0
SA Lifetime [sec]	28800
SA Lifetime [KB]	0
First Proposal Encryption Type	Not Defined
First Proposal Authentication Type	Not Defined
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined

2. From the 'Policy Index' drop-down list, select the rule you want to edit (up to 20 policy rules can be configured).

3. Configure the IPSec SPD parameters according to the table below.

4. Click the button **Create**; the IPSec rule is applied on-the-fly to the device.

5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

If no IPSec methods are defined (Encryption / Authentication), the default settings, shown in the following table are applied.

Table 3-26: Default IKE Second Phase Proposals

Proposal	Encryption	Authentication
Proposal 0	3DES	SHA1
Proposal 1	3DES	MD5
Proposal 2	DES	SHA1
Proposal 3	DES	MD5

Table 3-27: IPSec SPD Table Configuration Parameters

Parameter Name	Description	
IPSec Mode **[IPSecMode]**	Defines the IPSec mode of operation. ▪ **[0]** Transport (Default) ▪ **[1]** Tunneling	
Remote Tunnel IP Address **[IPSecPolicyRemoteTunnelIPAddress]**	Defines the IP address of the remote IPSec tunneling device. **Note:** This parameter is available only if the parameter IPSecMode is set to Tunneling (1).	IPSec is applied to outgoing packets that match the values defined for these parameters.
Remote Subnet Mask **[IPsecPolicyRemoteSubnetMask]**	Defines the subnet mask of the remote IPSec tunneling device. The default value is 255.255.255.255 (i.e., host-to-host IPSec tunnel). **Note:** This parameter is available only if the parameter IPSecMode is set to Tunneling (1).	
Remote IP Address **[IPSecPolicyRemoteIPAddress]**	Destination IP address (or FQDN) to which the IPSec mechanism is applied. **Notes:** ▪ This parameter is mandatory. ▪ When an FQDN is used, a DNS server must be configured (DNSPriServerIP).	
Local IP Address Type **[IPSecPolicyLocalIPAddressType]**	Determines the local interface to which the encryption is applied (applicable to multiple IPs and VLANs). ▪ **[0]** OAM = OAMP interface (default). ▪ **[1]** Control = Control interface.	
Source Port **[IPSecPolicySrcPort]**	Defines the source port to which the IPSec mechanism is applied. The default value is 0 (i.e., any port).	
Destination Port **[IPSecPolicyDstPort]**	Defines the destination port to which the IPSec mechanism is applied. The default value is 0 (i.e., any port).	
Protocol **[IPSecPolicyProtocol]**	Defines the protocol type to which the IPSec mechanism is applied. ▪ 0 = Any protocol (default). ▪ 17 = UDP. ▪ 6 = TCP. ▪ Any other protocol type defined by IANA (Internet Assigned Numbers Authority).	
Related Key Exchange Method Index **[IPsecPolicyKeyExchangeMethodIndex]**	Determines the index for the corresponding IKE entry. Note that several policies can be associated with a single IKE entry. The valid range is 0 to 19. The default value is 0.	

Parameter Name	Description
IKE Second Phase Parameters (Quick Mode)	
SA Lifetime (sec) **[PsecPolicyLifeInSec]**	Determines the time (in seconds) that the SA negotiated in the second IKE session (quick mode) is valid. After the time expires, the SA is re-negotiated. The default value is 28,800 (i.e., 8 hours).
SA Lifetime (KB) **[IPSecPolicyLifeInKB]**	Determines the lifetime (in kilobytes) that the SA negotiated in the second IKE session (quick mode) is valid. After this size is reached, the SA is re-negotiated. The default value is 0 (i.e., this parameter is ignored).
These lifetime parameters [SA Lifetime (sec) and SA Lifetime (KB)] determine the duration for which an SA is valid. When the lifetime of the SA expires, it is automatically renewed by performing the IKE second phase negotiations. To refrain from a situation where the SA expires, a new SA is negotiated while the old one is still valid. As soon as the new SA is created, it replaces the old one. This procedure occurs whenever an SA is about to expire.	
First to Fourth Proposal Encryption Type **[IPSecPolicyProposalEncryption_X]**	Determines the encryption type used in the quick mode negotiation for up to four proposals. For the *ini* file parameter, *X* depicts the proposal number (0 to 3)). The valid encryption values are: ▪ **[0]** None = No encryption ▪ **[1]** DES-CBC ▪ **[2]** Triple DES-CBC ▪ **[3]** AES-CBC ▪ Not Defined (default)
First to Fourth Proposal Authentication Type **[IPSecPolicyProposalAuthentication_X]**	Determines the authentication protocol used in the quick mode negotiation for up to four proposals. For the *ini* file parameter, *X* depicts the proposal number (0 to 3). The valid authentication values are: ▪ **[2]** HMAC-SHA-1-96 ▪ **[4]** HMAC-MD5-96 ▪ Not Defined (default)

3.4.6.7 Configuring the IKE Table

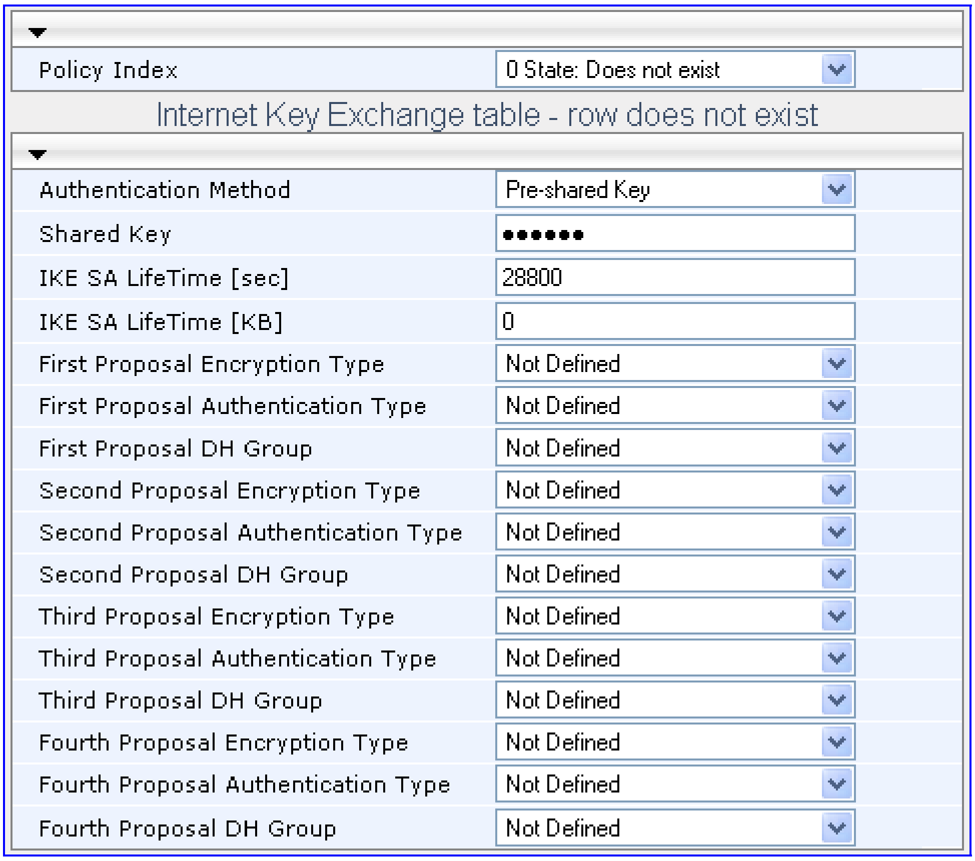
The 'IKE Table' page is used to configure the Internet Key Exchange (IKE) parameters.

Note: You can also configure the IKE table using the *ini* file table parameter IPSec_IKEDB_Table (refer to "Security Parameters" on page 276).

➢ To configure the IKE table, take these 5 steps:

1. Open the 'IKE Table' page (**Configuration** tab > **Security Settings** menu > **IKE Table** page item).

Figure 3-58: IKE Table Page



Policy Index	0 State: Does not exist

Internet Key Exchange table - row does not exist

Authentication Method	Pre-shared Key
Shared Key	••••••
IKE SA LifeTime [sec]	28800
IKE SA LifeTime [KB]	0
First Proposal Encryption Type	Not Defined
First Proposal Authentication Type	Not Defined
First Proposal DH Group	Not Defined
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Second Proposal DH Group	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Third Proposal DH Group	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined
Fourth Proposal DH Group	Not Defined

2. From the 'Policy Index' drop-down list, select the peer you want to edit (up to 20 peers can be configured).

3. Configure the IKE parameters according to the table below. Up to two IKE main mode proposals (Encryption / Authentication / DH group combinations) can be defined. The same proposals must be configured for all peers.

4. Click **Create**; a row is created in the IKE table.

5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

To delete a peer from the IKE table, select it from the 'Policy Index' drop-down list, click the button **Delete**, and then click **OK** at the prompt.

If no IKE methods are defined (Encryption / Authentication / DH Group), the default settings (shown in the following table) are applied.

Table 3-28: Default IKE First Phase Proposals

Proposal	Encryption	Authentication	DH Group
Proposal 0	3DES	SHA1	1024
Proposal 1	3DES	MD5	1024
Proposal 2	3DES	SHA1	786
Proposal 3	3DES	MD5	786

The parameters described in the following table 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.

Table 3-29: IKE Table Configuration Parameters

Parameter Name	Description
Authentication Method **[IkePolicyAuthenticationMethod]**	Determines the authentication method for IKE. ▪ **[0]** Pre-shared Key (default) ▪ **[1]** RSA Signature **Notes:** ▪ For pre-shared key authentication, peers participating in an IKE exchange must have a prior (out-of-band) knowledge of the common key (see IKEPolicySharedKey parameter). ▪ For RSA signature authentication, peers must be loaded with a certificate signed by a common CA. For additional information on certificates, refer to "Server Certificate Replacement" on page 105.
Shared Key **[IKEPolicySharedKey]**	Determines the pre-shared key (in textual format). Both peers must register the same pre-shared key for the authentication process to succeed. **Notes:** ▪ The pre-shared key forms the basis of IPSec security and should therefore, be handled cautiously (in the same way as sensitive passwords). It is not recommended to use the same pre-shared key for several connections. ▪ Since the *ini* file is in plain text format, loading it to the device over a secure network connection is recommended, preferably over a direct crossed-cable connection from a management PC. For added confidentiality, use the encoded *ini* file option (described in "Secured Encoded ini File" on page 255). ▪ After it is configured, the value of the pre-shared key cannot be obtained via Web interface, *ini* file, or SNMP (refer the *Product Reference Manual*).
IKE SA LifeTime (sec) **[IKEPolicyLifeInSec]**	Determines the time (in seconds) the SA negotiated in the first IKE session (main mode) is valid. After the time expires, the SA is re-negotiated. The default value is 28800 (i.e., 8 hours).
IKE SA LifeTime (KB) **[IKEPolicyLifeInKB]**	Determines the lifetime (in kilobytes) that the SA negotiated in the first IKE session (main mode) is valid. After this size is reached, the SA is re-negotiated. The default value is 0 (i.e., this parameter is ignored).
These lifetime parameters [IKE SA LifeTime (sec) and IKE SA LifeTime (KB)] determine the duration the SA created in the main mode phase is valid. When the lifetime of the SA expires, it's automatically renewed by performing the IKE first phase negotiations. To refrain from a situation where the SA expires, a new SA is negotiated while the old one is still valid. As soon as the new SA is created, it replaces the old one. This procedure occurs whenever an SA is about to expire.	
First to Fourth Proposal Encryption Type **[IKEPolicyProposalEncryption_X]**	Determines the encryption type used in the main mode negotiation for up to four proposals. For the *ini* file parameter, *X* depicts the proposal number (0 to 3).

Parameter Name	Description
	▪ **[1]** DES-CBC ▪ **[2]** Triple DES-CBC ▪ **[3]** AES-CBC ▪ Not Defined (default)
First to Fourth Proposal Authentication Type **[IKEPolicyProposalAuthentication_X]**	Determines the authentication protocol used in the main mode negotiation for up to four proposals. For the *ini* file parameter, *X* depicts the proposal number (0 to 3). ▪ **[2]** HMAC-SHA1-96) ▪ **[4]** HMAC-MD5-96 ▪ Not Defined (default)
First to Fourth Proposal DH Group **[IKEPolicyProposalDHGroup_X]**	Determines the length of the key created by the DH protocol for up to four proposals. For the *ini* file parameter, *X* depicts the proposal number (0 to 3). ▪ **[0]** DH-786-Bit ▪ **[1]** DH-1024-Bit ▪ Not Defined (default)

3.4.7 Protocol Configuration

The **Protocol Configuration** menu allows you to configure the device's SIP parameters and contains the following submenus:

- Protocol Definition (refer to "Configuring the Protocol Definition Parameters" on page 120)
- SIP Advanced Parameters (refer to "Configuring the SIP Advanced Parameters" on page 151)
- Manipulation Tables (refer to "Configuring the Number Manipulation Tables" on page 164)
- Routing Tables (refer to "Configuring the Routing Tables" on page 171)
- Profile Definitions (refer to "Configuring the Profile Definitions" on page 190)
- Trunk/IP Group (refer to "Configuring the Trunk and IP Groups" on page 195)
- Digital Gateway (refer to “Configuring the Digital Gateway Parameters” on page 207)

3.4.7.1 Configuring the Protocol Definition Parameters

The **Protocol Definition** submenu allows you to configure the main SIP protocol parameters. This submenu contains the following page items:

- SIP General Parameters (refer to "SIP General Parameters" on page 121)
- Proxy & Registration (refer to "Proxy & Registration Parameters" on page 132)
- Proxy Sets Table (refer to "Proxy Sets Table" on page 141)
- Coders (refer to "Coders" on page 144)
- DTMF & Dialing (refer to "DTMF & Dialing Parameters" on page 147)

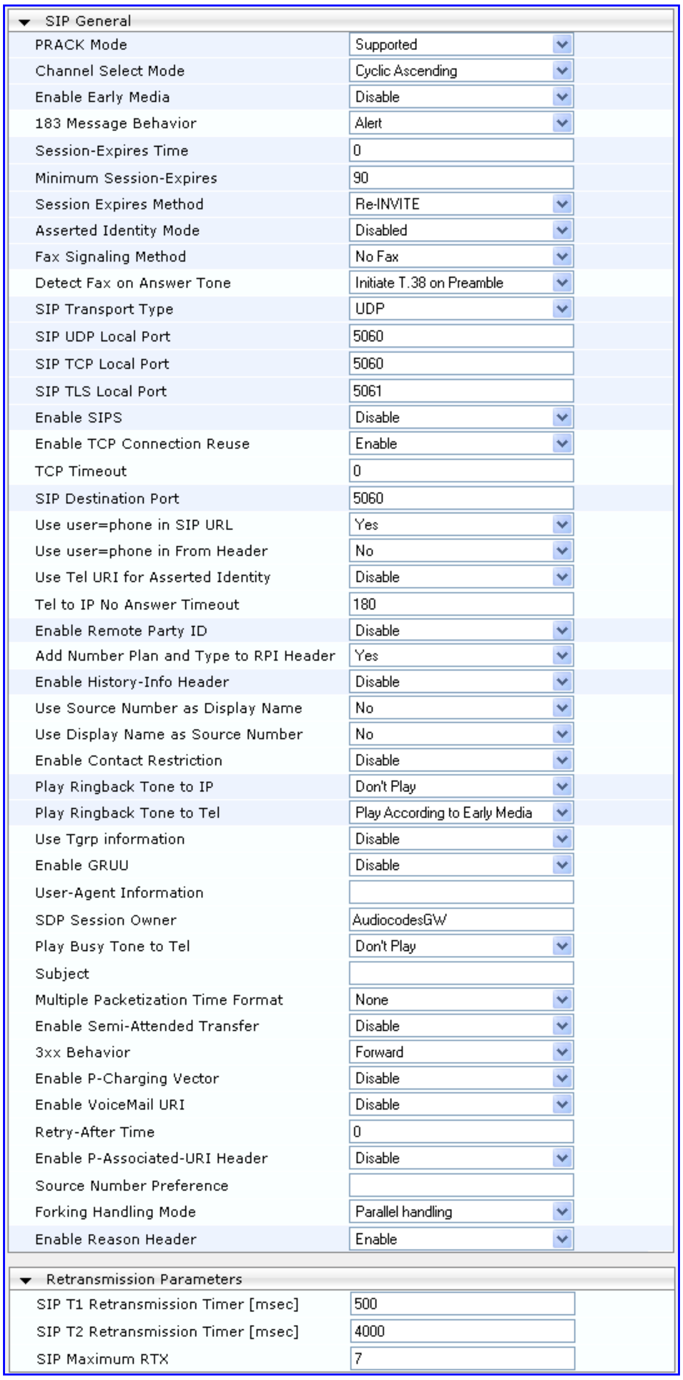
3.4.7.1.1 SIP General Parameters

The 'SIP General Parameters' page is used to configure general SIP parameters.

➢ **To configure the general SIP protocol parameters, take these 4 steps:**

1. Open the 'SIP General Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **SIP General Parameters** page item).

Figure 3-59: SIP General Parameters Page



SIP General

PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Disable
183 Message Behavior	Alert
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060
Use user=phone in SIP URL	Yes
Use user=phone in From Header	No
Use Tel URI for Asserted Identity	Disable
Tel to IP No Answer Timeout	180
Enable Remote Party ID	Disable
Add Number Plan and Type to RPI Header	Yes
Enable History-Info Header	Disable
Use Source Number as Display Name	No
Use Display Name as Source Number	No
Enable Contact Restriction	Disable
Play Ringback Tone to IP	Don't Play
Play Ringback Tone to Tel	Play According to Early Media
Use Tgrp information	Disable
Enable GRUU	Disable
User-Agent Information	
SDP Session Owner	AudiocodesGW
Play Busy Tone to Tel	Don't Play
Subject	
Multiple Packetization Time Format	None
Enable Semi-Attended Transfer	Disable
3xx Behavior	Forward
Enable P-Charging Vector	Disable
Enable VoiceMail URI	Disable
Retry-After Time	0
Enable P-Associated-URI Header	Disable
Source Number Preference	
Forking Handling Mode	Parallel handling
Enable Reason Header	Enable

Retransmission Parameters

SIP T1 Retransmission Timer [msec]	500
SIP T2 Retransmission Timer [msec]	4000
SIP Maximum RTX	7

2. Configure the parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-30: SIP General Parameters (Protocol Definition)

Parameter	Description
PRACK Mode **[PRACKMode]**	PRACK (Provisional Acknowledgment) mechanism mode for 1xx SIP reliable responses. ▪ **[0]** Disable ▪ **[1]** Supported (default) ▪ **[2]** Required **Notes:** ▪ The Supported and Required headers contain the '100rel' tag. ▪ The device sends PRACK messages if the 180/183 response is received with '100rel' in the Supported or Required headers.
Channel Select Mode **[ChannelSelectMode]**	Port (channel) allocation algorithm for IP-to-Tel calls. ▪ **[0]** By Dest Phone Number = Selects the device's channel according to the called number. (default.) ▪ **[1]** Cyclic Ascending = Selects the next available channel in an ascending cyclic order. Always selects the next higher channel number in the trunk group. When the device reaches the highest channel number in the trunk group, it selects the lowest channel number in the trunk group and then starts ascending again. ▪ **[2]** Ascending = Selects the lowest available channel. It always starts at the lowest channel number in the trunk group and if that channel is not available, selects the next higher channel. ▪ **[3]** Cyclic Descending = Selects the next available channel in descending cyclic order. Always selects the next lower channel number in the trunk group. When the device reaches the lowest channel number in the trunk group, it selects the highest channel number in the trunk group and then starts descending again. ▪ **[4]** Descending = Selects the highest available channel. Always starts at the highest channel number in the trunk group and if that channel is not available, selects the next lower channel. ▪ **[5]** Dest Number + Cyclic Ascending = First selects the device's port according to the called number. If the called number isn't found, it then selects the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released. ▪ **[6]** By Source Phone Number = Selects the device's channel according to the calling number. ▪ **[7]** Trunk Cyclic Ascending = Selects the device's port from the first channel of the next trunk (next to the trunk from which the previous channel was allocated. **Notes:** ▪ The internal numbers of the device's B-channels are defined by the TrunkGroup parameter. ▪ For defining the channel select mode per Trunk Group, refer to "Configuring the Trunk Group Settings" on page 197.

Parameter	Description
Enable Early Media **[EnableEarlyMedia]**	Enables the device to send a 183 Session Progress response with SDP (instead of 180 Ringing), allowing the media stream to be established prior to the answering of the call. ▪ **[0]** Disable = Early Media is disabled (default). ▪ **[1]** Enable = Enables Early Media. Sending a 183 response depends on the Progress Indicator (PI). It is sent only if PI is set to 1 or 8 are received in Proceeding or Alert PRI messages. For CAS devices, see the ProgressIndicator2IP parameter.
183 Message Behavior **[SIP183Behaviour]**	Defines the ISDN message that is sent when the 183 Session Progress message is received for IP-to-Tel calls. ▪ **[0]** Progress = The device sends a PROGRESS message (default). ▪ **[1]** Alert = The device sends an ALERT message (upon receipt of a 183 response) instead of an ISDN PROGRESS message.
Session-Expires Time **[SIPSessionExpires]**	Determines the numerical value that is sent in the Session-Expires header in the first INVITE request or response (if the call is answered). The valid range is 1 to 86,400 sec. The default is 0 (i.e., the Session-Expires header is disabled).
Minimum Session-Expires **[MinSE]**	Defines the time (in seconds) that is used in the Min-SE header. This header defines the minimum time that the user agent refreshes the session. The valid range is 10 to 100,000. The default value is 90.
Session Expires Method **[SessionExpiresMethod]**	Determines the SIP method used for session-timer updates. ▪ **[0]** Re-INVITE = Uses Re-INVITE messages for session-timer updates (default). ▪ **[1]** UPDATE = Uses UPDATE messages. **Notes:** ▪ The device can receive session-timer refreshes using both methods. ▪ The UPDATE message used for session-timer is excluded from the SDP body.
Asserted Identity Mode **[AssertedIdMode]**	Determines whether P-Asserted-Identity or P-Preferred-Identity is used in the generated INVITE request for Caller ID (or privacy). ▪ **[0]** Disabled = None (default) ▪ **[1]** Adding PAsserted Identity ▪ **[2]** Adding PPreferred Identity The Asserted ID mode defines the header (P-Asserted-Identity or P-Preferred-Identity) that is used in the generated INVITE request. The header also depends on the calling Privacy (allowed or restricted). The P-Asserted-Identity (or P-Preferred-Identity) headers are used to present the originating party's Caller ID. The Caller ID is composed of a Calling Number and (optionally) a Calling Name. P-Asserted-Identity (or P-Preferred-Identity) headers are used together with the Privacy header. If Caller ID is restricted (P-Asserted-Identity is not sent), the Privacy header includes the value 'id' ('Privacy: id'). Otherwise, for allowed Caller ID, 'Privacy: none' is used. If Caller ID is restricted (received from PSTN), the From header is set to <anonymous@anonymous.invalid>. The logic for filling the calling party parameters is as follows: the SIP header is selected first from which the calling party parameters are

Parameter	Description
	obtained: first priority is P-Asserted-Identity, second is Remote-Party-ID, and third is the From header. Once a URL is selected, all the calling party parameters are set from this header. If P-Asserted-Identity is selected, the Privacy header is checked and if the Privacy is set to 'id', the calling number is assumed restricted.
Fax Signaling Method **[IsFaxUsed]**	Determines the SIP signaling method for establishing and transmitting a fax session after a fax is detected. ▪ **[0]** No Fax = No fax negotiation using SIP signaling. Fax transport method is according to the parameter FaxTransportMode (default). ▪ **[1]** T.38 Relay = Initiates T.38 fax relay. ▪ **[2]** G.711 Transport = Initiates fax / modem using the coder G.711 A-law/µ-law with adaptations (refer to Note below). ▪ **[3]** Fax Fallback = Initiates T.38 fax relay. If the T.38 negotiation fails, the device re-initiates a fax session using the coder G.711 A-law/µ-law with adaptations (refer to the Note below). **Notes:** ▪ Fax adaptations (for options 2 and 3): Echo Canceller = On Silence Compression = Off Echo Canceller Non-Linear Processor Mode = Off Dynamic Jitter Buffer Minimum Delay = 40 Dynamic Jitter Buffer Optimization Factor = 13 ▪ If the device initiates a fax session using G.711 (option 2 and possibly 3), a 'gpmd' attribute is added to the SDP in the following format: For A-law: 'a=gpmd:8 vbd=yes;ecan=on'. For µ-law: 'a=gpmd:0 vbd=yes;ecan=on'. ▪ When IsFaxUsed is set to 1, 2, or 3, the parameter FaxTransportMode is ignored. ▪ When the value of IsFaxUsed is other than 1, T.38 might still be used without the control protocol's involvement. To completely disable T.38, set FaxTransportMode to a value other than 1. ▪ For detailed information on fax transport methods, refer to "Fax/Modem Transport Modes" on page 351.
Detect Fax on Answer Tone **[DetFaxOnAnswerTone]**	Determines when the device initiates a T.38 session for fax transmission. ▪ **[0]** Initiate T.38 on Preamble = The device to which the called fax is connected initiates a T.38 session on receiving Preamble signal from the fax (default). ▪ **[1]** Initiate T.38 on CED = The device to which the called fax is connected initiates a T.38 session on receiving a CED answer tone from the fax. This option can only be used to relay fax signals, as the device sends T.38 Re-INVITE on detection of any fax/modem Answer tone (2100 Hz, amplitude modulated 2100 Hz, or 2100 Hz with phase reversals). The modem signal fails when using T.38 for fax relay. **Notes:** ▪ For this parameter to take effect, you must reset the device. ▪ This parameters is applicable only if the *ini* file parameter IsFaxUsed is set to 1 or 3.

Parameter	Description
SIP Transport Type **[SIPTransportType]**	Determines the default transport layer for outgoing SIP calls initiated by the device. ▪ **[0]** UDP (default) ▪ **[1]** TCP ▪ **[2]** TLS (SIPS) **Notes:** ▪ It's recommended to use TLS for communication with a SIP Proxy and not for direct device-to-device communication. ▪ For received calls (i.e., incoming), the device accepts all these protocols. ▪ The value of this parameter is also used by the SAS application as the default transport layer for outgoing SIP calls.
SIP UDP Local Port **[LocalSIPPort]**	Local UDP port for SIP messages. The valid range is 1 to 65534. The default value is 5060.
SIP TCP Local Port **[TCPLocalSIPPort]**	Local TCP port for SIP messages. The valid range is 1 to 65534. The default value is 5060.
SIP TLS Local Port **[TLSLocalSIPPort]**	Local TLS port for SIP messages. The valid range is 1 to 65534. The default value is 5061. **Note:** The value of must be different than the value of 'SIP TCP Local Port' (TCPLocalSIPPort).
Enable SIPS **[EnableSIPS]**	Enables secured SIP (SIPS URI) connections over multiple hops. ▪ **[0]** Disable (default). ▪ **[1]** Enable. When 'SIP Transport Type' is set to TLS (SIPTransportType = 2) and 'Enable SIPS' is disabled, TLS is used for the next network hop only. When 'SIP Transport Type' is set to TCP or TLS (SIPTransportType = 2 or 1) and 'Enable SIPS' is enabled, TLS is used through the entire connection (over multiple hops). **Note:** If this parameter is enabled and 'SIP Transport Type' is set to UDP (SIPTransportType = 0), the connection fails.
Enable TCP Connection Reuse **[EnableTCPConnectionReuse]**	Enables the reuse of the same TCP connection for all calls to the same destination. ▪ **[0]** Disable = Use a separate TCP connection for each call (default). ▪ **[1]** Enable = Use the same TCP connection for all calls.
TCP Timeout **[SIPTCPTimeout]**	Defines the Timer B (INVITE transaction timeout timer) and Timer F (non-INVITE transaction timeout timer), as defined in RFC 3261, when the SIP Transport Type is TCP. The valid range is 0 to 40 sec. The default value is 64*SIPT1Rtx msec.
SIP Destination Port **[SIPDestinationPort]**	SIP destination port for sending initial SIP requests. The valid range is 1 to 65534. The default port is 5060. **Note:** SIP responses are sent to the port specified in the Via header.
Use user=phone in SIP URL **[IsUserPhone]**	Determines whether to add 'user=phone' string in SIP URI. ▪ **[0]** No = 'user=phone' string isn't used in SIP URI. ▪ **[1]** Yes = 'user=phone' string is part of the SIP URI (default).

Parameter	Description
Use user=phone in From Header **[IsUserPhoneInFrom]**	Determines whether to add 'user=phone' string in the From header. ▪ **[0]** No = Doesn't use 'user=phone' string in From header (default). ▪ **[1]** Yes = 'user=phone' string is part of the From header.
Use Tel URI for Asserted Identity **[UseTelURIForAssertedID]**	Determines the format of the URI in the P-Asserted-Identity and P-Preferred-Identity headers. ▪ **[0]** Disable = 'sip:' (default). ▪ **[1]** Enable = 'tel:'.
Tel to IP No Answer Timeout **[IPAlertTimeout]**	Defines the time (in seconds) that the device waits for a 200 OK response from the called party (IP side) after sending an INVITE message. If the timer expires, the call is released. The valid range is 0 to 3600. The default value is 180.
Enable Remote Party ID **[EnableRPIheader]**	Enables Remote-Party-ID (RPI) headers for calling and called numbers for Tel-to-IP calls. ▪ **[0]** Disable (default). ▪ **[1]** Enable = RPI headers are generated in SIP INVITE messages for both called and calling numbers.
Add Number Plan and Type to RPI Header **[AddTON2RPI]**	Determines whether the TON/PLAN parameters are included in the Remote-Party-ID (RPID) header. ▪ **[0]** No ▪ **[1]** Yes (default) If RPID header is enabled (EnableRPIHeader = 1) and AddTON2RPI = 1, it's possible to configure the calling and called number type and number plan using the Number Manipulation tables for Tel-to-IP calls.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Enable History-Info Header
[EnableHistoryInfo]</td><td>Enables usage of the History-Info header.
▪ **[0]** Disable = Disable (default)
▪ **[1]** Enable = Enable
User Agent Client (UAC) Behavior:
▪ Initial request: The History-Info header is equal to the Request URI. If a PSTN Redirect number is received, it is added as an additional History-Info header with an appropriate reason.
▪ Upon receiving the final failure response, the device copies the History-Info as is, adds the reason of the failure response to the last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows:
1. Q.850 Reason
2. SIP Reason
3. SIP Response code
▪ Upon receiving the final response (success or failure), the device searches for a Redirect reason in the History-Info (i.e., 3xx/4xx SIP reason). If found, it is passed to ISDN according to the following table:
<table>
<tr><th>SIP Reason Code</th><th>ISDN Redirecting Reason</th></tr>
<tr><td>302 - Moved Temporarily</td><td>Call Forward Universal (CFU)</td></tr>
<tr><td>408 - Request Timeout</td><td rowspan="3">Call Forward No Answer (CFNA)</td></tr>
<tr><td>480 - Temporarily Unavailable</td></tr>
<tr><td>487 - Request Terminated</td></tr>
<tr><td>486 - Busy Here</td><td rowspan="2">Call Forward Busy (CFB)</td></tr>
<tr><td>600 - Busy Everywhere</td></tr>
</table>
▪ If history reason is a Q.850 reason, it is translated to the SIP reason (according to the SIP-ISDN tables) and then to ISDN Redirect reason according to the table above.
User Agent Server (UAS) Behavior:
▪ The History-Info header is sent only in the final response.
▪ Upon receiving a request with History-Info, the UAS checks the policy in the request. If 'session', 'header', or 'history' policy tag is found, the (final) response is sent without History-Info; otherwise, it is copied from the request.</td></tr>
<tr><td>Use Source Number as Display Name
[UseSourceNumberAsDisplayName]</td><td>Determines the use of Tel Source Number and Display Name for Tel-to-IP calls.
▪ **[0]** No = If a Tel Display Name is received, the Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name. If no Display Name is received from the Tel side, the IP Display Name remains empty (default).
▪ **[1]** Yes = If a Tel Display Name is received, the Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name. If no Display Name is received from the Tel side, the Tel Source Number is used as the IP Source Number and also as the IP Display Name.
▪ **[2]** Overwrite = The Tel Source Number is used as the IP Source Number and also as the IP Display Name (even if the received Tel Display Name is not empty).</td></tr>
</table>

Parameter	Description
Use Display Name as Source Number **[UseDisplayNameAsSourceNumber]**	Determines the use of Source Number and Display Name for IP-to-Tel calls. ▪ **[0]** No = If IP Display Name is received, the IP Source Number is used as the Tel Source Number and the IP Display Name is used as the Tel Display Name. If no Display Name is received from IP, the Tel Display Name remains empty (default). ▪ **[1]** Yes = If an IP Display Name is received, it is used as the Tel Source Number and also as the Tel Display Name, and Presentation is set to Allowed (0). If no Display Name is received from IP, the IP Source Number is used as the Tel Source Number and Presentation is set to Restricted (1). For example: When 'from: 100 <sip:200@201.202.203.204>' is received, the outgoing Source Number and Display Name are set to '100' and the Presentation is set to Allowed (0). When 'from: <sip:100@101.102.103.104>' is received, the outgoing Source Number is set to '100' and the Presentation is set to Restricted (1).
Enable Contact Restriction **[EnableContactRestriction]**	Determines whether the device sets the Contact header of outgoing INVITE requests to ‘anonymous’ for restricted calls. ▪ **[0]** = Disabled (default) ▪ **[1]** = Enabled
Play Ringback Tone to IP **[PlayRBTone2IP]**	Determines whether or not the device plays a ringback tone (RBT) to the IP side of the call (IP-to-Tel calls). ▪ **[0]** Don't Play = Ringback tone isn't played (default). ▪ **[1]** Play = Ringback tone is played after SIP 183 session progress response is sent. If configured to 1 ('Play') and EnableEarlyMedia = 1, the device plays a ringback tone according to the following: ▪ For CAS interfaces: the device opens a voice channel, sends a 183+SDP response, and then plays a ringback tone to IP. ▪ For ISDN interfaces: if a Progress or an Alert message with PI (1 or 8) is received from the ISDN, the device opens a voice channel, sends a 183+SDP or 180+SDP response, but doesn't play a ringback tone to IP. If PI (1 or 8) is received from the ISDN, the device assumes that ringback tone is played by the ISDN switch. Otherwise, the device plays a ringback tone to IP after receiving an Alert message from the ISDN. It sends a 180+SDP response, signaling to the calling party to open a voice channel to hear the played ringback tone. **Notes:** ▪ To enable the device to send a 183/180+SDP responses, set EnableEarlyMedia to 1. ▪ If EnableDigitDelivery = 1, the device doesn't play a ringback tone to IP and doesn't send 183 or 180+SDP responses.
Play Ringback Tone to Tel **[PlayRBTone2Tel]**	Determines the method used to play a ringback tone to the Tel side. It applies to all trunks that are not configured by the parameter PlayRBTone2Trunk. Similar description as the parameter PlayRBTone2Trunk. ▪ **[0]** Don't Play = Ringback tone isn't played. ▪ **[1]** Play Local = Ringback tone is played to the Tel side of the call when 180/183 response is received.

Parameter	Description
	▪ **[2]** Play According to Early Media = Ringback tone is played to the Tel side of the call if no SDP is received in 180/183 responses. If 180/183 with SDP message is received, the device cuts through the voice channel and doesn't play ringback tone (default).
Use Tgrp Information **[UseSIPTgrp]**	Determines whether the SIP 'tgrp' parameter, which specifies the Trunk Group to which the call belongs is used, according to RFC 4904. For example: INVITE sip::+16305550100;tgrp=1;trunk-context=example.com@10.1.0.3;user=phone SIP/2.0 ▪ **[0]** Disable = The 'tgrp' parameter isn't used (default). ▪ **[1]** Send Only = The Trunk Group number is added to the 'tgrp' parameter value in the Contact header of outgoing SIP messages. If a Trunk Group number is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored. ▪ **[2]** Send and Receive = The functionality of outgoing SIP messages is identical to the functionality described in option (1). In addition, for incoming SIP messages, if the Request-URI includes a 'tgrp' parameter, the device routes the call according to that value (if possible). If the Contact header includes a 'tgrp' parameter, it is copied to the corresponding outgoing messages in that dialog.
Enable GRUU **[EnableGRUU]**	Determines whether the Globally Routable User Agent URIs (GRUU) mechanism is used. ▪ **[0]** Disable = Disable (default) ▪ **[1]** Enable = Enable The device obtains a GRUU by generating a normal REGISTER request. This request contains a Supported header with the value 'gruu'. The device includes a '+sip.instance' Contact header parameter for each contact for which the GRUU is desired. This Contact parameter contains a globally unique ID that identifies the device instance. The global unique ID is as follows: ▪ If registration is per endpoint (AuthenticationMode=0), it is the MAC address of the device concatenated with the phone number of the endpoint. ▪ If the registration is per device (AuthenticationMode=1) it is only the MAC address. ▪ When the User Information mechanism is used, the globally unique ID is the MAC address concatenated with the phone number of the endpoint (defined in the User-Info file). If the Registrar/Proxy supports GRUU, the REGISTER responses contain the 'gruu' parameter in each Contact header field. The Registrar/Proxy provides the same GRUU for the same AOR and instance-id in case of sending REGISTER again after expiration of the registration. The device places the GRUU in any header field which contains a URI. It uses the GRUU in the following messages: INVITE requests, 2xx responses to INVITE, SUBSCRIBE requests, 2xx responses to SUBSCRIBE, NOTIFY requests, REFER requests, and 2xx responses to REFER. **Note:** If the GRUU contains the 'opaque' URI parameter, the device obtains the AOR for the user by stripping the parameter. The resulting URI is the AOR.

Parameter	Description
	For example: AOR: sip:alice@example.com GRUU: sip:alice@example.com;opaque="kjh29x97us97d"
User-Agent Information **[UserAgentDisplayInfo]**	Defines the string that is used in the SIP request header User-Agent and SIP response header Server. If not configured, the default string 'AudioCodes product-name s/w-version' is used (e.g., User-Agent: Audiocodes-Sip-Gateway-Mediant 2000/v.5.40.010.006). When configured, the string 'UserAgentDisplayInfo s/w-version' is used (e.g., User-Agent: MyNewOEM/v.5.40.010.006). Note that the version number can't be modified. The maximum string length is 50 characters.
SDP Session Owner **[SIPSDPSessionOwner]**	Determines the value of the Owner line ('o' field) in outgoing SDP messages. The valid range is a string of up to 39 characters. The default value is 'AudiocodesGW'. For example: o=AudiocodesGW 1145023829 1145023705 IN IP4 10.33.4.126
Play Busy Tone to Tel **[PlayBusyTone2ISDN]**	Enables the device to play a busy or reorder tone to the PSTN after a Tel-to-IP call is released. ▪ **[0]** Don't Play = Immediately sends an ISDN Disconnect message (default). ▪ **[1]** Play when Disconnecting = Sends an ISDN Disconnect message with PI = 8 and plays a busy or reorder tone to the PSTN (depending on the release cause). ▪ **[2]** Play before Disconnect = Delays the sending of an ISDN Disconnect message for a user-defined time (configured by the TimeForReorderTone parameter) and plays a busy or reorder tone to the PSTN. Applicable only if the call is released from the IP [Busy Here (486) or Not Found (404)] before it reaches the Connect state; otherwise, the Disconnect message is sent immediately and no tones are played.
Subject **[SIPSubject]**	Defines the value of the Subject header in outgoing INVITE messages. If not specified, the Subject header isn't included (default). The maximum length is up to 50 characters.
Multiple Packetization Time Format **[MultiPtimeFormat]**	Determines whether the 'mptime' attribute is included in the outgoing SDP. ▪ **[0]** None = Disabled (default) ▪ **[1]** PacketCable = includes the 'mptime' attribute in the outgoing SDP -- PacketCable-defined format The 'mptime' attribute enables the device to define a separate Packetization period for each negotiated coder in the SDP. The 'mptime' attribute is only included if this parameter is enabled, even if the remote side includes it in the SDP offer. Upon receipt, each coder receives its 'ptime' value in the following precedence: from 'mptime' attribute, from 'ptime' attribute, and then from default value.
Enable Semi-Attended Transfer **[EnableSemiAttendedTransfer]**	Determines the device behavior when Transfer is initiated while in Alerting state. ▪ **[0]** Disable = Send REFER with Replaces (default). ▪ **[1]** Enable = Send CANCEL, and after a 487 response is received, send REFER without Replaces.

Parameter	Description
3xx Behavior **[3xxBehavior]**	Determines the device's behavior regarding call identifiers when a 3xx response is received for an outgoing INVITE request. The device can either use the same call identifiers (Call-ID, Branch, To, and From tags) or change them in the new initiated INVITE. ▪ **[0]** Forward = Use different call identifiers for a redirected INVITE message (default). ▪ **[1]** Redirect = Use the same call identifiers.
Enable P-Charging Vector **[EnablePChargingVector]**	Enables the addition of a P-Charging-Vector header to all outgoing INVITE messages. ▪ **[0]** Disable = Disable (default) ▪ **[1]** Enable = Enable
Enable VoiceMail URI **[EnableVMURI]**	Enables or disables the interworking of target and cause for redirection from Tel to IP and vice versa, according to RFC 4468. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Enable = Enable Upon receipt of an ISDN SETUP message with redirect values, the device maps the Redirect phone number to the SIP 'target' parameter and the Redirect number reason to the SIP 'cause' parameter in the Request-URI. **Redirecting Reason >> SIP Response Code** Unknown >> 404 User busy >> 486 No reply >> 408 Deflection >> 487/480 Unconditional >> 302 Others >> 302 If the device receives a Request-URI that includes a 'target' and 'cause' parameter, the 'target' is mapped to the Redirect phone number and the 'cause' is mapped to Redirect number reason.
Retry-After Time **[RetryAfterTime]**	Determines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the device. The time range is 0 to 3,600. The default value is 0.
Enable P-Associated-URI Header **[EnablePAssociatedURIHeader]**	Determines the device usage of the P-Associated-URI header. This header can be received in 200 OK responses to REGISTER requests. When enabled, the first URI in the P-Associated-URI header is used in subsequent requests as the From / P-Asserted-Id headers value. ▪ **[0]** Disable (default). ▪ **[1]** Enable. **Note:** P-Associated-URIs in registration responses is handled only if the device is registered per endpoint (using the User Information file).
Source Number Preference **[SourceNumberPreference]**	Determines the SIP header used to determine the Source Number in incoming INVITE messages. ▪ **“”** (empty string) = Use device's internal logic for header preference (default). ▪ **“FROM”** = Use the Source Number received in the From header.

Parameter	Description
	The valid range is a string of up to 10 characters. The default is an empty string.
Forking Handling Mode **[ForkingHandlingMode]**	Determines how the device reacts to forking of outgoing INVITE messages by the Proxy. ▪ **[0]** Sequential handling = The device opens a voice stream toward the first 18x SIP response that includes an SDP, and disregards any 18x response with an SDP received thereafter (default). ▪ **[1]** Parallel handling = The device opens a voice stream toward the first 18x SIP response that includes an SDP, and re-opens the stream toward any subsequent 18x responses with an SDP. **Note:** Regardless of the ForkingHandlingMode value, once a SIP 200 OK response is received, the device uses the RTP information and re-opens the voice stream, if necessary.
Enable Reason Header **[EnableReasonHeader]**	Enables / disables the usage of the SIP Reason header. ▪ **[0]** Disable. ▪ **[1]** Enable (default).
Retransmission Parameters	
SIP T1 Retransmission Timer [msec] **[SipT1Rtx]**	The time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message. The default is 500. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx. For example (assuming that SipT1Rtx = 500 and SipT2Rtx = 4000): ▪ The first retransmission is sent after 500 msec. ▪ The second retransmission is sent after 1000 (2*500) msec. ▪ The third retransmission is sent after 2000 (2*1000) msec. ▪ The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.
SIP T2 Retransmission Timer [msec] **[SipT2Rtx]**	The maximum interval (in msec) between retransmissions of SIP messages. The default is 4000. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.
SIP Maximum RTX **[SIPMaxRtx]**	Maximum number of UDP transmissions (first transmission plus retransmissions) of SIP messages. The range is 1 to 30. The default value is 7.

3.4.7.1.2 Proxy & Registration Parameters

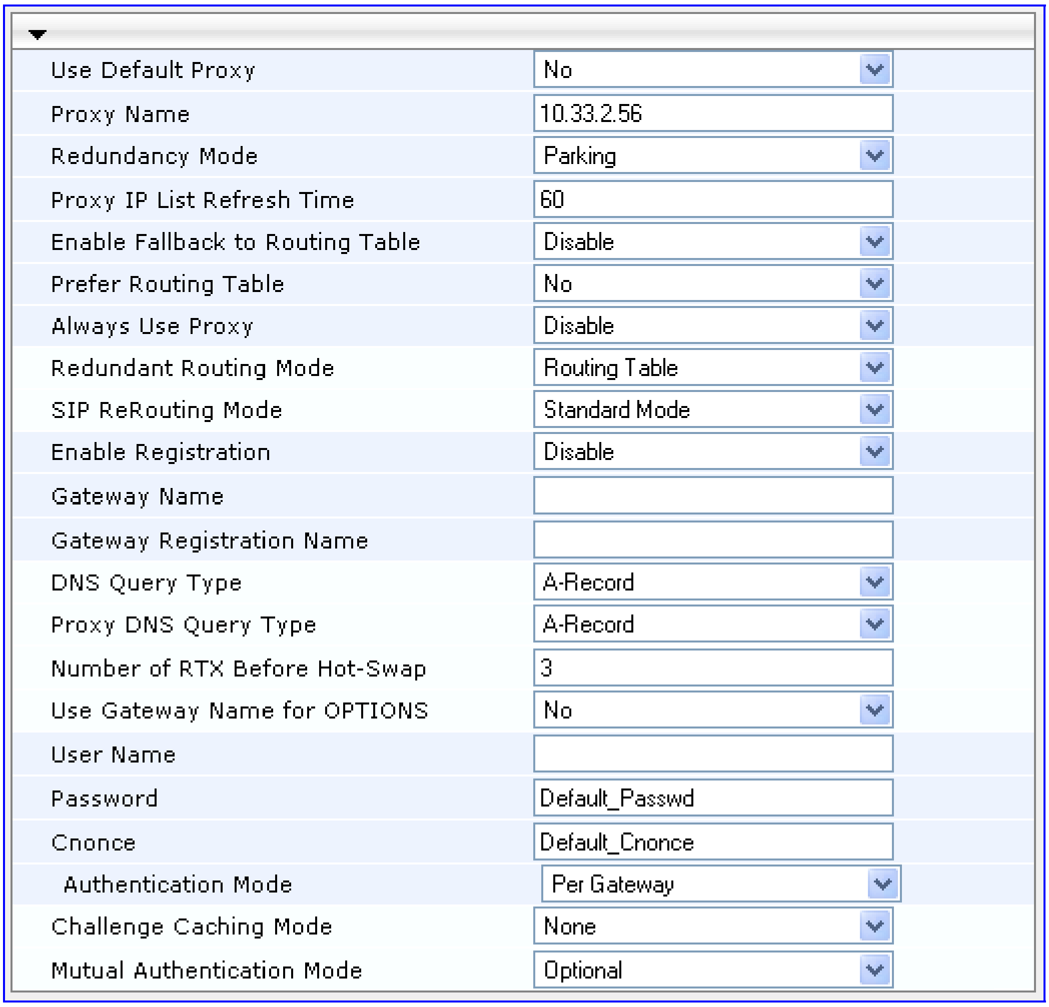
The 'Proxy & Registration' page allows you to configure parameters that are associated with Proxy and Registration.

> **Note:** To view whether the device or its endpoints have registered to a SIP Registrar/Proxy server, refer to Registration Status.

➢ To configure the Proxy & Registration parameters, take these 4 steps:

1. Open the 'Proxy & Registration' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **Proxy & Registration** page item).

Figure 3-60: Proxy & Registration Page



Use Default Proxy	No
Proxy Name	10.33.2.56
Redundancy Mode	Parking
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Always Use Proxy	Disable
Redundant Routing Mode	Routing Table
SIP ReRouting Mode	Standard Mode
Enable Registration	Disable
Gateway Name	
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Passwd
Cnonce	Default_Cnonce
Authentication Mode	Per Gateway
Challenge Caching Mode	None
Mutual Authentication Mode	Optional

2. Configure the Proxy and Registration parameters according to the following table.

3. Click the **Submit** button to save your changes, or click the **Register** or **Un-Register** buttons to save your changes and register / unregister to a Proxy / Registrar.

4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-31: Proxy & Registration Parameters

Parameter	Description
Proxy Parameters	
Use Default Proxy **[IsProxyUsed]**	Enables the use of a SIP Proxy server. ▪ **[0]** No = Proxy isn't used - the internal routing table is used instead (default). ▪ **[1]** Yes = Proxy is used. Parameters relevant to Proxy configuration are displayed. If you are using a Proxy server, enter the IP address of the Proxy server in the 'Proxy Sets table' (refer to "Proxy Sets Table" on page 141). If you are not using a Proxy server, you must configure the device's 'Tel to IP Routing' table (described in "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing' table if EnableSBC is set to 1 (refer to “Outbound IP Routing Table” on page 178).
Proxy Set Table (button)	Click the right-pointing arrow ➡ button to open the 'Proxy Sets Table' page to configure groups of proxy addresses. Alternatively, you can open this page from the **Proxy Sets Table** page item (refer to "Proxy Sets Table" on page 141 for a description of this page). **Note:** This button appears only if the 'Use Default Proxy' parameter is enabled.
Proxy Name **[ProxyName]**	Defines the Home Proxy Domain Name. If specified, the Proxy Name is used as the Request-URI in REGISTER, INVITE, and other SIP messages, and as the host part of the To header in INVITE messages. If not specified, the Proxy IP address is used instead. The value must be string of up to 49 characters.
Redundancy Mode **[ProxyRedundancyMode]**	Determines whether the device switches back to the primary Proxy after using a redundant Proxy. ▪ **[0]** Parking = device continues working with a redundant (now active) Proxy until the next failure, after which it works with the next redundant Proxy (default). ▪ **[1]** Homing = device always tries to work with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available). **Note:** To use ProxyRedundancyMode, enable Keep-alive with Proxy option (EnableProxyKeepAlive = 1 or 2).
Proxy IP List Refresh Time **[ProxyIPListRefreshTime]**	Defines the time interval (in seconds) between each Proxy IP list refresh. The range is 5 to 2,000,000. The default interval is 60.
Enable Fallback to Routing Table **[IsFallbackUsed]**	Determines whether the device falls back to the 'Tel to IP Routing' table (or 'Outbound IP Routing' table if EnableSBC is set to 1) for call routing when Proxy servers are unavailable. ▪ **[0]** Disable = Fallback is not used (default). ▪ **[1]** Enable = 'Tel to IP Routing' table (or 'Outbound IP Routing' table) is used when Proxy servers are unavailable. When the device falls back to its 'Tel to IP Routing' table (or 'Outbound IP Routing' table), the device continues scanning for a Proxy. When the device locates an active Proxy, it switches from

Parameter	Description
	internal routing back to Proxy routing. **Note:** To enable the redundant Proxies mechanism, set the parameter EnableProxyKeepAlive to 1 or 2.
Prefer Routing Table **[PreferRouteTable]**	Determines if the device's internal routing table takes precedence over a Proxy for routing calls. ▪ **[0]** No = Only a Proxy server is used to route calls (default). ▪ **[1]** Yes = The device checks the routing rules in the 'Tel to IP Routing' table (or 'Outbound IP Routing' table if EnableSBC is set to 1) for a match with the Tel-to-IP call. Only if a match is not found is a Proxy used.
Use Routing Table for Host Names and Profiles **[AlwaysUseRouteTable]**	Determines whether to use the device's internal routing table to obtain the URI host name and optionally, an IP profile (per call), even if a Proxy server is used. ▪ **[0]** Disable = Don't use internal routing table (default). ▪ **[1]** Enable = Use the 'Tel to IP Routing' table (or 'Outbound IP Routing' table if EnableSBC is set to 1). **Notes:** ▪ This parameter appears only if the 'Use Default Proxy' parameter is enabled. ▪ The domain name is used instead of a Proxy name or IP address in the INVITE SIP URI.
Always Use Proxy **[AlwaysSendToProxy]**	Determines whether the device sends SIP messages and responses through a Proxy server. ▪ **[0]** Disable = Use standard SIP routing rules (default). ▪ **[1]** Enable = All SIP messages and responses are sent to a Proxy server. **Note:** Applicable only if Proxy server is used (i.e., the parameter IsProxyUsed is set to 1).
Redundant Routing Mode **[RedundantRoutingMode]**	Determines the type of redundant routing mechanism to implement when a call can’t be completed using the main route. ▪ **[0]** Disable = No redundant routing is used. If the call can’t be completed using the main route (using the active Proxy or the first matching rule in the internal routing table), the call is disconnected. ▪ **[1]** Routing Table = Internal routing table is used to locate a redundant route (default). ▪ **[2]** Proxy = Proxy list is used to locate a redundant route.
SIP ReRouting Mode **[SIPReroutingMode]**	Determines the routing mode after a call redirection (i.e., a 3xx SIP response is received) or transfer (i.e., a SIP REFER request is received). ▪ **[0]** Standard = INVITE messages that are generated as a result of Transfer or Redirect are sent directly to the URI, according to the Refer-To header in the REFER message or Contact header in the 3xx response (default). ▪ **[1]** Proxy = Sends a new INVITE to the Proxy. **Note:** Applicable only if a Proxy server is used and the parameter AlwaysSendtoProxy is set to 0.

Parameter	Description
	▪ **[2]** Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination. **Notes:** ▪ When this parameter is set to [1] and the INVITE sent to the Proxy fails, the device re-routes the call according to the Standard mode [0]. ▪ When this parameter is set to [2] and the INVITE fails, the device re-routes the call according to the Standard mode [0]. If DNS resolution fails, the device attempts to route the call to the Proxy. If routing to the Proxy also fails, the Redirect / Transfer request is rejected. ▪ When this parameter is set to [2], the XferPrefix parameter can be used to define different routing rules for redirected calls. ▪ This parameter is disregarded if the parameter AlwaysSendToProxy is set to 1.
Proxy / Registrar Registration Parameters (**Note:** The proxy and registrar parameter fields appear only if 'Enable Registration' is enabled.)	
Enable Registration **[IsRegisterNeeded]**	Enables the device to register to a Proxy / Registrar server. ▪ **[0]** Disable = device doesn't register to Proxy / Registrar (default) server. ▪ **[1]** Enable = device registers to Proxy / Registrar server when the device is powered up and at every user-defined interval (configured by the parameter RegistrationTime). **Note:** The device sends a REGISTER request for each channel or for the entire device (according to the AuthenticationMode parameter).
Registrar Name **[RegistrarName]**	Registrar domain name. If specified, the name is used as the Request-URI in REGISTER messages. If it isn't specified (default), the Registrar IP address, or Proxy name or IP address is used instead. The valid range is up to 49 characters.
Registrar IP Address **[RegistrarIP]**	The IP address (or FQDN) and optionally, port number of the SIP Registrar server. The IP address is in dotted-decimal notation, e.g., 201.10.8.1:<5080>. **Notes:** ▪ If not specified, the REGISTER request is sent to the primary Proxy server. ▪ When a port number is specified, DNS NAPTR/SRV queries aren't performed, even if DNSQueryType is set to 1 or 2. ▪ If the RegistrarIP is set to an FQDN and is resolved to multiple addresses, the device also provides real-time switching (hotswap mode) between different Registrar IP addresses (IsProxyHotSwap is set to 1). If the first Registrar doesn't respond to the REGISTER message, the same REGISTER message is sent immediately to the next Proxy. EnableProxyKeepAlive must be set to 0 for this logic to apply. ▪ When a specific Transport Type is defined using RegistrarTransportType, a DNS NAPTR query is not performed even if DNSQueryType is set to 2.

Parameter	Description
Registrar Transport Type **[RegistrarTransportType]**	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the Registrar. ▪ **[-1]** Not Configured (default) ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When set to 'Not Configured', the value of the parameter SIPTransportType is used.
Registration Time **[RegistrationTime]**	Defines the time interval (in seconds) for registering to a Proxy server. The value is used in the Expires header. In addition, this parameter defines the time interval between Keep-Alive messages when the parameter EnableProxyKeepAlive is set to 2 (REGISTER). Typically, the device registers every 3,600 sec (i.e., one hour). The device resumes registration according to the parameter RegistrationTimeDivider. The valid range is 10 to 2,000,000. The default value is 180.
Re-registration Timing [%] **[RegistrationTimeDivider]**	Defines the re-registration timing (in percentage). The timing is a percentage of the re-register timing set by the Registrar server. The valid range is 50 to 100. The default value is 50. For example: If RegistrationTimeDivider is 70% and Registration Expires time is 3600, the device re-sends its registration request after 3600 x 70% = 2520 sec. **Note**: This parameter may be overriden if the parameter RegistrationTimeThreshold is greater than 0 (refer to the description of RegistrationTimeThreshold).
Registration Retry Time **[RegistrationRetryTime]**	Defines the time interval (in seconds) after which a Registration request is resent if registration fails with a 4xx response or if there is no response from the Proxy/Registrar server. The default is 30 seconds. The range is 10 to 3600.
Registration Time Threshold **[RegistrationTimeThreshold]**	Defines a threshold (in seconds) for re-registration timing. If this parameter is greater than 0, but lower than the computed re-registration timing (according to the parameter RegistrationTimeDivider), the re-registration timing is set to the following: timing set by the Registration server in the Expires header minus the value of the parameter RegistrationTimeThreshold. The valid range is 0 to 2,000,000. The default value is 0.
Re-register On INVITE Failure **[RegisterOnInviteFailure]**	Enables immediate re-registration if a failure response is received for an INVITE request sent by the device. ▪ **[0]** Disable = Disabled (default) ▪ **[1]** Enable = Enabled
ReRegister On Connection Failure **[ReRegisterOnConnectionFailure]**	Enables the device to perform SIP Re-Registration upon TCP/TLS connection failure. ▪ **[0]** Disable (default). ▪ **[1]** Enable.

Parameter	Description
Miscellaneous parameters	
Gateway Name **[SIPGatewayName]**	Assigns a name to the device (e.g., 'gateway1.com'). Ensure that the name you choose is the one with which the Proxy is configured to identify the device. **Note:** If specified, the device name is used as the host part of the SIP URI in the From header. If not specified, the device's IP address is used instead (default).
Gateway Registration Name **[GWRegistrationName]**	Defines the user name that is used in the From and To headers in REGISTER messages. If no value is specified (default) for this parameter, the UserName parameter is used instead. **Note:** This parameter is applicable only for single registration per device (i.e., AuthenticationMode is set to 1). When the device registers each channel separately (i.e., AuthenticationMode is set to 0), the user name is set to the channel's phone number.
DNS Query Type **[DNSQueryType]**	Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the Contact and Record-Route headers. ▪ **[0]** A-Record = A-Record (default) ▪ **[1]** SRV = SRV ▪ **[2]** NAPTR = NAPTR If set to A-Record [0], no NAPTR or SRV queries are performed. If set to SRV [1] and the Proxy / Registrar IP address parameter, Contact / Record-Route headers, or IP address defined in the Routing tables contains a domain name, an SRV query is performed. The device uses the first host name received from the SRV query. The device then performs a DNS A-record query for the host name to locate an IP address. If set to NAPTR [2], an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type. If the Proxy / Registrar IP address parameter, the domain name in the Contact / Record-Route headers, or the IP address defined in the Routing tables contains a domain name with port definition, the device performs a regular DNS A-record query. If a specific Transport Type is defined, a NAPTR query is not performed. **Note:** To enable NAPTR/SRV queries for Proxy servers only, use the parameter ProxyDNSQueryType.
Proxy DNS Query Type **[ProxyDNSQueryType]**	Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers. ▪ **[0]** A-Record = A-Record (default) ▪ **[1]** SRV = SRV ▪ **[2]** NAPTR = NAPTR If set to A-Record [0], no NAPTR or SRV queries are performed. If set to SRV [1] and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com),

Parameter	Description
	an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The device then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names, and the A-record queries return two IP addresses each, no additional searches are performed. If set to NAPTR [2], an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type. If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the device performs a regular DNS A-record query. If a specific Transport Type is defined, a NAPTR query is not performed. **Note:** When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.
Number of RTX Before Hot-Swap **[HotSwapRtx]**	Number of retransmitted INVITE/REGISTER messages before the call is routed (hot swap) to another Proxy/Registrar. The valid range is 1 to 30. The default value is 3. **Note:** This parameter is also used for alternative routing using the 'Tel to IP Routing' table (or 'Outbound IP Routing' table if EnableSBC is set to 1). If a domain name in the table is resolved into two IP addresses, and if there is no response for HotSwapRtx retransmissions to the INVITE message that is sent to the first IP address, the device immediately initiates a call to the second IP address.
Use Gateway Name for OPTIONS **[UseGatewayNameForOptions]**	Determines whether the device uses its IP address or gateway name in keep-alive SIP OPTIONS messages. ▪ **[0]** No = Use the device's IP address in keep-alive OPTIONS messages (default). ▪ **[1]** Yes = Use 'Gateway Name' (SIPGatewayName) in keep-alive OPTIONS messages. The OPTIONS Request-URI host part contains either the device's IP address or a string defined by the parameter SIPGatewayName. The device uses the OPTIONS request as a keep-alive message to its primary and redundant Proxies (i.e., the parameter EnableProxyKeepAlive is set to 1).
User Name **[UserName]**	User name used for Registration and Basic/Digest authentication with a Proxy / Registrar server. The parameter doesn't have a default value (empty string). **Note:** Applicable only if single device registration is used (i.e., Authentication Mode is set to Authentication Per gateway).
Password **[Password]**	The password used for Basic/Digest authentication with a Proxy / Registrar server. A single password is used for all device ports. The default is 'Default_Passwd'.

Parameter	Description
Cnonce **[Cnonce]**	Cnonce string used by the SIP server and client to provide mutual authentication. (Free format, i.e., 'Cnonce = 0a4f113b'). The default is 'Default_Cnonce'.
Authentication Mode **[AuthenticationMode]**	Determines the device's registration and authentication method. ▪ **[0]** Per Endpoint = Registration and Authentication separately for each B-channel. ▪ **[1]** Per Gateway = Single Registration and Authentication for the entire device (default). Single Registration and Authentication (Authentication Mode = 1) is usually defined for and digital modules.
Set Out-Of-Service On Registration Failure **[OOSOnRegistrationFail]**	Enables setting a , trunk, or the entire device (i.e., all endpoints) to out-of-service if registration fails. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enabled. If the registration is per Endpoint (i.e., AuthenticationMode is set to 0) or Account (refer to "Configuring the Trunk Group Settings" on page 197) and a specific endpoint/Account registration fails (SIP 4xx or no response), then that endpoint is set to out-of-service until a success response is received in a subsequent registration request. When the registration is per the entire device (i.e., AuthenticationMode is set to 1) and registration fails, all endpoints are set to out-of-service. If all the Accounts of a specific Trunk Group fail registration and if the Trunk Group comprises a complete trunk, then the trunk is set to out-of-service.
Challenge Caching Mode **[SIPChallengeCachingMode]**	Determines the mode for Challenge Caching, which reduces the number of SIP messages transmitted through the network. The first request to the Proxy is sent without authorization. The Proxy sends a 401/407 response with a challenge. This response is saved for further uses. A new request is resent with the appropriate credentials. Subsequent requests to the Proxy are automatically sent with credentials (calculated from the saved challenge). If the Proxy doesn't accept the new request and sends another challenge, the old challenge is replaced with the new one. ▪ **[0]** None = Challenges are not cached. Every new request is sent without preliminary authorization. If the request is challenged, a new request with authorization data is sent (default) ▪ **[1]** INVITE Only = Challenges issued for INVITE requests are cached. This prevents a mixture of REGISTER and INVITE authorizations. ▪ **[2]** Full = Caches all challenges from the proxies. **Note**: Challenge Caching is used with all proxies and not only with the active one.
Mutual Authentication Mode **[MutualAuthenticationMode]**	Determines the device's mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used. ▪ **[0]** Optional = Incoming requests that don't include AKA authentication information are accepted (default). ▪ **[1]** Mandatory = Incoming requests that don't include AKA authentication information are rejected.

3.4.7.1.3 Proxy Sets Table

The 'Proxy Sets Table' page allows you to define *Proxy Sets*. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). You can define up to six Proxy Sets, each having a unique ID number and each containing up to five Proxy server addresses. For each Proxy server address, you can define the transport type (i.e., UDP, TCP, or TLS). In addition, Proxy load balancing and redundancy mechanisms can be applied per Proxy Set (if a Proxy Set contains more than one Proxy address).

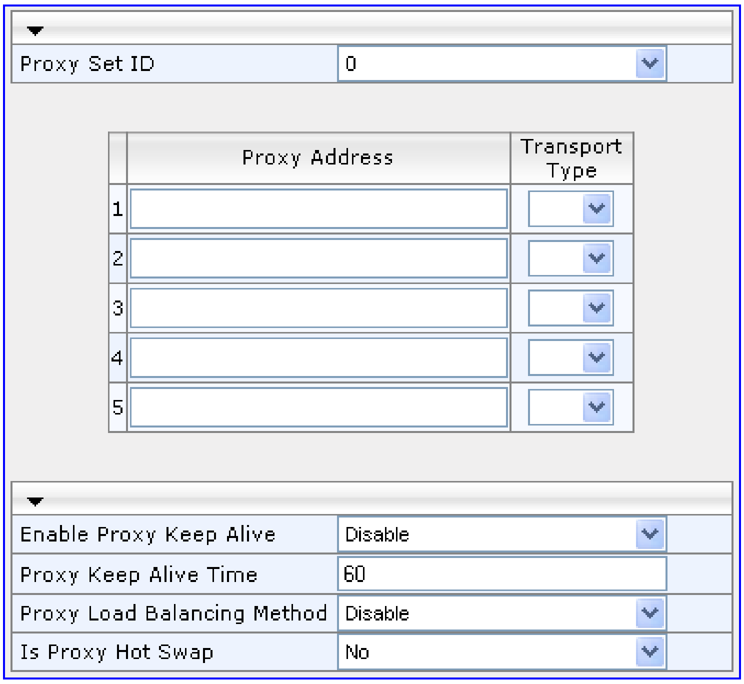
Proxy Sets can later be assigned to IP Groups of type SERVER only (refer to "Configuring the IP Groups" on page 201). When the device sends an INVITE message to an IP Group, it is sent to the IP address/domain name defined for the Proxy Set that is associated with the specific IP Group. In other words, the Proxy Set represents the **destination** of the call. Typically, for IP-to-IP call routing, at least two Proxy Sets are defined for call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.

Note: You can also configure the Proxy Sets table using the *ini* file table parameters ProxyIP and ProxySet (refer to "SIP Configuration Parameters" on page 284).

➢ To add Proxy servers and configure Proxy parameters, take these 5 steps:

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **Proxy Sets Table** page item).

Figure 3-61: Proxy Sets Table Page



Proxy Set ID	0

	Proxy Address	Transport Type
1		
2		
3		
4		
5		

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No

2. From the Proxy Set ID drop-down list, select an ID for the desired group.

3. Configure the Proxy parameters according to the following table.

4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-32: Proxy Sets Table Parameters

Parameter	Description
Proxy Set ID	The Proxy Set identification number. The valid range is 0 to 5 (i.e., up to 6 Proxy Set ID's can be configured). The Proxy Set ID #0 is used as the default Proxy Set, and if defined is backward compatible to the list of Proxies from earlier releases. **Note:** Although not recommended, you can use both default Proxy Set (ID #0) and IP Groups for call routing. For example, on the 'Trunk Group Settings' page (refer to "Configuring the Trunk Group Settings" on page 197), you can configure a Serving IP Group to where you want to route specific Trunk Group's channels, while all other device channels use the default Proxy Set. At the same, you can also use IP Groups in the 'Tel to IP Routing' table (refer to "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing' table if EnableSBC is set to 1 (refer to “Outbound IP Routing Table” on page 178) to configure the default Proxy Set if the parameter PreferRouteTable is set to 1. To summarize, if the default Proxy Set is used, the INVITE message is sent according to the following preferences: ▪ To the Trunk Group's Serving IP Group ID, as defined in the 'Trunk Group Settings' table. ▪ According to the 'Tel to IP Routing' table (or 'Outbound IP Routing' table if EnableSBC is set to 1), if the parameter PreferRouteTable is set to 1. ▪ To the default Proxy. Typically, when IP Groups are used, there is no need to use the default Proxy, and all routing and registration rules can be configured using IP Groups and the Account tables (refer to "Configuring the Account Table" on page 204).
Proxy Address	The IP address (and optionally port number) of the Proxy server. Up to five IP addresses can be configured per Proxy Set. Enter the IP address as an FQDN or in dotted-decimal notation (e.g., 201.10.8.1). You can also specify the selected port in the format: <IP address>:<port>. If you enable Proxy Redundancy (by setting the parameter EnableProxyKeepAlive to 1 or 2), the device can operate with multiple Proxy servers. If there is no response from the first (*primary*) Proxy defined in the list, the device attempts to communicate with the other (*redundant*) Proxies in the list. When a redundant Proxy is located, the device either continues operating with it until the next failure occurs, or reverts to the primary Proxy (refer to the parameter ProxyRedundancyMode). If none of the Proxy servers respond, the device goes over the list again. The device also provides real-time switching (Hot-Swap mode) between the primary and redundant proxies (refer to the parameter IsProxyHotSwap). If the first Proxy doesn't respond to the INVITE message, the same INVITE message is immediately sent to the next Proxy in the list. The same logic applies to REGISTER messages (if RegistrarIP is not defined).

Parameter	Description
	Notes: - If EnableProxyKeepAlive is set to 1 or 2, the device monitors the connection with the Proxies by using keep-alive messages (OPTIONS or REGISTER). - To use Proxy Redundancy, you must specify one or more redundant Proxies. - When a port number is specified (e.g., domain.com:5080), DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2.
Transport Type	The transport type per Proxy server. - **[0]** UDP - **[1]** TCP - **[2]** TLS - **[-1]** = Undefined **Note:** If no transport type is selected, the value of the global parameter SIPTransportType is used (refer to "SIP General Parameters" on page 121).
Proxy Load Balancing Method **[ProxyLoadBalancingMethod]**	Enables the Proxy Load Balancing mechanism per Proxy Set ID. - **[0]** Disable = Load Balancing is disabled (default). - **[1]** Round Robin = Round Robin. - **[2]** Random Weights = Random Weights. When the Round Robin algorithm is used, a list of all possible Proxy IP addresses is compiled. This list includes all IP addresses per Proxy Set, after necessary DNS resolutions (including NAPTR and SRV, if configured). After this list is compiled, the Proxy Keep-Alive mechanism (according to parameters EnableProxyKeepAlive and ProxyKeepAliveTime) tags each entry as 'offline' or 'online'. Load balancing is only performed on Proxy servers that are tagged as 'online'. All outgoing messages are equally distributed across the list of IP addresses. REGISTER messages are also distributed unless a RegistrarIP is configured. The IP addresses list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again. When the Random Weights algorithm is used, the outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server by using SRV records. The device sends the requests in such a fashion that each Proxy receives a percentage of the requests according to its' assigned weight. A single FQDN should be configured as a Proxy IP address. The Random Weights Load Balancing is not used in the following scenarios: - The Proxy Set includes more than one Proxy IP address. - The only Proxy defined is an IP address and not an FQDN. - SRV is not enabled (DNSQueryType). - The SRV response includes several records with a different Priority value.

Parameter	Description
Enable Proxy Keep Alive **[EnableProxyKeepAlive]**	Determines whether Keep-Alive with the Proxy is enabled or disabled. This parameter is configured per Proxy Set. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Using OPTIONS = Enables Keep-Alive with Proxy using OPTIONS. ▪ **[2]** Using REGISTER = Enable Keep-Alive with Proxy using REGISTER. If set to 'Using OPTIONS', the SIP OPTIONS message is sent every user-defined interval, as configured by the parameter ProxyKeepAliveTime. If set to 'Using REGISTER', the SIP REGISTER message is sent every user-defined interval, as configured by the parameter RegistrationTime. Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is communicating correctly. **Notes:** ▪ For Survivability mode for USER-type IP Groups, this parameter must be enabled (1 or 2). ▪ This parameter must be set to 'Using OPTIONS' when Proxy redundancy is used. ▪ When this parameter is set to 'Using REGISTER', the homing redundancy mode is disabled. ▪ When the active proxy doesn't respond to INVITE messages sent by the device, the proxy is tagged as 'offline'. The behavior is similar to a Keep-Alive (OPTIONS or REGISTER) failure.
Proxy Keep Alive Time **[ProxyKeepAliveTime]**	Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages. This parameter is configured per Proxy Set. The valid range is 5 to 2,000,000. The default value is 60. **Note:** This parameter is applicable only if the parameter EnableProxyKeepAlive is set to 1 (OPTIONS). When the parameter EnableProxyKeepAlive is set to 2 (REGISTER), the time interval between Keep-Alive messages is determined by the parameter RegistrationTime.
Is Proxy Hot-Swap **[IsProxyHotSwap]**	Enables the Proxy Hot-Swap redundancy mode per Proxy Set. ▪ **[0]** No = Disabled (default). ▪ **[1]** Yes = Proxy Hot-Swap mode is enabled. If Proxy Hot-Swap is enabled, the SIP INVITE/REGISTER message is initially sent to the first Proxy/Registrar server. If there is no response from the first Proxy/Registrar server after a specific number of retransmissions (configured by the parameter HotSwapRtx), the INVITE/REGISTER message is resent to the next redundant Proxy/Registrar server.

3.4.7.1.4 Coders

The 'Coders' page allows you to configure up to five coders (and their attributes) for the device. The first coder in the list is the highest priority coder and is used by the device whenever possible. If the far-end device cannot use the first coder, the device attempts to use the next coder in the list, and so forth.

Notes:

- The device always uses the packetization time requested by the remote side for sending RTP packets.
- For an explanation on V.152 support (and implementation of T.38 and VBD coders), refer to "Supporting V.152 Implementation" on page 357.
- You can also configure the Coders table using the *ini* file table parameter CoderName (refer to "SIP Configuration Parameters" on page 284).

The coders supported by the device are listed in the table below:

Table 3-33: Supported Coders

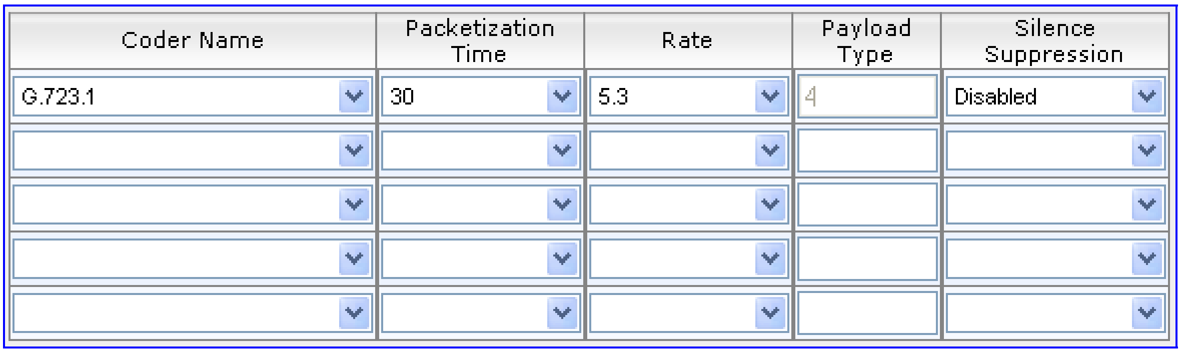
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711 A-law **[g711Alaw64k]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Always 8	▪ Disable **[0]** ▪ Enable **[1]**
G.711 U-law **[g711Ulaw64k]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Always 0	▪ Disable **[0]** ▪ Enable **[1]**
EG.711 A-law **[eg711Alaw]**	10 (default), 20, 30	Always 64	Dynamic (0-120)	N/A
EG.711 U-law **[eg711Ulaw]**	10 (default), 20, 30	Always 64	Dynamic (0-120)	N/A
G.729 **[g729]**	10, 20 (default), 30, 40, 50, 60, 80, 100	Always 8	Always 18	▪ Disable **[0]** ▪ Enable **[1]** ▪ Enable w/o Adaptations **[2]**
G.723.1 **[g7231]**	30 (default), 60, 90, 120	5.3 **[0]**, 6.3 **[1]** (default)	Always 4	▪ Disable **[0]** ▪ Enable **[1]**
G.726 **[g726]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	16 **[0]**, 24 **[1]**, 32 **[2]** (default) 40 **[3]**	Dynamic (0-120)	▪ Disable **[0]** ▪ Enable **[1]**
GSM-FR **[gsmFullRate]**	20 (default), 40, 60, 80	Always 13	Always 3	▪ Disable **[0]** ▪ Enable **[1]**
GSM-EFR **[gsmEnhancedFullRate]**	0, 20 (default), 30, 40, 50, 60, 80, 100	12.2	Dynamic (0-120)	▪ Disable **[0]** ▪ Enable **[1]**
AMR **[Amr]**	20 (default)	4.75 [0], 5.15 [1], 5.90 [2], 6.70 [3], 7.40 [4], 7.95 [5], 10.2 [6], 12.2 [7] (default)	Dynamic (0-120)	▪ Disable **[0]** ▪ Enable **[1]**

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
EVRC **[Evrc]**	20 (default), 40,60, 80, 100	Variable [0] (default), 1/8 [1], 1/2 [3], Full [4]	Dynamic (0-120)	▪ Disable **[0]** ▪ Enable **[1]**
iLBC **[iLBC]**	20 (default), 40, 60, 80, 100, 120	15 (default)	Dynamic (0-120)	▪ Disable **[0]** ▪ Enable **[1]**
	30 (default), 60, 90, 120	13		
MS-GSM **[gsmMS]**	40 (default)	Always 13	Always 3	▪ Disable **[0]** ▪ Enable **[1]**
QCELP **[QCELP]**	20 (default), 40, 60, 80, 100, 120	Always 13	Always 12	▪ Disable **[0]** ▪ Enable **[1]**
Transparent **[Transparent]**	20 (default), 40, 60, 80, 100, 120	Always 64	Dynamic (0-120)	▪ Disable **[0]** ▪ Enable **[1]**
G.711A-law_VBD **[g711AlawVbd]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Dynamic (0-120)	N/A
G.711U-law_VBD **[g711UlawVbd]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Dynamic (0-120)	N/A
T.38 **[t38fax]**	N/A	N/A	N/A	N/A

➢ To configure the device's coders, take these 9 steps:

1. Open the 'Coders' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **Coders** page item).

Figure 3-62: Coders Page



Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.723.1	30	5.3	4	Disabled

2. From the 'Coder Name' drop-down list, select the coder you want to use. For the full list of available coders and their corresponding attributes, refer to the table below.

3. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the selected coder. The packetization time determines how many coder payloads are combined into a single RTP packet.

4. From the 'Rate' drop-down list, select the bit rate (in kbps) for the selected coder.

5. In the 'Payload Type' field, if the payload type for the selected coder is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified). The payload type identifies the format of the RTP payload.

6. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the selected coder.

7. Repeat steps 2 through 6 for the second to fifth optional coders.

8. Click the **Submit** button to save your changes.

9. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- Each coder (i.e., 'Coder Name') can appear only once.
- If packetization time and / or rate are not specified, the default value is applied.
- Only the packetization time of the first coder in the coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined.
- For G.729, it's also possible to select silence suppression without adaptations.
- If the coder G.729 is selected and silence suppression is disabled (for this coder), the device includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is enabled or set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode).

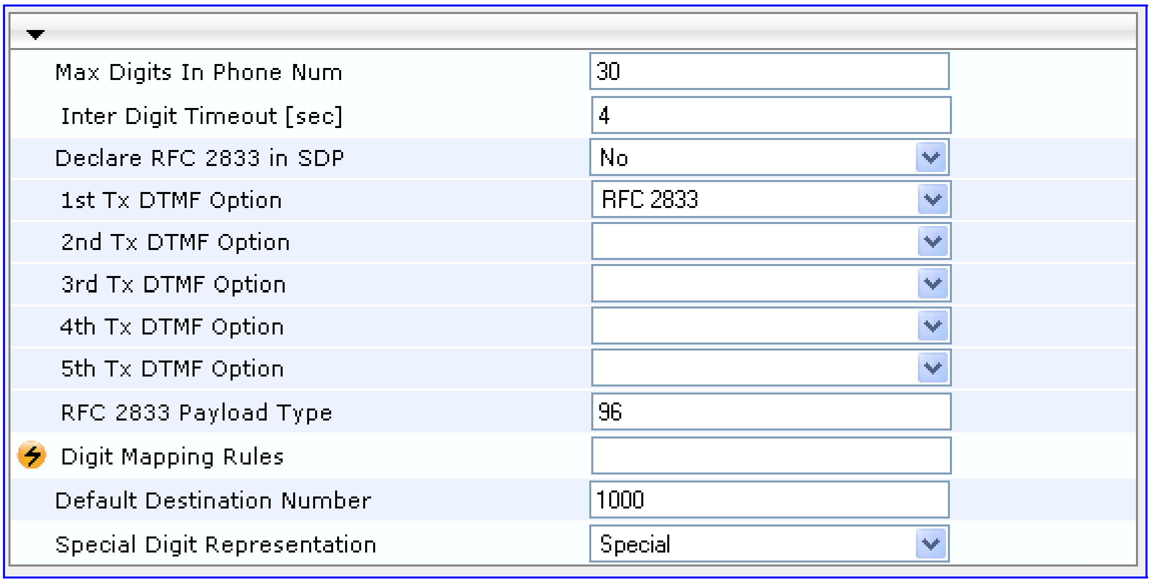
3.4.7.1.5 DTMF & Dialing Parameters

The 'DTMF & Dialing' page is used to configure parameters associated with dual-tone multi-frequency (DTMF) and dialing.

➢ To configure the DTMF and dialing parameters, take these 4 steps:

1. Open the 'DTMF & Dialing' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **DTMF & Dialing** page item).

Figure 3-63: DTMF & Dialing Page



Max Digits In Phone Num	30
Inter Digit Timeout [sec]	4
Declare RFC 2833 in SDP	No
1st Tx DTMF Option	RFC 2833
2nd Tx DTMF Option	
3rd Tx DTMF Option	
4th Tx DTMF Option	
5th Tx DTMF Option	
RFC 2833 Payload Type	96
Digit Mapping Rules	
Default Destination Number	1000
Special Digit Representation	Special

2. Configure the DTMF and dialing parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-34: DTMF and Dialing Parameters

Parameter	Description
Max Digits in Phone Num **[MaxDigits]**	Defines the maximum number of collected destination number digits that can be received from the Tel side when Tel-to-IP ISDN overlap dialing is performed . When the number of collected digits reaches the maximum, the device uses these digits for the called destination number. The valid range is 1 to 49. The default value is 30. **Note:** Digit Mapping Rules can be used instead.
Inter Digit Timeout for Overlap Dialing [sec] **[TimeBetweenDigits]**	Defines the time (in seconds) that the device waits between digits that are received from the Tel side when Tel-to-IP overlap dialing is performed (ISDN uses overlap dialing). When this inter-digit timeout expires, the device uses the collected digits to dial the called destination number. The valid range is 1 to 10. The default value is 4.
Declare RFC 2833 in SDP **[RxDTMFOption]**	Defines the supported Receive DTMF negotiation method. ▪ **[0]** No = Don't declare RFC 2833 telephony-event parameter in SDP.

Parameter	Description
	▪ **[3]** Yes = Declare RFC 2833 telephony-event parameter in SDP (default). The device is designed to always be receptive to RFC 2833 DTMF relay packets. Therefore, it is always correct to include the 'telephony-event' parameter as default in the SDP. However, some devices use the absence of the 'telephony-event' in the SDP to decide to send DTMF digits in-band using G.711 coder. If this is the case, you can set RxDTMFOption to 0.
1st to 5th Tx DTMF Option **[TxDTMFOption]**	Determines a single or several preferred transmit DTMF negotiation methods. ▪ **[0]** Not Supported = No negotiation - DTMF digits are sent according to the parameters DTMFTransportType and RFC2833PayloadType (default). ▪ **[1]** INFO (Nortel) = Sends DTMF digits according to IETF <draft-choudhuri-sip-info-digit-00>. ▪ **[2]** NOTIFY = Sends DTMF digits according to <draft-mahy-sipping-signaled-digits-01>. ▪ **[3]** INFO (Cisco) = Sends DTMF digits according to Cisco format. ▪ **[4]** RFC 2833. ▪ **[5]** INFO (Korea) = Sends DTMF digits according to Korea Telecom format. **Notes:** ▪ DTMF negotiation methods are prioritized according to the order of their appearance. ▪ When out-of-band DTMF transfer is used ([1], [2], [3], or [5]), the parameter DTMFTransportType is automatically set to 0 (DTMF digits are erased from the RTP stream). ▪ When RFC 2833 (4) is selected, the device: 1) Negotiates RFC 2833 Payload Type (PT) using local and remote SDPs. 2) Sends DTMF packets using RFC 2833 PT according to the PT in the received SDP. 3) Expects to receive RFC 2833 packets with the same PT as configured by the parameter RFC2833PayloadType. 4) Sends DTMF digits in transparent mode (as part of the voice stream). ▪ When TxDTMFOption is set to 0, the RFC 2833 PT is set according to the parameter RFC2833PayloadType for both transmit and receive. ▪ The *ini* file table parameter TxDTMFOption can be repeated 5 times for configuring the DTMF transmit methods.

Parameter	Description
RFC 2833 Payload Type **[RFC2833PayloadType]**	The RFC 2833 DTMF relay dynamic payload type. The valid range is 96 to 99, and 106 to 127. The default is 96. The 100, 102 to 105 range is allocated for proprietary usage. **Notes:** ▪ Certain vendors (e.g., Cisco) use payload type 101 for RFC 2833. ▪ When RFC 2833 payload type (PT) negotiation is used (the parameter TxDTMFOption is set to 4), this payload type is used for the received DTMF packets. If negotiation isn't used, this payload type is used for receive and for transmit.
Hook-Flash Option **[HookFlashOption]**	Determines the supported hook-flash Transport Type (i.e., method by which hook-flash is sent and received). ▪ **[0]** Not Supported = Hook-Flash indication isn't sent (default). ▪ **[1]** INFO = Send proprietary INFO message with Hook-Flash indication. ▪ **[4]** RFC 2833 ▪ **[5]** INFO (Lucent) = Send proprietary INFO message with Hook-Flash indication. **Notes:** ▪ The RFC 2833 (4) option is currently not supported. ▪ The DTMF HookFlashCode is send to IP according to the parameter HookFlashOption.
Digit Mapping Rules **[DigitMapping]**	Digit map pattern (used to reduce the dialing period when Overlap dialing is used). If the digit string (i.e., dialed number) matches one of the patterns in the digit map, the device stops collecting digits and establishes a call with the collected number. The digit map pattern can contain up to 52 options, each separated by a vertical bar (|). The maximum length of the entire digit pattern is 152 characters. Available notations: ▪ **[n-m]:** Range of numbers (not letters). ▪ **.** (single dot): Repeat digits until next notation (e.g., T). ▪ **x:** Any single digit. ▪ **T:** Dial timeout (configured by the parameter TimeBetweenDigits). ▪ **S:** Immediately applies a specific rule that is part of a general rule. For example, if your digit map includes a general rule 'x.T' and a specific rule '11x', for the specific rule to take precedence over the general rule, append 'S' to the specific rule (i.e., '11xS'). An example of a digit map is shown below: 11xS|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|*xx|91xxxxxxxxxx|9011x.T In the example above, the last rule can apply to International numbers - 9 for dialing tone, 011 Country Code, and then any number of digits for the local number ('x.'). **Note:** For PRI interfaces, the digitmap mechanism is applicable only when ISDN Overlap dialing is used (ISDNRxOverlap is set to 1).
Dial Tone Duration [sec] **[TimeForDialTone]**	Duration (in seconds) that the dial tone is played to an ISDN terminal. This parameter is applicable for overlap dialing when ISDNInCallsBehavior = 65536. The dial tone is played if the ISDN SETUP message doesn't include the called number. The valid range is 0 to 60. The default is 5.

Parameter	Description
Default Destination Number **[DefaultNumber]**	Defines the default destination phone number used if the received message doesn't contain a called party number and no phone number is configured in the 'Trunk Group' table (refer to “Configuring the Trunk Group Table” on page 195). The parameter is used as a starting number for the list of channels comprising all trunk groups in the device. The default value is 1000.
Special Digit Representation **[UseDigitForSpecialDTMF]**	Defines the representation for ‘special’ digits (‘*’ and ‘#’) that are used for out-of-band DTMF signaling (using SIP INFO/NOTIFY). ▪ **[0]** Special = Uses the strings ‘*’ and ‘#’ (default). ▪ **[1]** Numeric = Uses the numerical values 10 and 11.

3.4.7.2 Configuring the SIP Advanced Parameters

The **SIP Advanced Parameters** submenu allows you to configure advanced SIP control protocol parameters. This submenu contains the following page items:

- Advanced Parameters (refer to "General Parameters" on page 151)
- Supplementary Services (refer to "Supplementary Services" on page 159)
- Stand-Alone Survivability (refer to “Stand-Alone Survivability” on page 161)
- SBC Configuration (refer to “SBC Configuration” on page 163)

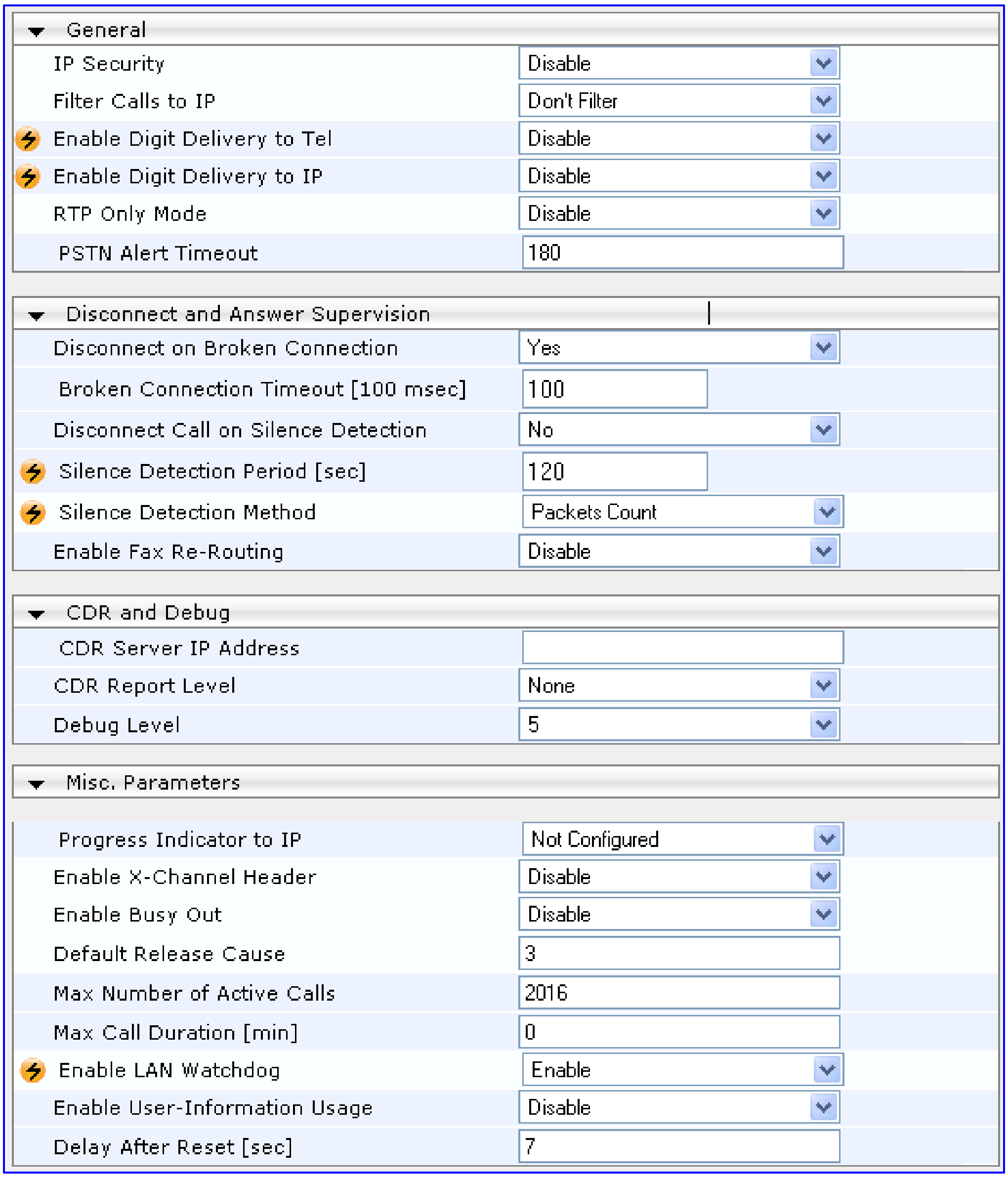
3.4.7.2.1 Advanced Parameters

The 'Advanced Parameters' page allows you to configure general control protocol parameters.

➢ To configure the advanced general protocol parameters, take these 4 steps:

1. Open the 'Advanced Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **SIP Advanced Parameters** submenu > **Advanced Parameters** page item).

Figure 3-64: Advanced Parameters Page



▼ General

IP Security	Disable
Filter Calls to IP	Don't Filter
⚡ Enable Digit Delivery to Tel	Disable
⚡ Enable Digit Delivery to IP	Disable
RTP Only Mode	Disable
PSTN Alert Timeout	180

▼ Disconnect and Answer Supervision

Disconnect on Broken Connection	Yes
Broken Connection Timeout [100 msec]	100
Disconnect Call on Silence Detection	No
⚡ Silence Detection Period [sec]	120
⚡ Silence Detection Method	Packets Count
Enable Fax Re-Routing	Disable

▼ CDR and Debug

CDR Server IP Address	
CDR Report Level	None
Debug Level	5

▼ Misc. Parameters

Progress Indicator to IP	Not Configured
Enable X-Channel Header	Disable
Enable Busy Out	Disable
Default Release Cause	3
Max Number of Active Calls	2016
Max Call Duration [min]	0
⚡ Enable LAN Watchdog	Enable
Enable User-Information Usage	Disable
Delay After Reset [sec]	7

2. Configure the parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-35: Advanced Parameters Description

Parameter	Description
General	
IP Security **[SecureCallsFromIP]**	Determines whether the device accepts SIP calls received from only IP addresses defined in the 'Tel to IP Routing' table (refer to "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing' table if EnableSBC is set to 1 (refer to “Outbound IP Routing Table” on page 178). This is useful in preventing unwanted SIP calls or messages and/or VoIP spam. ▪ **[0]** Disable = device accepts all SIP calls (default). ▪ **[1]** Enable = device accepts SIP calls only from IP addresses defined in the 'Tel to IP Routing' table (or 'Outbound IP Routing' table). The device rejects all calls from unknown IP addresses. **Note:** Specifying the IP address of a Proxy server in the 'Tel to IP Routing' table (or 'Outbound IP Routing' table) enables the device to accept only calls originating from the Proxy server while rejecting all other calls that don’t appear in this table.
Filter Calls to IP **[FilterCalls2IP]**	Enables filtering of Tel-to-IP calls when a Proxy is used (i.e., IsProxyUsed parameter is set to 1 -- refer to "Proxy & Registration Parameters" on page 132). ▪ **[0]** Don't Filter = device doesn't filter calls when using a Proxy. (default) ▪ **[1]** Filter = Filtering is enabled. When this parameter is enabled and a Proxy is used, the device first checks the 'Tel-to-IP Routing' table or 'Outbound IP Routing' table before making a call through the Proxy. If the number is not allowed (i.e., number isn't listed in the table or a call restriction routing rule of IP address 0.0.0.0 is applied), the call is released. **Note:** When no Proxy is used, this parameter must be disabled and filtering is according to the 'Tel-to-IP Routing' table (or 'Outbound IP Routing' table).
Enable Digit Delivery to IP **[EnableDigitDelivery2IP]**	The Digit Delivery feature enables sending DTMF digits to the destination IP address after the Tel-to-IP call is answered. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enable digit delivery to IP. To enable this feature, modify the called number to include at least one 'p' character. The device uses the digits before the 'p' character in the initial INVITE message. After the call is answered, the device waits for the required time (number of 'p' multiplied by 1.5 seconds) and then sends the rest of the DTMF digits using the method chosen (in-band or out-of-band). **Note:** The called number can include several 'p' characters (1.5 seconds pause), for example, 1001pp699, 8888p9p300.
Enable Digit Delivery to Tel **[EnableDigitDelivery]**	Enables the Digit Delivery feature, which sends DTMF digits (of the called number) to the device's B-channel (phone line) after the call is answered [line offhooked (FXS) or seized (FXO)] for IP-to-Tel calls. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enable Digit Delivery feature for the device (two-stage dialing).

Parameter	Description
	If the called number in IP-to-Tel call includes the characters 'w' or 'p', the device places a call with the first part of the called number (before 'w' or 'p') , and plays DTMF digits after the call is answered. If the character 'w' is used, the device waits for detection of dial tone before it starts playing DTMF digits. For example, if the called number is '1007766p100', the device places a call with 1007766 as the destination number, then after the call is answered, it waits 1.5 seconds ('p') and plays the rest of the number (100) as DTMF digits. Additional examples: 1664wpp102, 66644ppp503, and 7774w100pp200.
RTP Only Mode **[RTPOnlyMode]**	Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a Control session. The remote IP address is determined according to the 'Tel to IP Routing' table (refer to "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing' table (refer to “Outbound IP Routing Table” on page 178). The port is the same port as the local RTP port (set by BaseUDPPort and the channel on which the call is received). ▪ **[0]** Disable = Disable (default). ▪ **[1]** Transmit & Receive = Send and receive RTP. ▪ **[2]** Transmit Only= Send RTP only. ▪ **[3]** Receive Only= Receive RTP only. **Notes:** ▪ To configure the RTP Only mode per trunk, use the RTPOnlyModeForTrunk_ID (refer to “Configuring the Trunk Settings” on page 82). ▪ If per trunk configuration (using RTPOnlyModeForTrunk) is set to other than default, the RTPOnlyMode parameter value is overridden.
PSTN Alert Timeout **[PSTNAlertTimeout]**	Alert Timeout (in seconds) (ISDN T301 timer) for calls to PSTN. This timer is used between the time a SETUP message is sent to the Tel side (IP-to-Tel call establishment) and a CONNECT message is received. If an ALERTING message is received, the timer is restarted. The default is 180 seconds. The range is 1 to 600. **Note:** If per trunk configuration (using TrunkPSTNAlertTimeout) is set to other than default (refer to “Configuring the Trunk Settings” on page 82), the PSTNAlertTimeout parameter value is overridden.
Reanswer Time **[RegretTime]**	Determines the time period the device waits for an MFC R2 Resume (Reanswer) signal once a Suspend (Clear back) signal is received from the PBX. If this timer expires, the call is released. **Note:** Applicable only for MFC R2 CAS Brazil variant. The valid range is 0 to 255 (in seconds). The default value is 0.
Disconnect and Answer Supervision	
Send Digit Pattern on Connect **[TelConnectCode]**	Defines a digit pattern to send to the Tel side after SIP 200 OK is received from the IP side. The digit pattern is a pre-defined DTMF sequence that is used to indicate an answer signal (e.g., for billing). The valid range is 1 to 8 characters. **Note:** This parameter is applicable to FXO and CAS.
Disconnect on Broken Connection **[DisconnectOnBrokenCo**	Determines whether the device releases the call if RTP packets are not received within a user-defined timeout. ▪ **[0]** No

Parameter	Description
nnection]	▪ **[1]** Yes (default) **Notes:** ▪ The timeout is set by the parameter BrokenConnectionEventTimeout. ▪ This feature is applicable only if the RTP session is used without Silence Compression. If Silence Compression is enabled, the device doesn't detect a broken RTP connection. ▪ During a call, if the source IP address (from where the RTP packets are sent) is changed without notifying the device, the device filters these RTP packets. To overcome this, set DisconnectOnBrokenConnection to 0; the device doesn't detect RTP packets arriving from the original source IP address and switches (after 300 msec) to the RTP packets arriving from the new source IP address.
Broken Connection Timeout **[BrokenConnectionEventTimeout]**	The time period (in 100 msec units) that an RTP packet is not received after which a call is disconnected. The valid range is 1 to 1,000. The default value is 100 (i.e., 10 seconds). **Notes:** ▪ Applicable only if DisconnectOnBrokenConnection = 1. ▪ Currently, this feature works only if Silence Suppression is disabled.
Disconnect Call on Silence Detection **[EnableSilenceDisconnect]**	Determines whether calls are disconnected after detection of silence. ▪ **[1]** Yes = The device disconnects calls in which silence occurs (in both call directions) for more than a user-defined time. ▪ **[0]** No = Call is not disconnected when silence is detected (default). The silence duration can be set by the FarEndDisconnectSilencePeriod parameter (default 120). **Note:** To activate this feature, set EnableSilenceCompression and FarEndDisconnectSilenceMethod to 1.
Silence Detection Period [sec] **[FarEndDisconnectSilencePeriod]**	Duration of silence period (in seconds) prior to call disconnection. The range is 10 to 28,800 (i.e., 8 hours). The default is 120 seconds. **Note:** This parameter is applicable only to devices that use DSP templates 2 and 3.
Silence Detection Method **[FarEndDisconnectSilenceMethod]**	Silence detection method. ▪ **[0]** None = Silence detection option is disabled. ▪ **[1]** Packets Count = According to packet count. ▪ **[2]** Voice/Energy Detectors = N/A. ▪ **[3]** All = N/A.
Enable Fax Re-Routing **[EnableFaxReRouting]**	Enables or disables re-routing of Tel-to-IP calls that are identified as fax calls. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enabled. If a CNG tone is detected on the Tel side of a Tel-to-IP call, a 'FAX' prefix is appended to the destination number before routing and manipulations. An entry of ‘FAX’ as destination number in the 'Tel-to-IP Routing' table is then used to route the call, and the destination number

Parameter	Description
	manipulation mechanism is used to remove the 'FAX' prefix, if required. If the initial INVITE used to establish the voice call (not fax) was already sent, a CANCEL (if not connected yet) or a BYE (if already connected) is sent to tear down the voice call. **Notes:** ▪ To enable this feature, set CNGDetectorMode to 2, and IsFaxUsed to 1, 2, or 3. ▪ The 'FAX' prefix in routing and manipulation tables is case sensitive.
CDR and Debug	
CDR Server IP Address **[CDRSyslogServerIP]**	Defines the destination IP address to where CDR logs are sent. The default value is a null string, which causes CDR messages to be sent with all Syslog messages to the Syslog server. **Note:** The CDR messages are sent to UDP port 514 (default Syslog port).
CDR Report Level **[CDRReportLevel]**	Determines whether Call Detail Records (CDR) are sent to the Syslog server and when they are sent. ▪ **[0]** None = CDRs are not used (default). ▪ **[1]** End Call = CDR is sent to the Syslog server at the end of each call. ▪ **[2]** Start & End Call = CDR report is sent to Syslog at the start and end of each call. ▪ **[3]** Connect & End Call = CDR report is sent to Syslog at connection and at the end of each call. ▪ **[4]** Start & Connect & End Call = CDR report is sent to Syslog at the start, at connection, and at the end of each call. The CDR Syslog message complies with RFC 3161 and is identified by: Facility = 17 (local1) and Severity = 6 (Informational).
Debug Level **[GwDebugLevel]**	Syslog debug logging level. ▪ **[0]** 0 = Debug is disabled (default). ▪ **[1]** 1 = Flow debugging is enabled. ▪ **[2]** 2 = Flow and device interface debugging are enabled. ▪ **[3]** 3 = Flow, device interface, and stack interface debugging are enabled. ▪ **[4]** 4 = Flow, device interface, stack interface, and session manager debugging are enabled. ▪ **[5]** 5 = Flow, device interface, stack interface, session manager, and device interface expanded debugging are enabled. **Note:** Usually set to 5 if debug traces are needed.
Misc. Parameters	
Progress Indicator to IP **[ProgressIndicator2IP]**	▪ **[-1]** Not Configured = for ISDN spans, the progress indicator (PI) that is received in ISDN Proceeding, Progress, and Alert messages is used as described in the options below. (default) ▪ **[0]** No PI = For IP-to-Tel calls, the device sends 180 Ringing SIP response to IP after receiving ISDN Alert or (for CAS) after placing a call to PBX/PSTN. ▪ **[1]** PI =1**, [8]** PI =8: For IP-to-Tel calls, if EnableEarlyMedia = 1, the device sends 180 Ringing with SDP in response to an ISDN Alert or

Parameter	Description
	it sends a 183 Session Progress message with SDP in response to only the first received ISDN Proceeding or Progress message after a call is placed to PBX/PSTN over the trunk.
Enable X-Channel Header **[XChannelHeader]**	Determines whether the x-channel header is added to SIP messages for trunk / B-channel information. ▪ **[0]** Disable = x-channel header is not used (default). ▪ **[1]** Enable = x-channel header is generated with trunk/B-channel and IP address information. The header provides information on the E1/T1 physical trunk/B-channel on which the call is received or placed. For example, 'x-channel: DS/DS1-5/22;IP=192.168.13.1', where 'DS/DS-1' is a constant string, '5' is the trunk number, '22' is the B-channel, and in addition, the device's IP address is added to the header. This header is generated by the device and is sent in INVITE messages and 183/180/200OK responses.
Enable Busy Out **[EnableBusyOut]**	Determines whether the Busy Out feature is enabled. ▪ **[0]** Disable = 'Busy out' feature is not used (default). ▪ **[1]** Enable = 'Busy out' feature is enabled. When Busy Out is enabled and certain scenarios exist, the device performs the following: All E1/T1 trunks are automatically taken out of service by taking down the D-Channel or by sending a Service Out message for T1 PRI trunks supporting these messages (NI-2, 4/5-ESS, DMS-100, and Meridian). These behaviors are performed due to one of the following scenarios: ▪ Physically disconnected from the network (i.e., Ethernet cable is disconnected). ▪ The Ethernet cable is connected, but the device can't communicate with any host. Note that LAN Watch-Dog must be activated (EnableLANWatchDog = 1). ▪ The device can't communicate with the proxy (according to the Proxy keep-alive mechanism) and no other alternative exists to send the call. ▪ The IP Connectivity mechanism is enabled (using AltRoutingTel2IPEnable) and there is no connectivity to any destination IP address. **Note:** The Busy Out behavior varies between different protocol types.
Default Release Cause **[DefaultReleaseCause]**	Defines the default Release Cause (sent to IP) for IP-to-Tel calls when the device initiates a call release and an explicit matching cause for this release isn't found. The default release cause is NO_ROUTE_TO_DESTINATION (3). Other common values include NO_CIRCUIT_AVAILABLE (34), DESTINATION_OUT_OF_ORDER (27), etc. **Notes:** ▪ The default release cause is described in the Q.931 notation and is translated to corresponding SIP 40x or 50x values (e.g., 3 to SIP 404 and 34 to SIP 503). ▪ When the Trunk is disconnected or is not synchronized, the internal cause is 27. This cause is mapped, by default, to SIP 502. ▪ For mapping SIP-to-Q.931 and Q.931-to-SIP release causes, refer to

Parameter	Description
	Release Reason Mapping on page 394. - For a list of SIP responses-Q.931 release cause mapping, refer to "Release Cause Mapping" on page 189.
Delay After Reset [sec] **[GWAppDelayTime]**	Defines the time interval (in seconds) that the device's operation is delayed after a reset. The valid range is 0 to 45. The default value is 7 seconds. **Note:** This feature helps to overcome connection problems caused by some LAN routers or IP configuration parameters' modifications by a DHCP server.
Max Number of Active Calls **[MaxActiveCalls]**	Defines the maximum number of simultaneous active calls supported by the device. If the maximum number of calls is reached, new calls are not established. The default value is the maximum available channels (no restriction on the maximum number of calls). The valid range is 1 to 240.
Max Call Duration (min) **[MaxCallDuration]**	Defines the maximum call duration (in minutes). If this time expires, both sides of the call are released (IP and Tel). The valid range is 0 to 35,791. The default is 0 (i.e., no limitation).
Enable LAN Watchdog **[EnableLanWatchDog]**	Determines whether the LAN Watch-Dog feature is enabled**.** - **[0]** Disable = Disable LAN Watch-Dog (default). - **[1]** Enable = Enable LAN Watch-Dog. When LAN Watch-Dog is enabled, the device's overall communication integrity is checked periodically. If no communication for about 3 minutes is detected, the device performs a self test. If the self test succeeds, the problem is logical link down (i.e., Ethernet cable disconnected on the switch side), and the Busy Out mechanism is activated if enabled (EnableBusyOut = 1). If the self test fails, the device restarts to overcome internal fatal communication error. **Note:** Enable LAN Watchdog is relevant only if the Ethernet connection is full duplex.
Enable User-Information Usage **[EnableUserInfoUsage]**	Enables or disables usage of the User Information loaded to the device in the User Information auxiliary file. (For a description on User Information, refer to "Loading Auxiliary Files" on page 231.) - **[0]** Disable = Disabled (default). - **[1]** Enable = Enabled.
First Call Ringback Tone ID **[FirstCallRBTId]**	Determines the index of the first Ringback Tone in the CPT file. This option enables an Application server to request the device to play a distinctive Ringback tone to the calling party according to the destination of the call. The tone is played according to the Alert-Info header received in the 180 Ringing SIP response (the value of the Alert-Info header is added to the value of this parameter). The valid range is -1 to 1,000. The default value is -1 (i.e., play standard Ringback tone). **Notes:** - It is assumed that all Ringback Tones are defined in sequence in the CPT file. - In case of an MLPP call, the device uses the value of this parameter plus 1 as the index of the Ringback tone in the CPT file (e.g., if this value is set to 1, then the index is 2, i.e., 1 + 1).

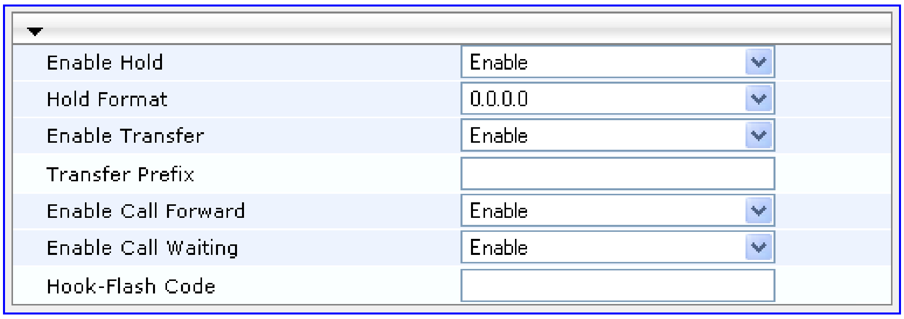
3.4.7.2.2 Supplementary Services

The 'Supplementary Services' page is used to configure parameters that are associated with supplementary services. For detailed information on supplementary services, refer to "Working with Supplementary Services" on page 377.

➢ To configure the supplementary services' parameters, take these 4 steps:

1. Open the 'Supplementary Services' page (**Configuration** tab > **Protocol Configuration** menu > **SIP Advanced Parameters** submenu > **Supplementary Services** page item).

Figure 3-65: Supplementary Services Page



Enable Hold	Enable
Hold Format	0.0.0.0
Enable Transfer	Enable
Transfer Prefix	
Enable Call Forward	Enable
Enable Call Waiting	Enable
Hook-Flash Code	

2. Configure the supplementary services parameters according to the table below.
3. Click the **Submit** button to save your changes, or click the **Subscribe to MWI** or **Unsubscribe to MWI** buttons to save your changes and to subscribe / unsubscribe to the MWI server.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-36: Supplementary Services Parameters

Parameter	Description
Enable Hold **[EnableHold]**	Enables interworking of the Hold/Retrieve supplementary service from PRI to SIP. ▪ **[0]** Disable = Disables. ▪ **[1]** Enable = Enables (default). **Notes:** ▪ This capability is only supported by the Euro ISDN variant and only from TE (user) to NT (network). ▪ To support interworking of the Hold/Retrieve supplementary service from SIP to ISDN, set EnableHold2ISDN to 1.
Enable Hold to ISDN **[EnableHold2ISDN]**	Enables interworking of the Hold/Retrieve supplementary service from SIP to PRI. ▪ **[0]** = Disabled (default) ▪ **[1]** = Enabled **Notes:** ▪ This capability is supported only for QSIG and Euro ISDN variants. ▪ To support interworking of the Hold/Retrieve supplementary service from ISDN to SIP, set the parameter EnableHold to 1

Parameter	Description
Hold Format **[HoldFormat]**	Determines the format of the call hold request. ▪ **[0]** 0.0.0.0 = The connection IP address in SDP is 0.0.0.0 (default). ▪ **[1]** Send Only = The SDP contains the attribute 'a=sendonly'. **Note:** This parameter is applicable only to QSIG and Euro ISDN protocols.
Held Timeout **[HeldTimeout]**	Determines the time interval that the device can allow a call to remain on hold. If a Resume (un-hold Re-INVITE) message is received before the timer expires, the call is renewed. If this timer expires, the call is released. ▪ **[-1]** = The call is placed on hold indefinitely until the initiator of on hold retrieves the call again(default). ▪ **[0 - 2400]** =Time to wait in seconds, after which the call is released.
Enable Transfer **[EnableTransfer]**	Determines whether call transfer is enabled. ▪ **[0]** Disable = Disable the call transfer service. ▪ **[1]** Enable = The device responds to a REFER message with the Referred-To header to initiate a call transfer (default). **Notes:** ▪ To use call transfer, the devices at both ends must support this option. ▪ To use call transfer, set the parameter EnableHold to 1.
Transfer Prefix **[xferPrefix]**	Defines the string that is added as a prefix to the transferred / forwarded called number when the REFER / 3xx message is received. **Notes:** ▪ The number manipulation rules apply to the user part of the REFER-TO / Contact URI before it is sent in the INVITE message. ▪ This parameter can be used to apply different manipulation rules to differentiate transferred number from the originally dialed number.
Enable Call Forward **[EnableForward]**	Determines whether Call Forward is enabled. ▪ **[0]** Disable = Disable the Call Forward service. ▪ **[1]** Enable = Enable Call Forward service(default). The device doesn't initiate call forward, it can only respond to call forward requests. **Note:** To use this service, the devices at both ends must support this option.
Enable Call Waiting **[EnableCallWaiting]**	Determines whether Call Waiting is enabled. ▪ **[0]** Disable = Disable the Call Waiting service. ▪ **[1]** Enable = Enable the Call Waiting service (default). If enabled, when the device initiates a Tel-to-IP call to a destination that is busy, it plays a Call Waiting Ringback tone to the caller. **Notes:** ▪ The device's Call Progress Tones file must include a Call Waiting Ringback tone. ▪ The EnableHold parameter must be enabled on the called side. ▪ For information on the Call Waiting feature, refer to Call Waiting. ▪ For information on the Call Progress Tones file, refer to Configuring the Call Progress Tones File.

Parameter	Description
Hook-Flash Code **[HookFlashCode]**	Determines the digit pattern used by the PBX to indicate a Hook Flash event. When this pattern is detected from the Tel side, the device responds as if a Hook Flash event occurs and sends a SIP INFO message if HookFlashOption is set to 1, indicating Hook Flash. If configured and a Hook Flash indication is received from the IP side, the device generates this pattern to the Tel side. The valid range is a 25-character string. The default is a null string.
MLPP (Multilevel Precedence and Preemption) Note: For additional MLPP parameters, refer to “Configuring the Digital Gateway Parameters” on page 207	
Call Priority Mode **[CallPriorityMode]**	Enables Priority Calls handling. ▪ **[0]** Disable = Disable (default). ▪ **[1]** MLPP = Priority Calls handling is enabled.
MLPP DiffServ **[MLPPDiffserv]**	Defines the DiffServ value (differentiated services code point -- DSCP) used in IP packets containing SIP messages that are related to MLPP calls. The valid range is 0 to 63. The default value is 50.

3.4.7.2.3 Stand-Alone Survivability

The 'SAS Configuration' page allows you to configure the device's Stand-Alone Survivability (SAS) feature. This feature is useful for providing a local backup via the PSTN in Small or Medium Enterprises (SME) that are serviced by IP Centrex services. In such environments, the enterprise's incoming and outgoing telephone calls (external and internal) are controlled by the Proxy, which communicates with the enterprise through the WAN interface. SAS ensures that incoming, outgoing, and internal calls service is maintained in case of a WAN or Proxy failure, using a PSTN (or an alternate VoIP) backup connection and the device's built-in internal routing. To utilize the SAS feature, the VoIP CPEs such as IP phones or residential gateways need to be defined so that their Proxy and Registrar destination addresses and UDP port equal the SAS feature's IP address and SAS local SIP UDP port.

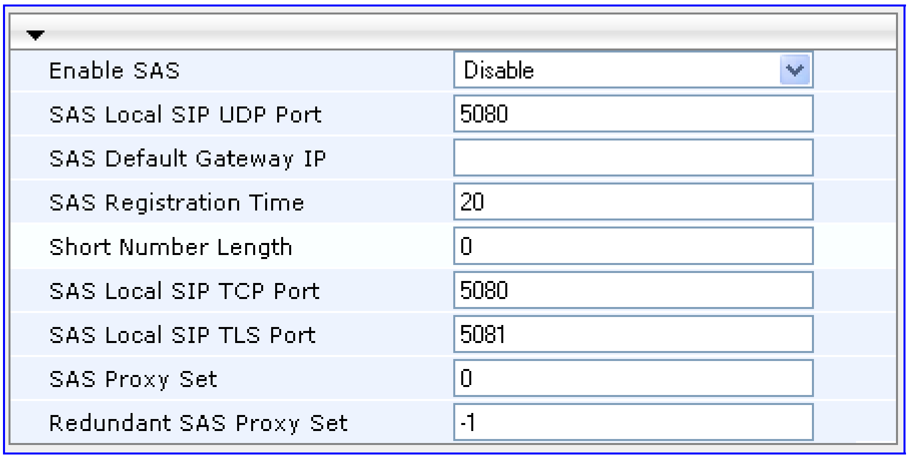
Notes:

- The 'SAS Configuration' page is Feature Key dependant and therefore is available only if included in the device's Feature Key (refer to “Upgrading the Software Upgrade Key” on page 233).
- For a detailed explanation on SAS and for configuring various SAS setups, refer to "Stand-Alone Survivability (SAS) Feature" on page 346).
- For additional SAS parameters (configurable only using the *ini* file), refer to "SIP Configuration Parameters" on page 284.

➢ To configure the Stand-Alone Survivability parameters, take these 4 steps:

1. Open the 'SAS Configuration' page (**Configuration** tab > **Protocol Configuration** menu > **SIP Advanced Parameters** submenu > **Stand-Alone Survivability** page item).

Figure 3-66: SAS Configuration Page



Enable SAS	Disable
SAS Local SIP UDP Port	5080
SAS Default Gateway IP	
SAS Registration Time	20
Short Number Length	0
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
Redundant SAS Proxy Set	-1

2. Configure the parameters according to the table below.
3. Click the **Submit** button to apply your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-37: Stand-Alone Survivability Parameters Description

Parameter	Description
Enable SAS **[EnableSAS]**	Enables the Stand-Alone Survivability (SAS) feature. ▪ **[0]** Disable Disabled (default) ▪ **[1]** Enable = SAS is enabled When enabled, the device receives the registration requests from different SIP entities in the local network and then forwards them to the defined proxy. If the connection to the proxy fails ('Emergency Mode'), the device serves as a proxy by allowing calls internal to the local network or outgoing to PSTN.
SAS Local SIP UDP Port **[SASLocalSIPUDPPort]**	Local UDP port for sending and receiving SIP messages for SAS. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port. The valid range is 1 to 65,534. The default value is 5080.
SAS Default Gateway IP **[SASDefaultGatewayIP]**	The default gateway used in SAS 'Emergency Mode'. When an incoming SIP INVITE is received and the destination Address-Of-Record is not included in the SAS database, the request is immediately sent to this default gateway. The address can be configured as an IP address (dotted-decimal notation) or as a domain name (up to 49 characters). The default is a null string, which is interpreted as the local IP address of the gateway.

Parameter	Description
SAS Registration Time **[SASRegistrationTime]**	Determines the value of the SIP Expires header that is sent in a 200 OK response to an incoming REGISTER message when in SAS 'Emergency Mode'. The valid range is 10 to 2,000,000. The default value is 20.
Short Number Length **[SASShortNumberLength]**	This parameter is obsolete; instead, use the parameter SASRegistrationManipulation.
SAS Local SIP TCP Port **[SASLocalSIPTCPPort]**	Local TCP port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port. The valid range is 1 to 65,534. The default value is 5080.
SAS Local SIP TLS Port **[SASLocalSIPTLSPort]**	Local TLS port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port. The valid range is 1 to 65,534. The default value is 5081.
SAS Proxy Set **[SASProxySet]**	Determines the Proxy Set (index number) used in SAS Normal mode to forward REGISTER and INVITE requests from the users that are served by the SAS application. The valid range is 0 to 5. The default value is 0 (i.e., default Proxy Set).
Redundant SAS Proxy Set **[RedundantSASProxySet]**	Determines the Proxy Set (index number) used in SAS Emergency mode for fallback when the user is not found in the Registered Users database. Each time a new SIP request arrives, the SAS application checks whether the user is listed in the registration database. If the user is located in the database, the request is sent to the user. If the user is not found, the request is forwarded to the next redundant SAS defined in the Redundant SAS Proxy Set. If that SAS Proxy IP appears in the Via header of the request, it is not forwarded (so that loops are prevented in the request's course). If no such redundant SAS exists, the SAS sends the request to its default gateway (configured by the parameter SASDefaultGatewayIP). The valid range is -1 to 5. The default value is -1 (i.e., no redundant Proxy Set).

3.4.7.2.4 SBC Configuration

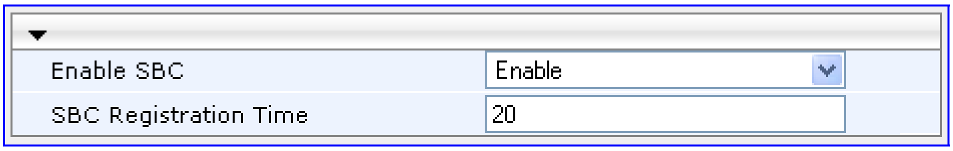
The 'SBC Settings' page allows you to enable the device's IP-to-IP call routing feature. To enable IP-to-IP capabilities, the following prerequisites must be fulfilled:

- The device must be loaded with the Feature Key that includes the SBC feature (refer to "Upgrading the Software Upgrade Key" on page 233).
- The device must be running SIP version 5.4 or later.

➢ To configure the SBC parameters, take these 4 steps:

1. Open the 'SBC Settings' page (**Configuration** tab > **Protocol Configuration** menu > **SIP Advanced Parameters** submenu > **SBC Configuration** page item).

Figure 3-67: SBC Settings Page



Enable SBC: Enable

SBC Registration Time: 20

2. Configure the SBC parameters according to the following table.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to Saving Configuration.

Table 3-38: SBC Parameters

Parameter	Description
Enable SBC **[EnableSBC]**	Enables or disables the SBC feature. ▪ **[0]** Disable (default) ▪ **[1]** Enable
SBC Registration Time **[SBCRegistrationTime]**	Configures the value (in sec) sent in the "expires" when the device replies with a SIP 200 OK in response to Registration requests. The default is 20. **Note:** This parameter is applicable only to clients belonging to IP groups of type "USER".

3.4.7.3 Configuring the Number Manipulation Tables

The device provides four Number Manipulation tables for incoming (IP-to-Tel) and outgoing (Tel-to-IP) calls. These tables are used to modify the destination and source telephone numbers so that the calls can be routed correctly. For example, telephone number manipulation can be implemented for the following:

- Strip or add dialing plan digits from or to the number. For example, a user may need to first dial 9 before dialing the phone number to indicate an external line. This number (9) can then be removed (by the Manipulation table) before the call is setup.
- Allow or disallow Caller ID information to be sent according to destination or source prefixes.
- Assign NPI/TON to IP-to-Tel calls. The device can use a single global setting for NPI/TON classification or it can use the setting in this table on a call-by-call basis.

The number manipulation is configured in the following tables:

- **For Tel-to-IP calls:**
  - Destination Phone Number Manipulation Table for Tel-to-IP Calls (NumberMapTel2IP *ini* file parameter)
  - Source Phone Number Manipulation Table for Tel-to-IP Calls (SourceNumberMapTel2IP *ini* file parameter)

- **For IP-to-Tel calls:**
  - Destination Phone Number Manipulation Table for IP-to-Tel Calls (NumberMapIP2Tel *ini* file parameter)
  - Source Phone Number Manipulation Table for IP-to-Tel Calls (SourceNumberMapIP2Tel *ini* file parameter)

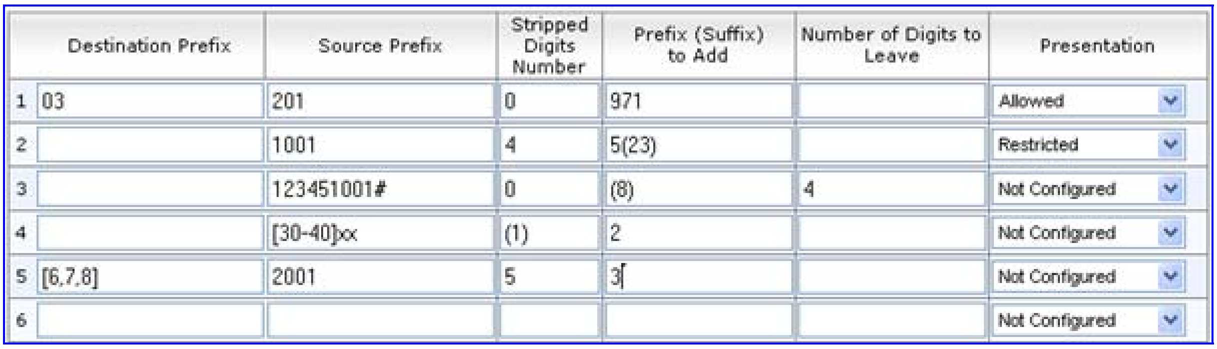
Notes:

- Number manipulation can occur before or after a routing decision is made. For example, you can route a call to a specific Trunk Group according to its original number, and then you can remove or add a prefix to that number before it is routed. To determine when number manipulation is performed, configure the 'IP to Tel Routing Mode' parameter (RouteModeIP2Tel) described in "IP to Trunk Group Routing" on page 181, and 'Tel to IP Routing Mode' parameter (RouteModeTel2IP) described in "Tel to IP Routing Table" on page 175 (or “Outbound IP Routing Table” on page 178).
- For configuring number manipulation using *ini* file table parameters NumberMapIP2Tel, NumberMapTel2IP, SourceNumberMapIP2Tel, and SourceNumberMapTel2IP, refer to "Number Manipulation and Routing Parameters" on page 313.

➢ To configure the Number Manipulation tables, take these 5 steps:

1. Open the required 'Number Manipulation' page (**Configuration** tab > **Protocol Configuration** menu > **Manipulation Tables** submenu > **Dest Number IP->Tel**, **Dest Number Tel->IP**, **Source Number IP->Tel**, or **Source Number Tel->IP** page item); the relevant Manipulation table page is displayed (e.g., 'Source Phone Number Manipulation Table for Tel→IP Calls' page).

Figure 3-68: Source Phone Number Manipulation Table for Tel-to-IP Calls



	Destination Prefix	Source Prefix	Stripped Digits Number	Prefix (Suffix) to Add	Number of Digits to Leave	Presentation
1	03	201	0	971		Allowed
2		1001	4	5(23)		Restricted
3		123451001#	0	(8)	4	Not Configured
4		[30-40]xx	(1)	2		Not Configured
5	[6,7,8]	2001	5	3		Not Configured
6						Not Configured

The figure above shows an example of the use of manipulation rules in the 'Source Phone Number Manipulation Table for Tel→IP Calls':

- When the destination number is 035000 and source number is 20155, the source number is changed to 97120155.
- When the source number is 1001876, it is changed to 587623.
- When the source number is 1234510012001, it is changed to 20018.
- When the source number is 3122, it is changed to 2312.

2. From the 'Table Index' drop-down list, select the range of entries that you want to edit (up to 20 entries can be configured for Source Number IP-to-Tel Manipulation, up to 120 entries can be configured for Source Number Tel-to-IP Manipulation, and up to 100 entries for Destination Number Manipulation).
3. Configure the Number Manipulation table according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- The manipulation rules are executed in the following order:
  1. Number of stripped digits.
  2. Number of digits to leave.
  3. Prefix / suffix to add.
- The manipulation rules can be applied to any incoming call whose source IP address (if applicable), source Trunk Group (if applicable), source IP Group (if applicable), destination number prefix and source number prefix matches the values defined in the 'Source IP Address', 'Source Trunk Group', 'Source IP Group', 'Destination Prefix', and 'Source Prefix' fields respectively. The number manipulation can be performed using a combination of each of the above criteria, or using each criterion independently.
- For available notations that represent multiple numbers, refer to "Dialing Plan Notation" on page 168.

Table 3-39: Number Manipulation Parameters Description

Parameter	Description
Source Trunk Group **[_SrcTrunkGroupID]**	The source Trunk Group (1-99) for Tel-to-IP calls. To denote any Trunk Group, leave this field empty. **Notes:** ▪ This parameter is available only in the 'Source Phone Number Manipulation Table for Tel -> IP Calls' and 'Destination Phone Number Manipulation Table for Tel -> IP Calls' pages. ▪ For IP-to-IP call routing, this parameter is not required (i.e., leave the field empty).
Source IP Group **[_SrcIPGroupID]**	The IP Group from where the IP-to-IP call originated. Typically, this IP Group of an incoming INVITE is determined/classified using the ‘Inbound IP Routing’ table. If not used (i.e., any IP Group), simply leave the field empty. **Notes:** ▪ This parameter is available only in the 'Source Phone Number Manipulation Table for Tel -> IP Calls' page. ▪ If this Source IP Group has a Serving IP Group, then all calls originating from this Source IP Group is sent to the Serving IP Group. In this scenario, this table is used only if the parameter PreferRouteTable is set to 1.
Destination Prefix **[_DestinationPrefix]**	Destination (called) telephone number prefix. An asterisk (*) represents any number.

Parameter	Description
Source Prefix **[_SourcePrefix]**	Source (calling) telephone number prefix. An asterisk (*) represents any number.
Source IP **[_SourceAddress]**	Source IP address of the caller (obtained from the Contact header in the INVITE message). **Notes:** - This parameter is applicable only to the Number Manipulation tables for IP-to-Tel calls. - The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99. - The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all IP addresses between 10.8.8.0 and 10.8.8.255.
Stripped Digits From Left **[_RemoveFromLeft]**	Number of digits to remove from the left of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 1234.
Stripped Digits From Right **[_RemoveFromRight]**	Number of digits to remove from the right of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 5551.
Prefix to Add **[_Prefix2Add]**	The number or string that you want added to the front of the telephone number. For example, if you enter '9' and the phone number is 1234, the new number is 91234.
Suffix to Add **[_Suffix2Add]**	The number or string that you want added to the end of the telephone number. For example, if you enter '00' and the phone number is 1234, the new number is 123400.
Number of Digits to Leave **[_LeaveFromRight]**	The number of digits that you want to retain from the right of the phone number.
NPI **[_NumberPlan]**	The Numbering Plan Indicator (NPI) assigned to this entry. - **[0]** Unknown (default) - **[9]** Private - **[1]** E.164 Public - **[-1]** Not Configured = value received from PSTN/IP is used **Notes:** - This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls. - For a detailed list of the available NPI/TON values, refer to Numbering Plans and Type of Number on page 169
TON **[_NumberType]**	The Type of Number (TON) assigned to this entry. - If you selected 'Unknown' for the NPI, you can select Unknown **[0].** - If you selected 'Private' for the NPI, you can select Unknown **[0],** Level 2 Regional **[1],** Level 1 Regional **[2],** PISN Specific **[3]** or Level 0 Regional (Local) **[4].** - If you selected 'E.164 Public' for the NPI, you can select Unknown **[0],** International **[1],** National **[2],** Network Specific **[3],** Subscriber [4] or Abbreviated **[6].**

Parameter	Description
	Notes: - This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls. - The default is 'Unknown'.
Presentation **[_IsPresentationRestricted]**	Determines whether Caller ID is permitted: - Not Configured = privacy is determined according to the Caller ID table (refer to Caller ID). - Allowed = sends Caller ID information when a call is made using these destination / source prefixes. - Restricted = restricts Caller ID information for these prefixes. **Notes:** - Only applicable to Number Manipulation tables for source number manipulation. - If 'Presentation' is set to 'Restricted' and 'Asserted Identity Mode' is set to 'P-Asserted', the From header in the INVITE message includes the following: From: 'anonymous' <sip: anonymous@anonymous.invalid> and 'privacy: id' header.

3.4.7.3.1 Dialing Plan Notation

The dialing plan notation applies to the Number Manipulation tables, 'Tel to IP Routing' table (refer to "Tel to IP Routing Table" on page 175), and 'IP to Trunk Group Routing' table (refer to "IP to Trunk Group Routing" on page 181). The dialing notation applies to digits entered for the destination and source prefixes to represent multiple numbers.

Table 3-40: Dialing Plan Notations

Notation	Description	Example
[n-m]	Represents a range of numbers. **Note:** Range of letters is not supported.	- **[5551200-5551300]#:** represents all numbers from 5551200 to 5551300. - **123[100-200]#:** represents all numbers from 123100 to 123200.
[n,m,...]	Represents multiple numbers. Up to three digits can be used to denote each number.	- **[2,3,4,5,6]#:** represents a one-digit number that starts with 2, 3, 4, 5, or 6. - **[11,22,33]xxx#:** represents a four-digit number that starts 11, 22, or 33. - **[111,222]xxx#:** represents a four-digit number that starts 111 or 222.
x	Represents any single digit.	**54324:** represents any number that starts with 54324.
Pound sign (#) at the end of a number	Represents the end of a number.	**54324xx#:** represents a 7-digit number that starts with 54324.
A single asterisk (*)	Represents any number.	***:** represents any number (i.e., all numbers).

The device matches the rules starting at the top of the table (i.e., top rules take precedence over lower rules). For this reason, enter more specific rules above more generic rules. For example, if you enter 551 in entry 1 and 55 in entry 2, the device applies rule 1 to numbers that start with 551 and applies rule 2 to numbers that start with 550, 552, 553, 554, 555, 556, 557, 558 and 559. However, if you enter 55 in entry 1 and 551 in entry 2, the device applies rule 1 to all numbers that start with 55 including numbers that start with 551.

3.4.7.3.2 Numbering Plans and Type of Number

Numbers are classified by their Numbering Plan Indication (NPI) and their Type of Number (TON). The device supports all NPI/TON classifications used in the standard. The list of ISDN ETSI NPI/TON values is shown in the following table:

Table 3-41: NPI/TON Values for ISDN ETSI

NPI	TON	Description
Unknown [0]	Unknown [0]	A valid classification, but one that has no information about the numbering plan.
E.164 Public [1]	Unknown [0]	A public number in E.164 format, but no information on what kind of E.164 number.
	International [1]	A public number in complete international E.164 format, e.g., 16135551234.
	National [2]	A public number in complete national E.164 format, e.g., 6135551234.
	Subscriber [4]	A public number in complete E.164 format representing a local subscriber, e.g., 5551234.
Private [9]	Unknown [0]	A private number, but with no further information about the numbering plan.
	Level 2 Regional [1]	
	Level 1 Regional [2]	A private number with a location, e.g., 3932200.
	PISN Specific [3]	
	Level 0 Regional (local) [4]	A private local extension number, e.g., 2200.

For NI-2 and DMS-100 ISDN variants, the valid combinations of TON and NPI for calling and called numbers include (Plan/Type):

- 0/0 - Unknown/Unknown
- 1/1 - International number in ISDN/Telephony numbering plan
- 1/2 - National number in ISDN/Telephony numbering plan
- 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan
- 9/4 - Subscriber (local) number in Private numbering plan

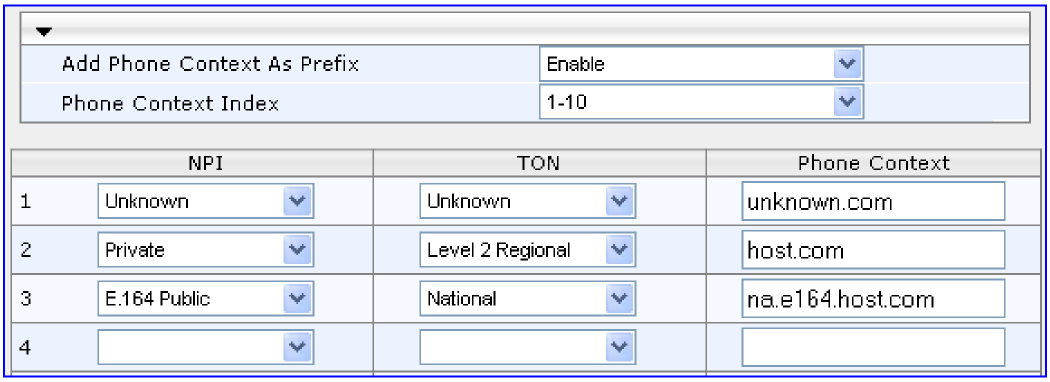
3.4.7.3.3 Mapping NPI/TON to Phone-Context

The 'Phone-Context Table' page is used to map NPI and TON to the Phone-Context SIP parameter. When a call is received from the ISDN, the NPI and TON are compared against the table and the Phone-Context value is used in the outgoing SIP INVITE message. The same mapping occurs when an INVITE with a Phone-Context attribute is received. The Phone-Context parameter appears in the standard SIP headers where a phone number is used (Request-URI, To, From, Diversion).

➢ To configure the Phone-Context tables, take these 4 steps:

1. Open the 'Phone Context Table' page (**Configuration** tab > **Protocol Configuration** menu > **Manipulation Tables** submenu > **Phone Context Table** page item).

Figure 3-69: Phone Context Table Page



Add Phone Context As Prefix: Enable

Phone Context Index: 1-10

	NPI	TON	Phone Context
1	Unknown	Unknown	unknown.com
2	Private	Level 2 Regional	host.com
3	E.164 Public	National	na.e164.host.com
4			

2. Configure the Phone Context table according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Notes:

- Several rows with the same NPI-TON or Phone-Context are allowed. In such a scenario, a Tel-to-IP call uses the first match.
- Phone-Context '+' is a unique case as it doesn't appear in the Request-URI as a Phone-Context parameter. Instead, it's added as a prefix to the phone number. The '+' isn't removed from the phone number in the IP-to-Tel direction.
- You can also configure the Phone Context table using the *ini* file table parameter PhoneContext (refer to "Number Manipulation and Routing Parameters" on page 313).

Table 3-42: Phone-Context Parameters Description

Parameter	Description
Add Phone Context As Prefix **[AddPhoneContextAsPrefix]**	Determines whether the received Phone-Context parameter is added as a prefix to the outgoing ISDN SETUP message with Called and Calling numbers. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Enable = Enable.

Parameter	Description
NPI	Select the Number Plan assigned to this entry. ▪ **[0]** Unknown = Unknown (default) ▪ **[1]** E.164 Public = E.164 Public ▪ **[9]** Private = Private For a detailed list of the available NPI/TON values, refer to Numbering Plans and Type of Number on page 169.
TON	Select the Number Type assigned to this entry. ▪ If you selected Unknown as the NPI, you can select Unknown **[0]**. ▪ If you selected Private as the NPI, you can select Unknown **[0]**, Level 2 Regional **[1]**, Level 1 Regional **[2]**, PSTN Specific **[3]**, or Level 0 Regional (Local) **[4]**. ▪ If you selected E.164 Public as the NPI, you can select Unknown **[0]**, International **[1]**, National **[2]**, Network Specific **[3]**, Subscriber **[4]**, or Abbreviated **[6]**.
Phone Context	The Phone-Context SIP URI parameter.

3.4.7.4 Configuring the Routing Tables

The **Routing Tables** submenu allows you to configure the device's call routing. This submenu includes the following page items:

- Routing General Parameters (refer to "Routing General Parameters" on page 171)
- Tel to IP Routing (refer to "Tel to IP Routing Table" on page 175)
- Outbound IP Routing (refer to “Outbound IP Routing Table” on page 178)
- IP to Trunk Group Routing (refer to "IP to Trunk Group Routing" on page 181)
- Inbound IP Routing (refer to “Inbound IP Routing Table” on page 184)
- Internal DNS Table (refer to "Internal DNS Table" on page 186)
- Internal SRV Table (refer to "Internal SRV Table" on page 187)
- Reasons for Alternative Routing (refer to "Reasons for Alternative Routing" on page 188)
- Release Cause Mapping (refer to “Release Cause Mapping” on page 189)

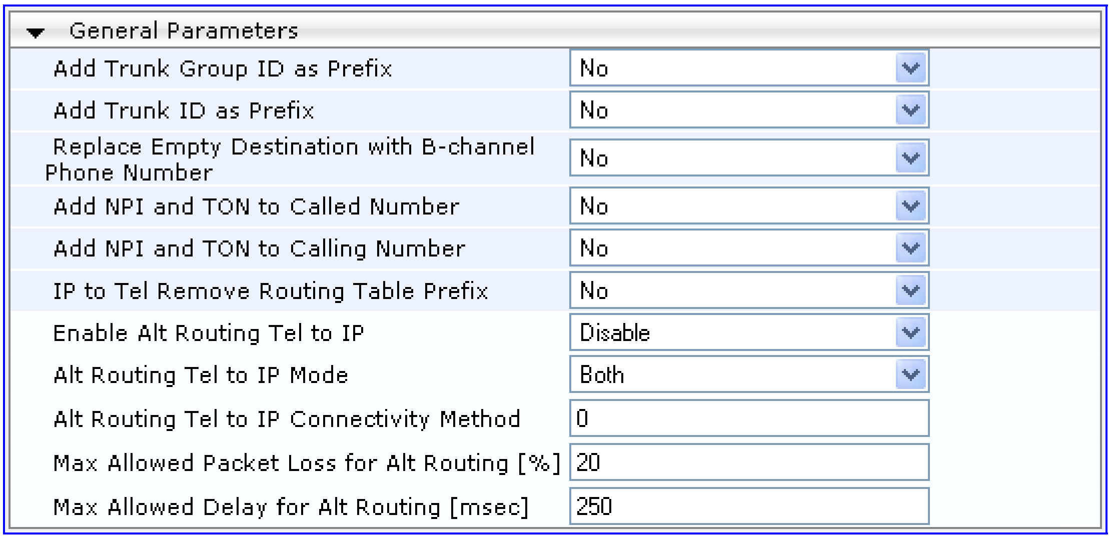
3.4.7.4.1 Routing General Parameters

The 'Routing General Parameters' page allows you to configure the device's IP-to-Tel and Tel-to-IP routing parameters.

➢ To configure the general routing parameters, take these 4 steps:

1. Open the 'Routing General Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Routing General Parameters** page item).

Figure 3-70: Routing General Parameters Page



▼ General Parameters

Add Trunk Group ID as Prefix	No
Add Trunk ID as Prefix	No
Replace Empty Destination with B-channel Phone Number	No
Add NPI and TON to Called Number	No
Add NPI and TON to Calling Number	No
IP to Tel Remove Routing Table Prefix	No
Enable Alt Routing Tel to IP	Disable
Alt Routing Tel to IP Mode	Both
Alt Routing Tel to IP Connectivity Method	0
Max Allowed Packet Loss for Alt Routing [%]	20
Max Allowed Delay for Alt Routing [msec]	250

2. Configure the general parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-43: Routing General Parameters Description

Parameter	Description
Add Trunk Group ID as Prefix **[AddTrunkGroupAsPrefix]**	Determines whether the device's Trunk Group ID is added as a prefix to the destination phone number for Tel-to-IP calls. ▪ **[0]** No = Don't add Trunk Group ID as prefix (default). ▪ **[1]** Yes = Add Trunk Group ID as prefix to called number. **Notes:** ▪ This option can be used to define various routing rules. ▪ To use this feature, you must configure the Trunk Group IDs (refer to "Configuring the Trunk Group Table" on page 195).
Add Trunk ID as Prefix **[AddPortAsPrefix]**	Determines whether the Trunk ID is added as a prefix to the called number for Tel-to-IP calls. ▪ **[0]** No = Don't add Trunk ID as prefix (default). ▪ **[1]** Yes = Enable add Trunk ID as prefix. If enabled, the Trunk ID (single digit in the range 1 to 8) is added as a prefix to the called (destination) phone number. This option can be used to define various routing rules.
Replace Empty Destination with B-channel Phone Number **[ReplaceEmptyDstWithPortNumber]**	Determines whether the internal channel number is used as the destination number if the called number is missing. ▪ **[0]** No (default) ▪ **[1]** Yes **Note:** Applicable only for Tel-to-IP calls and if the called number is missing.
Add NPI and TON to Calling Number	Determines whether Numbering Plan Indicator (NPI) and Type of Numbering (TON) are added to the Calling Number

Parameter	Description
[AddNPIandTON2CallingNumber]	for Tel-to-IP calls. ▪ **[0]** No = Do not change the Calling Number (default). ▪ **[1]** Yes = Add NPI and TON to the Calling Number ISDN Tel-to-IP call. For example: After receiving a Calling Number of 555, NPI of 1, and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.
Add NPI and TON to Called Number **[AddNPIandTON2CalledNumber]**	Determines whether NPI and TON are added to the Called Number for Tel-to-IP calls. ▪ **[0]** No = Do not change the Called Number (default). ▪ **[1]** Yes = Add NPI and TON to the Called Number of ISDN Tel-to-IP call. For example: After receiving a Called Number of 555, NPI of 1 and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.
IP to Tel Remove Routing Table Prefix **[RemovePrefix]**	Determines whether the device removes the prefix from the destination number for IP-to-Tel calls. ▪ **[0]** No = Don't remove prefix (default) ▪ **[1]** Yes = Remove the prefix (defined in the 'IP to Trunk Group Routing' table - refer to "IP to Trunk Group Routing" on page 181) from a telephone number for an IP-to-Tel call, before forwarding it to Tel. For example: To route an incoming IP-to-Tel call with destination number 21100, the 'IP to Trunk Group Routing' table is scanned for a matching prefix. If such a prefix is found (e.g., 21), then before the call is routed to the corresponding Trunk Group, the prefix (21) is removed from the original number, and therefore, only 100 remains. **Notes:** ▪ Applicable only if number manipulation is performed after call routing for IP-to-Tel calls (i.e., RouteModeIP2Tel parameter is set to 0). ▪ Similar operation (of removing the prefix) is also achieved by using the usual number manipulation rules.
Source IP Address Input **[SourceIPAddressInput]**	Determines the IP address that the device uses to determine the source of incoming INVITE messages for IP-to-Tel routing. ▪ **[-1]** = Not configured (default). ▪ **[0]** SIP Contact Header = Use the IP address received in the Contact header of the incoming INVITE message. ▪ **[1]** Layer 3 Source IP = Use the actual IP address (Layer 3) from which the SIP packet was received. **Note:** If the IP-to-IP feature is enabled (i.e., supported by the Feature Key and EnableSBC is set to 1 - refer to “SBC Configuration” on page 163), this parameter is automatically set to 1. If the IP-to-IP feature is disabled, this parameter is automatically set to 0.

Parameter	Description
Enable Alt Routing Tel to IP **[AltRoutingTel2IPEnable]**	Enables the Alternative Routing feature for Tel-to-IP calls. ▪ **[0]** Disable = Disables the Alternative Routing feature (default). ▪ **[1]** Enable = Enables the Alternative Routing feature. ▪ **[2]** Status Only = The Alternative Routing feature is disabled, but read-only information on the Quality of Service of the destination IP addresses is provided. For information on the Alternative Routing feature, refer to "Configuring Alternative Routing (Based on Connectivity and QoS)" on page 361.
Alt Routing Tel to IP Mode **[AltRoutingTel2IPMode]**	Determines the event(s) reason for triggering Alternative Routing. ▪ **[0]** None = Alternative routing is not used. ▪ **[1]** Connectivity = Alternative routing is performed if ping to initial destination fails. ▪ **[2]** QoS = Alternative routing is performed if poor QoS is detected. ▪ **[3]** Both = Alternative routing is performed if either ping to initial destination fails, poor Quality of Service is detected, or DNS host name is not resolved (default). **Notes:** ▪ QoS is quantified according to delay and packet loss calculated according to previous calls. QoS statistics are reset if no new data is received within two minutes. For information on the Alternative Routing feature, refer to "Configuring Alternative Routing (Based on Connectivity and QoS)" on page 361. ▪ To receive quality information (displayed in the 'Quality Status' and 'Quality Info.' fields in "IP Connectivity" on page 252) per destination, this parameter must be set to 2 or 3.
Alt Routing Tel to IP Connectivity Method **[AltRoutingTel2IPConnMethod]**	Determines the method used by the device for periodically querying the connectivity status of a destination IP address. ▪ **[0]** ICMP Ping (default) = Internet Control Message Protocol (ICMP) ping messages. ▪ **[1]** SIP OPTIONS = The remote destination is considered offline if the latest OPTIONS transaction timed out. Any response to an OPTIONS request, even if indicating an error, brings the connectivity status to online.
Alt Routing Tel to IP Keep Alive Time **[AltRoutingTel2IPKeepAliveTime]**	Defines the time interval (in seconds) between SIP OPTIONS Keep-Alive messages used for the IP Connectivity application. The valid range is 5 to 2,000,000. The default value is 60.
Max Allowed Packet Loss for Alt Routing [%] **[IPConnQoSMaxAllowedPL]**	Packet loss percentage at which the IP connection is considered a failure and Alternative Routing mechanism is activated. The range is 1 to 20%. The default value is 20%.

Parameter	Description
Max Allowed Delay for Alt Routing [msec] **[IPConnQoSMaxAllowedDelay]**	Transmission delay (in msec) at which the IP connection is considered a failure and Alternative Routing mechanism is activated. The range is 100 to 1000. The default value is 250.

3.4.7.4.2 Tel to IP Routing Table

The 'Tel to IP Routing' page provides a table for configuring up to up to 50 routing rules for Tel-to-IP calls, where Tel calls are routed to destinations based on IP address (or IP Group).

Note: The 'Tel to IP Routing' page appears only if the parameter EnableSBC is set to 0 (default) in "SBC Configuration" on page 163. If this parameter is enabled, the 'Outbound IP Routing Table' page appears instead (refer to "Outbound IP Routing Table" on page 178 for a description of this page).

This routing table associates called and/or calling telephone number prefixes (originating from a specific Trunk Group), with a destination IP address (or Fully Qualified Domain Name - FQDN) or IP Group. When a call is routed by the device (i.e., a Proxy server isn't used), the called and calling numbers are compared to the list of prefixes in this table. Calls that match these prefixes are sent to the corresponding IP address. If the number dialed does not match these prefixes, the call is not made.

When using a Proxy server, you do not need to configure this table unless you require one of the following:

- Fallback routing when communication with Proxy servers is lost.
- Implement the 'Filter Calls to IP' and 'IP Security' features.
- Obtain different SIP URI host names (per called number).
- Assign IP profiles.

Note that for this table to take precedence over a Proxy for routing calls, set the parameter PreferRouteTable to 1. The device checks the 'Destination IP Address' field in this table for a match with the outgoing call. A Proxy is used only if a match is not found.

Possible uses for Tel-to-IP routing include the following:

- Fallback to internal routing table if there is no communication with the Proxy servers.
- Call Restriction (when Proxy isn't used): rejects all outgoing Tel-to-IP calls that are associated with the destination IP address 0.0.0.0.
- IP Security: When the IP Security feature is enabled (SecureCallFromIP = 1), the device accepts only those IP-to-Tel calls with a source IP address defined in the 'Tel to IP Routing' table.
- Filter Calls to IP: When a Proxy is used, the device checks the 'Tel to IP Routing' table before a telephone number is routed to the Proxy. If the number is not allowed (number isn't listed or a Call Restriction routing rule is applied), the call is released.
- Always Use Routing Table: When this feature is enabled (AlwaysUseRouteTable = 1), even if a Proxy server is used, the SIP URI host name in the sent INVITE message is obtained from this table. Using this feature, you can assign a different SIP URI host name for different called and/or calling numbers.

- Assign Profiles to destination addresses (also when a Proxy is used).
- Alternative Routing (when a Proxy isn't used): an alternative IP destination for telephone number prefixes is available. To associate an alternative IP address to a called telephone number prefix, assign it with an additional entry (with a different IP address), or use an FQDN that resolves into two IP addresses. The call is sent to the alternative destination when one of the following occurs:
    - No ping to the initial destination is available, poor QoS (delay or packet loss, calculated according to previous calls) is detected, or a DNS host name is not resolved. For detailed information on Alternative Routing, refer to "Configuring Alternative Routing (Based on Connectivity and QoS" on page 361.
    - A release reason defined in the 'Reasons for Alternative Tel to IP Routing' table is received (refer to "Reasons for Alternative Routing" on page 188).

  Alternative routing (using this table) is commonly implemented when there is no response to an INVITE message (after INVITE retransmissions). The device then issues an internal 408 'No Response' implicit release reason. If this reason is included in the 'Reasons for Alternative Routing' table, the device immediately initiates a call to the redundant destination using the next matched entry in the 'Tel to IP Routing' table. Note that if a domain name in this table is resolved into two IP addresses, the timeout for INVITE retransmissions can be reduced by using the parameter 'Number of RTX Before Hotswap'.

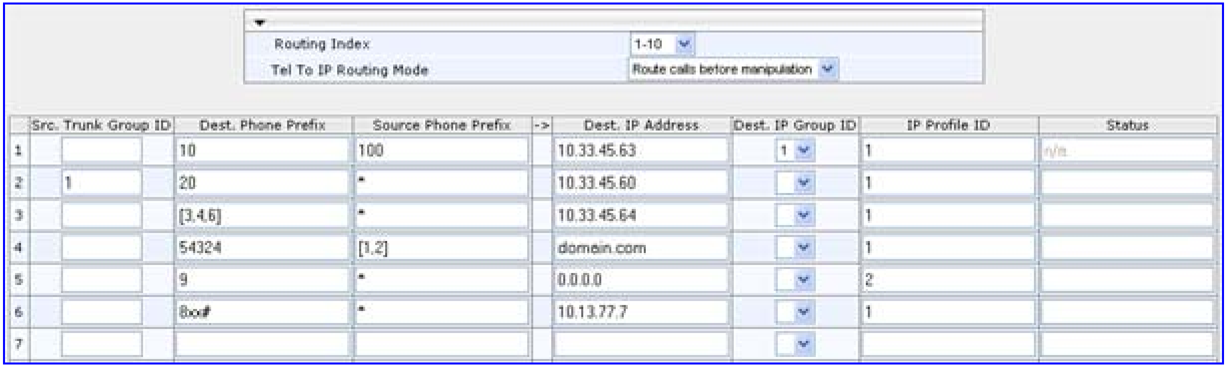
Notes:

- If the alternative routing destination is the device itself, the call can be configured to be routed back to the PSTN. This feature is referred to as 'PSTN Fallback', meaning that if poor voice quality occurs over the IP network, the call is routed through the legacy telephony system (PSTN).
- Tel-to-IP routing can be performed before or after applying the number manipulation rules. To control when number manipulation is performed, use the 'Tel to IP Routing Mode' (or RouteModeTel2IP *ini* file) parameter, described in the table below.
- You can also configure the 'Tel to IP Routing' table using the *ini* file table parameter Prefix (refer to "Number Manipulation and Routing Parameters" on page 313).

➢ To configure the Tel to IP Routing table, take these 5 steps:

1. Open the 'Tel to IP Routing' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Tel to IP Routing** page item).

Figure 3-71: Tel to IP Routing Page



Routing Index: 1-10
Tel To IP Routing Mode: Route calls before manipulation

	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Dest. IP Group ID	IP Profile ID	Status
1		10	100		10.33.45.63	1	1	n/a
2	1	20	*		10.33.45.60		1	
3		[3,4,6]	*		10.33.45.64		1	
4		54324	[1,2]		domain.com		1	
5		9	*		0.0.0.0		2	
6		8xx#	*		10.13.77.7		1	
7								

2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.

3. Configure the Tel to IP Routing table according to the table below.

4. Click the **Submit** button to save your changes.

5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-44: Tel to IP Routing Table Parameters Description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Tel to IP Routing Mode
<b>[RouteModeTel2IP]</b></td><td>Determines whether to route Tel calls to IP before or after manipulation of destination number.
▪ <b>[0]</b> Route calls before manipulation = Tel-to-IP calls are routed before the number manipulation rules are applied (default).
▪ <b>[1]</b> Route calls after manipulation = Tel-to-IP calls are routed after the number manipulation rules are applied.
<b>Notes:</b> Not applicable if outbound Proxy routing is used.</td></tr>
<tr><td>Src. Trunk Group ID
<b>[PREFIX_SrcTrunkGroupID]</b></td><td>The source Trunk Group for Tel-to-IP calls.
The range is 1-99.
<b>Notes:</b>
▪ If this parameter is not required in the routing rule, leave the field empty.
▪ To denote any Trunk Group, you can enter the asterisk (*) symbol.</td></tr>
<tr><td>Dest. Phone Prefix
<b>[PREFIX_DestinationPrefix]</b></td><td>Represents a called telephone number prefix. The prefix can be 1 to 19 digits long. An asterisk (*) represents all numbers.</td></tr>
<tr><td>Source Phone Prefix
<b>[PREFIX_SourcePrefix]</b></td><td>Represents a calling telephone number prefix. The prefix can be 1 to 19 digits long. An asterisk (*) represents all numbers.</td></tr>
<tr><td colspan="2">All Tel calls matching all or any combination of the above routing rules are subsequently sent to the destination IP address defined below.
<b>Notes:</b>
▪ For alternative routing, additional entries of the same prefixes can be configured.
▪ For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168.</td></tr>
<tr><td>Dest. IP Address
<b>[PREFIX_DestAddress]</b></td><td>The destination IP address (in dotted decimal notation) to where these calls must be sent. Domain names (e.g., domain.com) can be used instead of IP addresses.
<b>Notes:</b>
▪ If you select a destination IP Group (in the 'Dest IP Group ID' field below), then the IP address you define in this 'Dest IP Address' field is not used for routing and therefore, not required.
▪ To discard outgoing IP calls of a specific Tel-to-IP routing rule, enter 0.0.0.0. For example, if you want to prohibit dialing of international calls, then in the 'Dest Phone Prefix' field, enter 00 and in the 'Dest IP Address' field, enter 0.0.0.0.
▪ For routing calls between phones connected to the device (i.e., local routing), enter the device's IP address. When the device's IP address is unknown (e.g., when DHCP is used), enter the IP address 127.0.0.1.</td></tr>
</table>

Parameter	Description
	▪ When using domain names, you must enter a DNS server IP address or alternatively, define these names in the 'Internal DNS Table' (refer to "Internal DNS Table" on page 186).
Port **[PREFIX_DestPort]**	The destination port to where you want to route the Tel-to-IP call.
Transport Type **[PREFIX_TransportType]**	The transport layer type for sending the Tel-to-IP calls: ▪ **[-1]** Not Configured ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When 'Not Configured' is selected, the transport type defined by the parameter SIPTransportType (refer to "SIP General Parameters" on page 121) is used.
Dest IP Group ID **[PREFIX_DestIPGroupID]**	The IP Group (1-9) to where you want to route the Tel-to-IP call. The SIP INVITE messages are sent to the IP address(es) of the Proxy Set that is associated with the selected IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Dest IP Address' field). However, if both parameters are configured, the INVITE message is sent only to the IP Group. If the parameter AlwaysUseRouteTable is set to 1 (in the 'IP Group' table, refer to "Configuring the IP Groups" on page 201), the request URI host name in the INVITE message is set to the value of the parameter 'Dest IP Address' (if not empty); otherwise, it is set to the value of the parameter 'SIP Group Name' (defined in the 'IP Group' table). **Note:** To configure Proxy Sets, refer to "Proxy Sets Table" on page 141.
IP Profile ID **[PREFIX_ProfileId]**	The IP Profile ID (configured in "Configuring the Profile Definitions" on page 190) assigned to this routing rule entry for the IP destination.
Status	A read-only field representing the Quality of Service of the destination IP address: ▪ n/a = Alternative Routing feature is disabled. ▪ OK = IP route is available. ▪ Ping Error = No ping to IP destination; route is not available. ▪ QoS Low = Bad QoS of IP destination; route is not available. ▪ DNS Error = No DNS resolution (only when domain name is used instead of an IP address).

3.4.7.4.3 Outbound IP Routing Table

The 'Outbound IP Routing Table' page allows you to configure the device for routing outbound (i.e., sent) IP-to-IP calls. This table routes inbound IP calls (identified in "Inbound IP Routing Table" on page 184) received from an IP Group (refer to "Configuring the IP Groups" on page 201) to a specific IP Group destination (or IP address).

> **Note:** The 'Outbound IP Routing Table' page appears only if the parameter EnableSBC is set to 1 (i.e., enabled) in "SBC Configuration" on page 163. If this parameter is not enabled (default), the 'Tel to IP Routing' page appears instead (refer to "Tel to IP Routing Table" on page 175 for a description of this page).

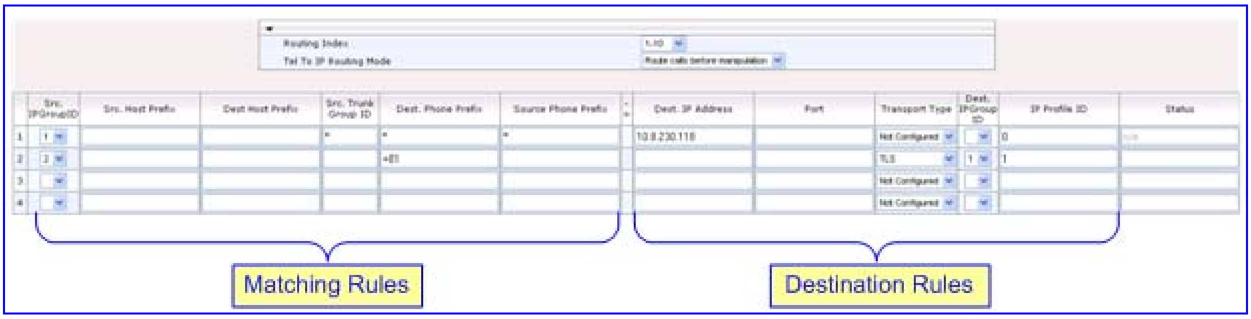
This table allows you to configure the device's routing rules for sending inbound IP calls matching some or all of the following criteria to a destination IP address or IP Group:

- Source IP Group
- Source host prefix
- Destination host prefix
- Trunk Group
- Destination telephone prefix
- Source telephone prefix

➢ To configure Outbound IP Routing, take these 5 steps:

1. Open the 'Outbound IP Routing Table' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Tel to IP Routing** page item).

Figure 3-72: Outbound IP Routing Page



Routing Index: 1-10

Tel To IP Routing Mode: Route calls before manipulation

	Src. IPGroupID	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix		Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	IP Profile ID	Status
1	1			*	*	*		10.8.230.118		Not Configured		0	[illegible]
2	2				+81					TLS	1	1	
3										Not Configured			
4										Not Configured			

2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.
3. Configure the Outbound IP Routing table according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-45: Outbound IP Routing Table Description

Parameter	Description
Tel to IP Routing Mode **[RouteModeTel2IP]**	Determines whether to route the inbound IP calls to the IP destination before or after manipulation of destination number. ▪ **[0]** Route calls before manipulation = IP-to-IP calls are routed before the number manipulation rules are applied (default). ▪ **[1]** Route calls after manipulation = IP-to-IP calls are routed after the number manipulation rules are applied. **Note:** Not applicable if outbound Proxy routing is used.

Parameter	Description
Src. IPGroupID **[PREFIX_SrcIPGroupID]**	The IP Group ID from where the IP-to-IP call originated. Typically, the IP Group of an incoming INVITE is determined according to the 'Inbound IP Routing' table. To denote all IP Groups, leave the field empty. **Notes:** ▪ If this Source IP Group has a Serving IP Group, then all calls originating from this Source IP Group are sent to the Serving IP Group. In this scenario, this table is used only if the parameter PreferRouteTable is set to 1. ▪ For defining IP Groups, refer to "Configuring the IP Groups" on page 201.
Src. Host Prefix **[PREFIX_SrcHostPrefix]**	The prefix of the SIP URI host name in the From header of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. To denote any prefix, use the asterisk (*) symbol
Dest. Host Prefix **[PREFIX_DestHostPrefix]**	The request SIP URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. To denote any prefix, use the asterisk (*) symbol
Src. Trunk Group ID **[PREFIX_SrcTrunkGroupID]**	The source Trunk Group (1-99) for Tel-to-IP calls. For IP-to-IP calls, this parameter is not required (i.e., leave the field empty). To denote any Trunk Group, leave this field empty. **Note:** For defining Trunk Groups, refer to "Configuring the Trunk Group Table" on page 195.
Dest. Phone Prefix **[PREFIX_DestinationPrefix]**	Represents a called telephone number prefix. The prefix can be 1 to 19 digits long. An asterisk (*) represents all numbers.
Source Phone Prefix **[PREFIX_SourcePrefix]**	Represents a calling telephone number prefix. The prefix can be 1 to 19 digits long. An asterisk (*) represents all numbers.
Outbound IP calls matching all or any combination of the above routing rules are subsequently sent to the destination IP address or IP Group defined below. **Notes:** ▪ For alternative routing, additional entries of the same prefixes can be configured. ▪ For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168.	
Dest. IP Address **[PREFIX_DestAddress]**	The destination IP address to where the outbound call is sent. Domain names (e.g., domain.com) can be used instead of IP addresses. **Notes:** ▪ If you select a destination IP Group (in the 'Dest IP Group ID' field below), then the IP address you define in this 'Dest IP Address' field is not used for routing and therefore, not required. ▪ When using domain names, you must enter a DNS server IP address or alternatively, define these names in the 'Internal DNS Table' (refer to "Internal DNS Table" on page 186). ▪ To discard outgoing IP calls, define the IP address as 0.0.0.0. ▪ The IP address 127.0.0.1 can be used when the IP address of the device itself is unknown (for example, when DHCP is used).
Port **[PREFIX_DestPort]**	The destination port.

Parameter	Description
Transport Type **[PREFIX_TransportType]**	The transport layer type for sending the outbound SIP IP calls: ▪ **[-1]** Not Configured ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When 'Not Configured' is selected, the transport type defined by the parameter SIPTransportType (refer to "SIP General Parameters" on page 121) is used.
Dest. IP Group ID **[PREFIX_DestIPGroupID]**	The IP Group (1 to 9) to where you want to route the outbound IP-to-IP call. The INVITE messages are sent to the IP address(es) defined for the Proxy Set that is associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Dest IP Address' field above). However, if both parameters are configured, the INVITE message is sent only to the IP Group. If the destination IP Group is of type USER, the device searches for a match between the request URI (of the received INVITE) to an AOR registration record in the device's internal database. The INVITE is then sent to the IP address of the registered contact. If the parameter 'AlwaysUseRouteTable' (AlwaysUseRouteTable) is set to 'Enable' (1) in the ‘IP Group’ table (refer to "Configuring the IP Groups" on page 201), the request SIP URI host name in the INVITE message is set to the value of the parameter 'Dest IP Address' (if defined); otherwise, it is set to the value of the parameter 'SIP Group Name' (defined in the ‘IP Group’ table). **Note:** This parameter is also used as the ‘Serving IP Group’ in the ‘Account’ table for acquiring authentication user/password for this call.
IP Profile ID **[PREFIX_ProfileId]**	IP Profile ID (defined in "IP Profile Settings" on page 193) assigned to the outbound IP call. This allows you to assign many different configuration attributes (e.g., voice coders) to this IP Group outbound routing rule.
Status	A read-only field representing the Quality of Service of the destination IP address: ▪ n/a = Alternative Routing feature is disabled. ▪ OK = IP route is available. ▪ Ping Error = No ping to IP destination; route is not available. ▪ QoS Low = Bad QoS of IP destination; route is not available. ▪ DNS Error = No DNS resolution (only when domain name is used instead of an IP address).

3.4.7.4.4 IP to Trunk Group Routing Table

The 'IP to Trunk Group Routing Table' page provides a table for routing incoming IP calls to groups of channels (E1/T1 B-channels)called Trunk Groups. Trunk Group ID's are assigned to the device's channels in the 'Trunk Group Table' page (refer to “Configuring the Trunk Group Table” on page 195). You can add up to 24 IP-to-Trunk Group routing rules in the table.

> **Note:** The 'IP to Trunk Group Routing Table' page appears only if the parameter EnableSBC is set to 0 (default) in "SBC Configuration" on page 163. If this parameter is enabled, the 'Inbound IP Routing Table' page appears instead (refer to "Inbound IP Routing Table" on page 184 for a description of this page).

The IP-to-Tel calls are routed to Trunk Groups according to any one of the following (or a combination thereof) criteria:

- Destination and source host prefix
- Destination and source phone prefix
- Source IP address

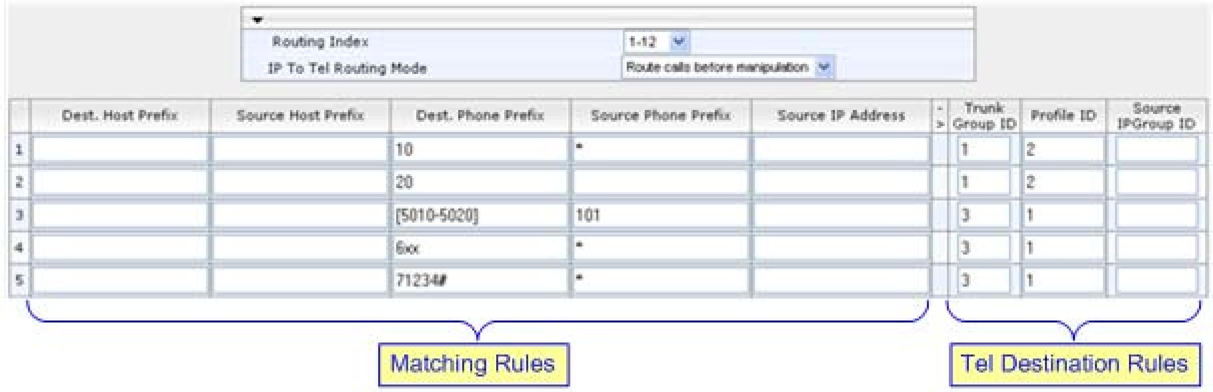
Once the call is routed to the specific Trunk Group, the call is sent to the device's channels pertaining to that Trunk Group. The specific channel within the Trunk Group to which the call is sent is determined according to the Trunk Group's channel selection mode. This channel selection mode can be defined per Trunk Group (refer to "Configuring the Trunk Group Settings" on page 197) or for all Trunk Groups using the global parameter ChannelSelectMode.(refer to "SIP General Parameters" on page 121).

> **Notes:**
>
> - When a call release reason (defined in "Reasons for Alternative Routing" on page 188) is received for a specific IP-to-Tel call, an alternative Trunk Group for that call can be configured. This is performed by assigning the call to an additional routing rule in the table (i.e., repeat the same routing rule, but with a different Trunk Group ID).
> - You can also configure the 'IP to Trunk Group Routing' table using the *ini* file table parameter PSTNPrefix (refer to "Number Manipulation and Routing Parameters" on page 313).

➢ To configure the IP to Trunk Group Routing table, take these 5 steps:

1. Open the 'IP to Trunk Group Routing' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **IP to** Trunk **Group Routing** page item).

Figure 3-73: IP to Trunk Group Routing Table Page



Routing Index: 1-12

IP To Tel Routing Mode: Route calls before manipulation

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	- >	Trunk Group ID	Profile ID	Source IPGroup ID
1			10	*			1	2	
2			20				1	2	
3			[5010-5020]	101			3	1	
4			6xx	*			3	1	
5			71234#	*			3	1	

2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.

3. Configure the table according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes so they are available after a power failure, refer to "Saving Configuration" on page 230.

Table 3-46: IP to Trunk Group Routing Table Description

Parameter	Description
IP to Tel Routing Mode **[RouteModeIP2Tel]**	Determines whether to route IP calls to the Trunk Group before or after manipulation of destination number (configured in "Configuring the Number Manipulation Tables" on page 164). ▪ **[0]** Route calls before manipulation = IP-to-Tel calls are routed before the number manipulation rules are applied (default). ▪ **[1]** Route calls after manipulation = IP-to-Tel calls are routed after the number manipulation rules are applied.
Dest. Host Prefix **[PstnPrefix_DestHostPrefix]**	The request URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. **Note:** For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168. However, the asterisk (*) wildcard cannot be used to depict any source host prefix.
Source Host Prefix **[PstnPrefix_SrcHostPrefix]**	The From URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty.. **Notes:** ▪ For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168. However, the asterisk (*) wildcard cannot be used to depict any source host prefix. ▪ If the P-asserted-ID header is present in the incoming INVITE message, then the parameter 'Source Host Prefix' is compared to the P-Asserted-ID URI hostname and not to the From header.
Dest. Phone Prefix **[PstnPrefix_DestPrefix]**	Represents a called telephone number prefix. The prefix can be 1 to 49 digits long. **Note:** For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168.
Source Phone Prefix **[PstnPrefix_SourcePrefix]**	Represents a calling telephone number prefix. The prefix can be 1 to 49 digits long. **Note:** For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168.
Source IP Address **[PstnPrefix_SourceAddress]**	The source IP address of an IP-to-Tel call (obtained from the Contact header in the INVITE message) that can be used for routing decisions. **Notes:** ▪ You can configure from where the source IP address is obtained, using the parameter SourceIPAddressInput (refer to "Routing General Parameters" on page 171). ▪ The source IP address can include the "x" wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. ▪ The source IP address can include the asterisk (*) wildcard to

Parameter	Description
	represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.
Trunk Group ID **[PstnPrefix_TrunkGroupId]**	The Trunk Group to which incoming SIP calls are assigned that match all or any combination (including only a single parameter) of the parameters described above.
Profile ID **[PstnPrefix_ProfileId]**	The IP Profile (configured in "IP Profile Settings" on page 193) that is assigned to the routing rule.
Source IP Group ID **[PstnPrefix_SrcIPGroupID]**	The source IP Group (1-9) associated with the incoming IP-to-Tel call. This is the IP Group from where the INVITE message originated. This IP Group can later be used as the 'Serving IP Group' in the Account table (refer to "Configuring the Account Table" on page 204) for obtaining authentication user name/password for this call.

3.4.7.4.5 Inbound IP Routing Table

The 'Inbound IP Routing Table' page allows you to identify received calls as inbound IP-to-IP calls and assign them to an IP Group (defined in "Configuring the IP Groups" on page 201), termed the *Source* IP Group. This table identifies these IP calls based on any combination of the following criteria rules:

- Destination and source host prefixes
- Destination and source telephone number prefixes
- Source IP address

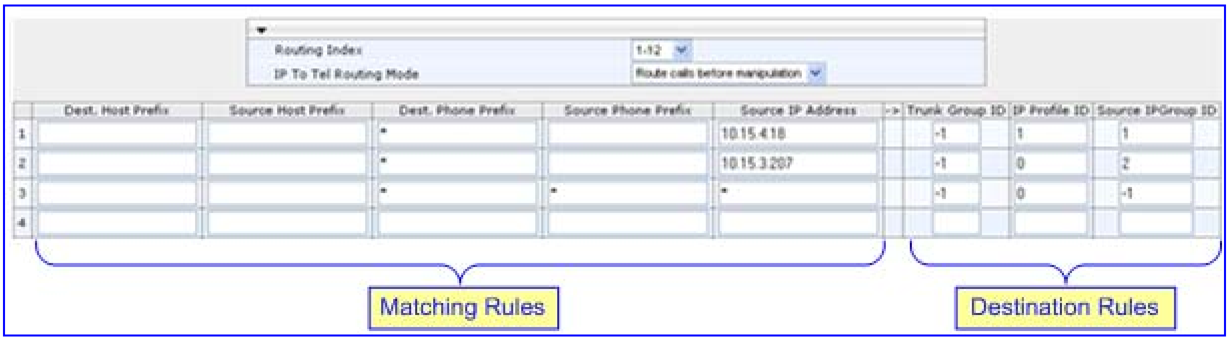
Assigning these IP calls to Trunk Group ID '-1' identifies them as inbound IP-to-IP calls. These calls, now pertaining to an IP Group, can later be routed to an outbound destination IP Group (refer to "Outbound IP Routing Table" on page 178).

Note: The 'Inbound IP Routing Table' page appears only if the parameter EnableSBC is set to 1 (i.e., enabled) in "SBC Configuration" on page 163. If this parameter is not enabled (default), the 'IP to Trunk Group Routing Table' page appears instead (refer to "IP to Trunk Group Routing Table" on page 181 for a description of this page).

➢ To configure Inbound Routing, take these 5 steps:

1. Open the 'Inbound IP Routing Table' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **IP to Trunk Group Routing** page item).

Figure 3-74: Inbound IP Routing Table



Routing Index: 1-12
IP To Tel Routing Mode: Route calls before manipulation

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Trunk Group ID	IP Profile ID	Source IPGroup ID
1			*		10.15.4.18		-1	1	1
2			*		10.15.3.207		-1	0	2
3			*	*	*		-1	0	-1
4									

2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.
3. Configure the table according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes so they are available after a power fail, refer to "Saving Configuration" on page 230.

Table 3-47: Inbound IP Routing Table Description

Parameter	Description
IP to Tel Routing Mode **[RouteModeIP2Tel]**	Determines whether to route the IP calls before or after manipulation of the destination number (configured in "Configuring the Number Manipulation Tables" on page 164). ▪ **[0]** Route calls before manipulation = IP-to-IP calls are routed before the number manipulation rules are applied (default). ▪ **[1]** Route calls after manipulation = IP-to-IP outbound calls are routed after the number manipulation rules are applied.
Dest. Host Prefix **[PstnPrefix_DestHostPrefix_**	The Request URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any destination host prefix.
Source Host Prefix **[PstnPrefix_SrcHostPrefix]**	The From header URI host name prefix of the incoming INVITE message. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any source host prefix.
Dest. Phone Prefix **[PstnPrefix_DestPrefix]**	The called telephone number prefix. The prefix can be 1 to 49 digits long. **Note:** For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168.
Source Phone Prefix **[PstnPrefix_SourcePrefix]**	The calling telephone number prefix. The prefix can be 1 to 49 digits long. **Note:** For notations representing multiple numbers, refer to "Dialing Plan Notation" on page 168.
Source IP Address **[PstnPrefix_SourceAddress]**	The source IP address of an IP-to-IP call (obtained from the Contact header in the SIP INVITE message). **Notes:** ▪ The source IP address can include the letter "x" wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. ▪ The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.
Inbound SIP IP calls matching all or any combination of the above routing rules are subsequently assigned to the IP Group selected below.	
Trunk Group ID **[PstnPrefix_TrunkGroupId]**	Identifies these calls as IP-to-IP calls when set to -1.
IP Profile ID **[PstnPrefix_ProfileId]**	IP profile (configured in "IP Profile Settings" on page 193) assigned to the inbound IP-to-IP call.

Parameter	Description
Source IP Group ID **[PstnPrefix_SrcIPGroupID]**	The IP Group (1-9) to which you want to assign this inbound IP-to-IP call. This defines the IP Group (configured in the "Configuring the IP Groups" on page 201) from where the SIP INVITE message is received. This IP Group can later be used in the 'Outbound IP Routing' table, and as the Serving IP Group in the 'Account' table for obtaining authentication user name/password for this call.

3.4.7.4.6 Internal DNS Table

The 'Internal DNS Table' page, similar to a DNS resolution is used to translate up to 20 host (domain) names into IP addresses (e.g., when using the 'Tel to IP Routing' table or 'Outbound IP Routing' table if EnableSBC is enabled). Up to four different IP addresses can be assigned to the same host name, typically used for alternative routing (for Tel-to-IP call routing).

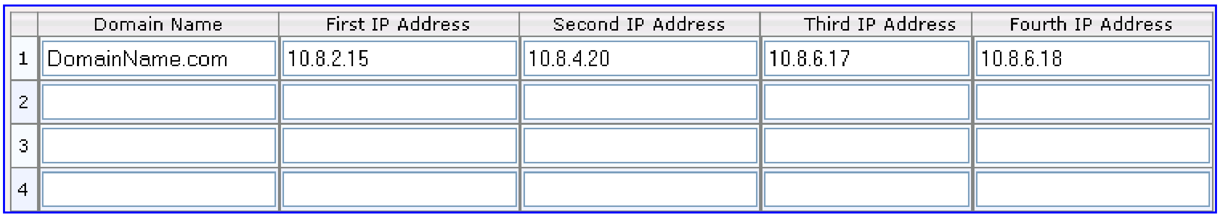
Notes:

- The device initially attempts to resolve a domain name using the Internal DNS table. If the domain name isn't listed in the table, the device performs a DNS resolution using an external DNS server.
- You can also configure the DNS table using the *ini* file table parameter DNS2IP (refer to "Networking Parameters" on page 260).

➢ To configure the internal DNS table, take these 6 steps:

1. Open the 'Internal DNS Table' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Internal DNS Table** page item).

Figure 3-75: Internal DNS Table Page



	Domain Name	First IP Address	Second IP Address	Third IP Address	Fourth IP Address
1	DomainName.com	10.8.2.15	10.8.4.20	10.8.6.17	10.8.6.18
2					
3					
4					

2. In the 'Domain Name' field, enter the host name to be translated. You can enter a string of up to 31 characters long.
3. In the 'First IP Address' field, enter the first IP address (in dotted-decimal format notation) to which the host name is translated.
4. Optionally, in the 'Second IP Address', 'Third IP Address', and 'Second IP Address' fields, enter the next IP addresses to which the host name is translated.
5. Click the **Submit** button to save your changes.
6. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

3.4.7.4.7 Internal SRV Table

The 'Internal SRV Table' page provides a table for resolving host names to DNS A-Records. Three different A-Records can be assigned to each host name. Each A-Record contains the host name, priority, weight, and port.

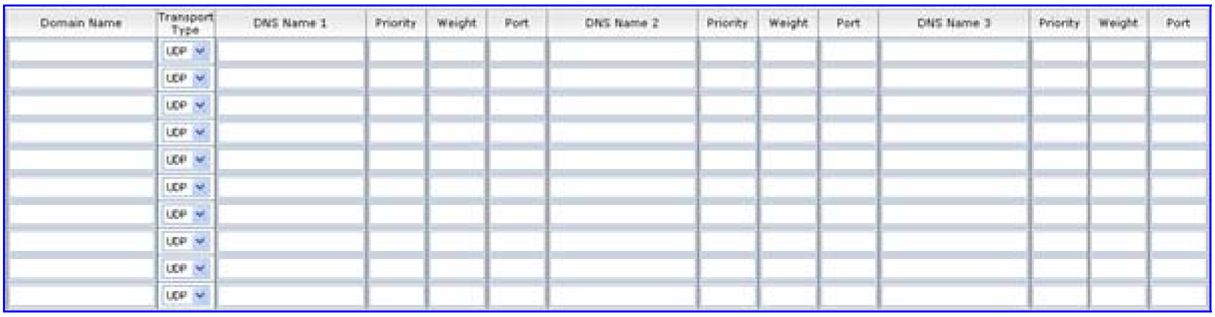
Notes:

- If the Internal SRV table is configured, the device initially attempts to resolve a domain name using this table. If the domain name isn't found, the device performs an Service Record (SRV) resolution using an external DNS server.
- You can also configure the Internal SRV table using the *ini* file table parameter SRV2IP (refer to "Networking Parameters" on page 260).

➢ To configure the Internal SRV table, take these 9 steps:

1. Open the 'Internal SRV Table' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Internal SRV Table** page item).

Figure 3-76: Internal SRV Table Screen



Domain Name	Transport Type	DNS Name 1	Priority	Weight	Port	DNS Name 2	Priority	Weight	Port	DNS Name 3	Priority	Weight	Port
	UDP												
	UDP												
	UDP												
	UDP												
	UDP												
	UDP												
	UDP												
	UDP												
	UDP												
	UDP												

2. In the 'Domain Name' field, enter the host name to be translated. You can enter a string of up to 31 characters long.
3. From the 'Transport Type' drop-down list, select a transport type.
4. In the 'DNS Name 1' field, enter the first DNS A-Record to which the host name is translated.
5. In the 'Priority', 'Weight' and 'Port' fields, enter the relevant values
6. Repeat steps 4 through 5, for the second and third DNS names, if required.
7. Repeat steps 2 through 6, for each entry.
8. Click the **Submit** button to save your changes.
9. To save the changes so they are available after a hardware reset or power fail, refer to "Saving Configuration" on page 230.

3.4.7.4.8 Reasons for Alternative Routing

The 'Reasons for Alternative Routing' page includes two groups - IP to Tel Reasons and Tel to IP Reasons. Each group allows you to define up to four different release reasons. If a call is released as a result of one of these reasons, the device tries to find an alternative route for that call. The release reason for IP-to-Tel calls is provided in Q.931 notation. The release reason for Tel-to-IP calls is provided in SIP 4xx, 5xx, and 6xx response codes. For Tel-to-IP calls, an alternative IP address is provided; for IP-to-Tel calls an alternative Trunk Group is provided. Refer to "Tel to IP Routing Table" on page 175 for information on defining an alternative IP address; refer to "IP to Trunk Group Routing" on page 181 for information on defining an alternative Trunk Group.

You can use the 'Reasons for Alternative Routing' page for the following example scenarios:

- **Tel-to-IP calls:** when there is no response to an INVITE message (after INVITE retransmissions), the device issues an internal 408 'No Response' implicit release reason.
- **IP-to-Tel calls:** when the destination is busy and release reason #17 is issued or for other call releases that issue the default release reason (#3). Refer to DefaultReleaseCause in "Advanced Parameters" on page 151.

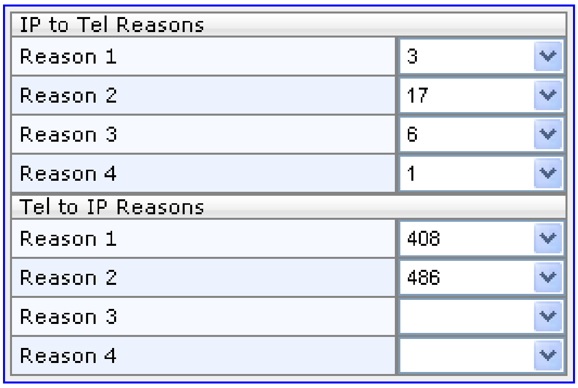
Notes:

- The reasons for alternative routing for Tel-to-IP calls only apply when a Proxy isn't used.
- For Tel-to-IP calls, the device sends the call to an alternative route only after the call has failed and the device has subsequently attempted twice to establish the call unsuccessfully.
- You can also configure alternative routing using the *ini* file table parameters AltRouteCauseTel2IP and AltRouteCauseIP2Tel (refer to "Number Manipulation and Routing Parameters" on page 313).

➢ To configure the reasons for alternative routing, take these 5 steps:

1. Open the 'Reasons for Alternative Routing' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Reasons for Alternative Routing** page item).

Figure 3-77: Reasons for Alternative Routing Page



IP to Tel Reasons	
Reason 1	3
Reason 2	17
Reason 3	6
Reason 4	1
Tel to IP Reasons	
Reason 1	408
Reason 2	486
Reason 3	
Reason 4	

2. In the 'IP to Tel Reasons' group, select up to four different call failure reasons that invoke an alternative IP-to-Tel routing.

3. In the 'Tel to IP Reasons' group, select up to four different call failure reasons that invoke an alternative Tel-to-IP routing.

4. Click the **Submit** button to save your changes.

5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

3.4.7.4.9 Release Cause Mapping

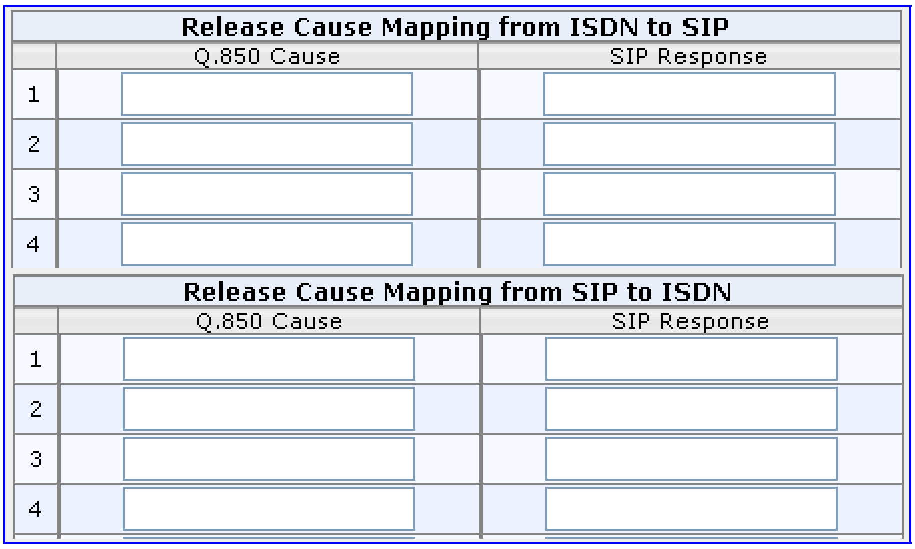
The 'Release Cause Mapping' page consists of two groups that allow the device to map up to 12 different SIP Responses to Q.850 Release Causes and vice versa, thereby overriding the hard-coded mapping mechanism (described in "Release Reason Mapping" on page 394).

Note: You can also configure SIP Responses-Q.850 Release Causes mapping using the *ini* file table parameters CauseMapISDN2SIP and CauseMapSIP2ISDN (refer to "ISDN and CAS Interworking-Related Parameters" on page 307).

➢ To configure Release Cause Mapping, take these 5 steps:

1. Open the 'Release Cause Mapping' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Release Cause Mapping** page item).

Figure 3-78: Release Cause Mapping Page



Release Cause Mapping from ISDN to SIP

	Q.850 Cause	SIP Response
1		
2		
3		
4		

Release Cause Mapping from SIP to ISDN

	Q.850 Cause	SIP Response
1		
2		
3		
4		

2. In the 'Release Cause Mapping from ISDN to SIP' group, map (up to 12) different Q.850 Release Causes to SIP Responses.

3. In the 'Release Cause Mapping from SIP to ISDN' group, map (up to 12) different SIP Responses to Q.850 Release Causes.

4. Click the **Submit** button to save your changes.

5. To save the changes so they are available after a power fail, refer to "Saving Configuration" on page 230.

3.4.7.5 Configuring the Profile Definitions

The **Profile Definitions** submenu includes the following page items:

- Coder Group Settings (refer to "Coder Group Settings" on page 190)
- Tel Profile Settings (refer to "Tel Profile Settings" on page 192)
- IP Profile Settings (refer to "IP Profile Settings" on page 193)

Implementing the device's Profile features, provides the device with high-level adaptation when connected to a variety of equipment (at both Tel and IP sides) and protocols, each of which requires different system behavior.

You can assign different Profiles (behavior) per call, using the call routing tables:

- 'Tel to IP Routing' page (refer to "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing Table' page if EnableSBC is set to 1 (refer to “Outbound IP Routing Table” on page 178)
- 'IP to Trunk Group Routing' page (refer to "IP to Trunk Group Routing" on page 181) or 'Inbound IP Routing Table' page (refer to “Inbound IP Routing Table” on page 184) if EnableSBC is set to 1,

In addition, you can associate different Profiles per the device's channels.

Each Profile contains a set of parameters such as coders, T.38 Relay, Voice and DTMF Gain, Silence Suppression, Echo Canceler, RTP DiffServ, Current Disconnect and more. The Profiles feature allows you to customize these parameters or turn them on or off, per source or destination routing and/or per the device's trunks (channels). For example, specific E1/T1 spans can be assigned a Profile that always uses G.711.

Each call can be associated with one or two Profiles - Tel Profile and/or IP Profile. If both IP and Tel profiles apply to the same call, the coders and other common parameters of the preferred Profile (determined by the Preference option) are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters take precedence.

Notes:

- The default values of the parameters in the 'Tel Profile Settings' and 'IP Profile Settings' pages are identical to their default values in their respective primary configuration page.
- If you modify a parameter in its primary configuration page (or*ini* file) that also appears in the profile pages, the parameter's new value is automatically updated in the profile pages. However, once you modify any parameter in the profile pages, modifications to parameters in the primary configuration pages (or*ini* file) no longer impact that profile pages.

3.4.7.5.1 Coder Group Settings

The 'Coder Group Settings' page provides a table for defining up to four different coder groups. These coder groups are used in the 'Tel Profile Settings' and 'IP Profile Settings' pages to assign different coders to Profiles.

For each coder group you can define up to five coders, where the first coder (and its attributes) in the table takes precedence over the second coder, and so on. The first coder is the highest priority coder and is used by the device whenever possible. If the far end device cannot use the coder assigned as the first coder, the device attempts to use the next coder and so on. For a list of coders supported by the device, refer to "Coders" on page 144.

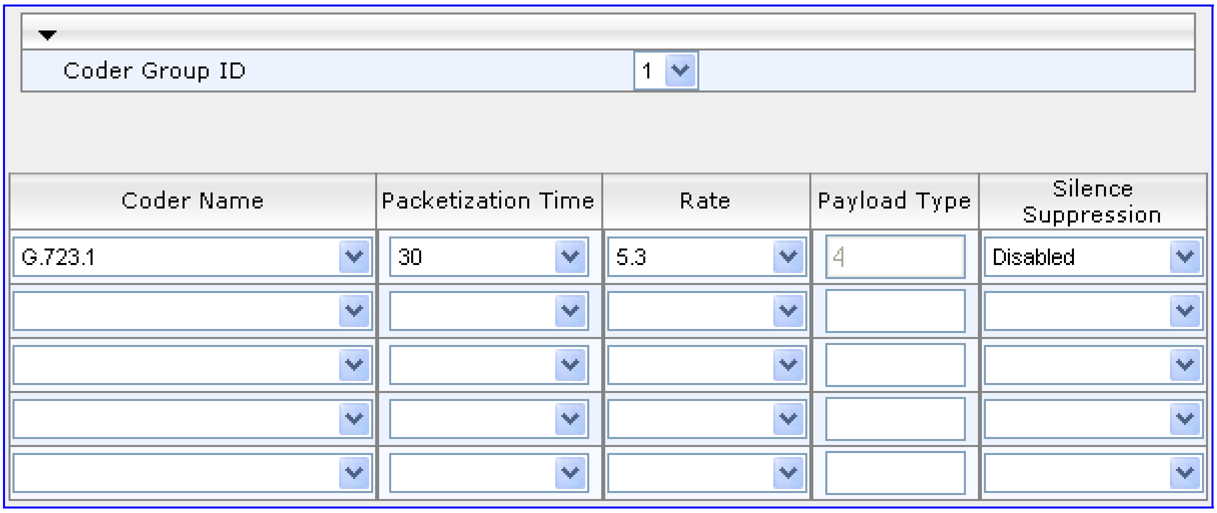
Notes:

- Each coder type can appear only once per Coder Group.
- The device always uses the packetization time requested by the remote side for sending RTP packets. If not specified, the packetization time (ptime) is assigned the default value.
- Only the packetization time of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined.
- For G.729, you can also select silence suppression without adaptations.
- If silence suppression is enabled for G.729, the device includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception is when the remote device is a Cisco gateway (IsCiscoSCEMode).
- You can also configure the coder groups using the *ini* file table parameter CoderName (refer to "SIP Configuration Parameters" on page 284).

➢ To configure coder groups, take these 11 steps:

1. Open the 'Coder Group Settings' page (**Configuration** tab > **Protocol Configuration** menu > **Profile Definitions** submenu > **Coder Group Settings** page item).

Figure 3-79: Coder Group Settings Page



Coder Group ID: 1

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.723.1	30	5.3	4	Disabled

2. From the 'Coder Group ID' drop-down list, select a coder group ID.
3. From the 'Coder Name' drop-down list, select the first coder for the coder group.
4. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the coder. The packetization time determines how many coder payloads are combined into a single RTP packet.
5. From the 'Rate' drop-down list, select the bit rate (in kbps) for the coder you selected.
6. In the 'Payload Type' field, if the payload type for the coder you selected is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified). The payload type identifies the format of the RTP payload.

7. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the coder you selected.
8. Repeat steps 3 through 7 for the second to fifth coders (optional).
9. Repeat steps 2 through 8 for the second to fourth coder groups (optional).
10. Click the **Submit** button to save your changes.
11. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

3.4.7.5.2 Tel Profile Settings

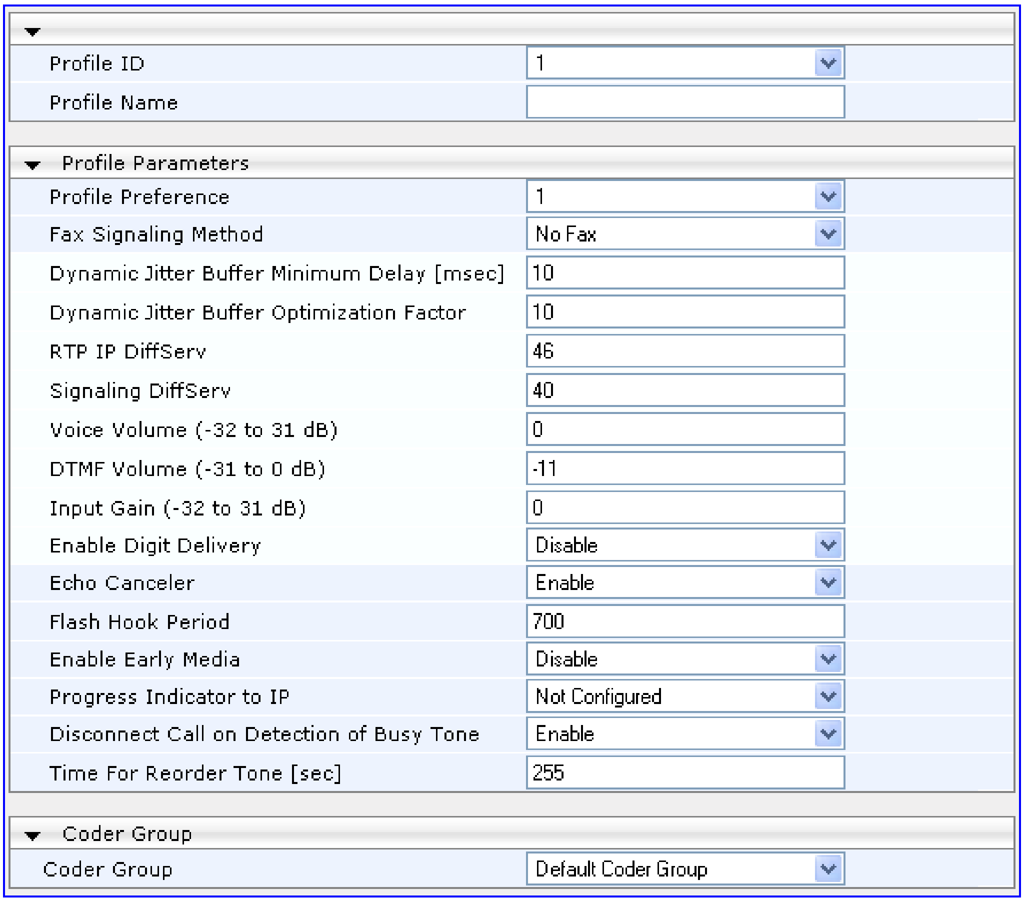
The 'Tel Profile Settings' page allows you to define up to nine different Tel Profiles. You can then assign these Tel Profiles to the device's channels (in the 'Trunk Group Table' page), thereby applying different behaviors to different channels.

> **Note:** You can also configure Tel Profiles using the *ini* file table parameter TelProfile (refer to "SIP Configuration Parameters" on page 284).

➢ To configure Tel Profiles, take these 9 steps:

1. Open the 'Tel Profile Settings' page (**Configuration** tab > **Protocol Configuration** menu > **Profile Definitions** submenu > **Tel Profile Settings** page item).

Figure 3-80: Tel Profile Settings Page



Profile ID	1
Profile Name	
Profile Parameters	
Profile Preference	1
Fax Signaling Method	No Fax
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Voice Volume (-32 to 31 dB)	0
DTMF Volume (-31 to 0 dB)	-11
Input Gain (-32 to 31 dB)	0
Enable Digit Delivery	Disable
Echo Canceler	Enable
Flash Hook Period	700
Enable Early Media	Disable
Progress Indicator to IP	Not Configured
Disconnect Call on Detection of Busy Tone	Enable
Time For Reorder Tone [sec]	255
Coder Group	
Coder Group	Default Coder Group

2. From the 'Profile ID' drop-down list, select the Tel Profile identification number you want to configure.

3. In the 'Profile Name' field, enter an arbitrary name that enables you to easily identify the Tel Profile.

4. From the 'Profile Preference' drop-down list, select the priority of the Tel Profile, where '1' is the lowest priority and '20' is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk in the description of the parameter TelProfile) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
   Note: If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.

5. Configure the Profile's parameters according to your requirements. For detailed information on each parameter, refer to its description on the page in which it is configured as an individual parameter.

6. From the 'Coder Group' drop-down list, select the Coder Group (refer to "Coder Group Settings" on page 190) or the device's default coder (refer to "Coders" on page 144) to which you want to assign the Profile.

7. Repeat steps 2 through 6 to configure additional Tel Profiles (optional).

8. Click the **Submit** button to save your changes.

9. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

3.4.7.5.3 IP Profile Settings

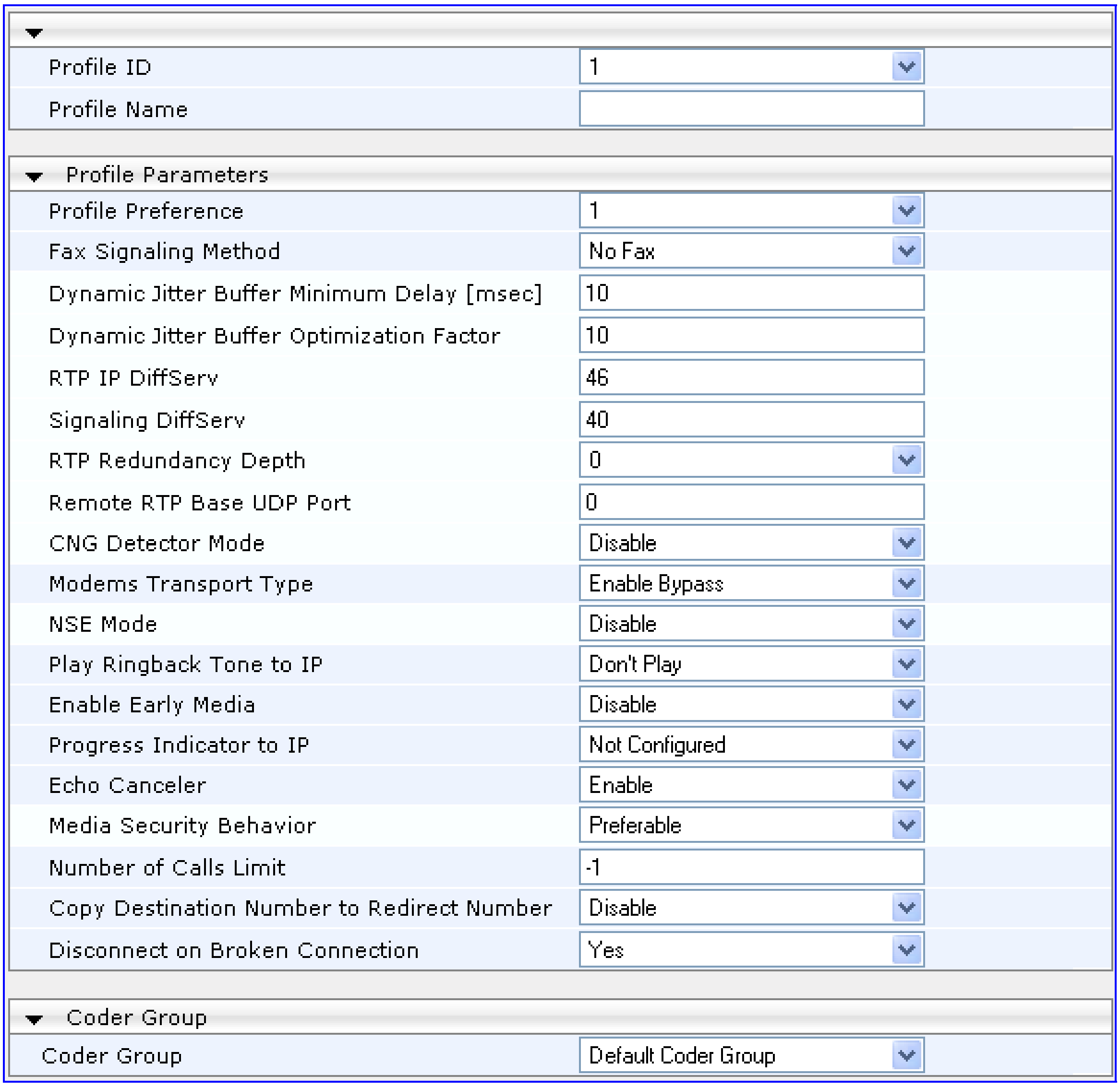
The 'IP Profile Settings' page allows you to define up to nine different IP Profiles. You can then assign these IP Profiles to routing rules in the 'Tel to IP Routing' page (refer to "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing Table' if EnableSBC is set to 1 (refer to “Outbound IP Routing Table” on page 178) and 'IP to Trunk Group Routing' page (refer to "IP to Trunk Group Routing" on page 181) or 'Inbound IP Routing Table' if EnableSBC is set to 1 (refer to “Inbound IP Routing Table” on page 184). IP Profiles can also be used when working with a Proxy server (set AlwaysUseRouteTable to 1).

Note: You can also configure the IP Profiles using the *ini* file table parameter IPProfile (refer to "SIP Configuration Parameters" on page 284).

➢ To configure the IP Profile settings, take these 9 steps:

1. Open the 'IP Profile Settings' page (**Configuration** tab > **Protocol Configuration** menu > **Profile Definitions** submenu > **IP Profile Settings** page item).

Figure 3-81: IP Profile Settings Page



Profile ID	1
Profile Name	

Profile Parameters

Profile Preference	1
Fax Signaling Method	No Fax
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
RTP Redundancy Depth	0
Remote RTP Base UDP Port	0
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Play Ringback Tone to IP	Don't Play
Enable Early Media	Disable
Progress Indicator to IP	Not Configured
Echo Canceler	Enable
Media Security Behavior	Preferable
Number of Calls Limit	-1
Copy Destination Number to Redirect Number	Disable
Disconnect on Broken Connection	Yes

Coder Group

Coder Group	Default Coder Group

2. From the 'Profile ID' drop-down list, select an identification number for the IP Profile.

3. In the 'Profile Name' field, enter an arbitrary name that allows you to easily identify the IP Profile.

4. From the 'Profile Preference' drop-down list, select the priority of the IP Profile, where '1' is the lowest priority and '20' is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk in the description of the parameter IPProfile) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Note: If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.

5. Configure the IP Profile's parameters according to your requirements. For detailed information on each parameter, refer to the description on the page in which it is configured as an individual parameter. Parameters that are unique to IP Profile are described in the table below.

6. From the 'Coder Group' drop-down list, select the coder group you want to assign to the Profile. You can select the device's default coders (refer to "Coders" on page 144) or one of the coder groups you defined in the 'Coder Group Settings' page (refer to "Coder Group Settings" on page 190).

7. Repeat steps 2 through 6 for the next IP Profiles (optional).

8. Click the **Submit** button to save your changes.

9. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-48: Description of Parameter Unique to IP Profile

Parameter	Description
Number of Calls Limit	Maximum number of concurrent calls. If the profile is set to some limit, the device maintains the number of concurrent calls (incoming and outgoing) pertaining to the specific profile. A limit value of '-1' indicates that there is no limitation on calls for that specific profile (default). A limit value of '0' indicates that all calls are rejected. When the number of concurrent calls is equal to the limit, the device rejects any new incoming and outgoing calls belonging to that profile.

3.4.7.6 Configuring the Trunk and IP Groups

The Trunk**/IP Group** menu allows you to configure groups of channels. This submenu includes the following page items:

- Trunk Group (refer to “Configuring the Trunk Group Table” on page 195)
- Trunk Group Settings (refer to "Configuring the Trunk Group Settings" on page 197)
- IP Group Table (refer to "Configuring the IP Groups" on page 201)
- Account Table (refer to "Configuring the Account Table" on page 204)

3.4.7.6.1 Configuring the Trunk Group Table

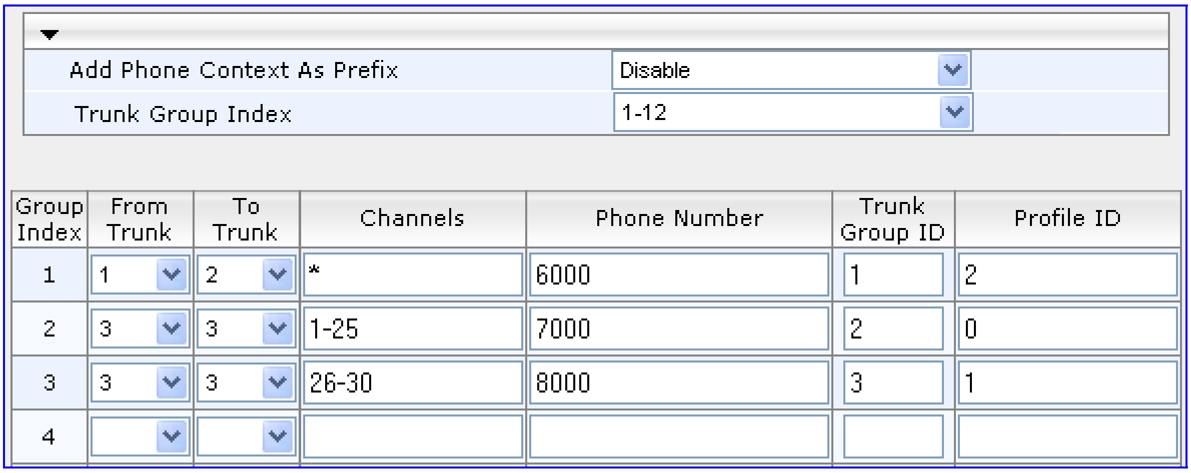
The 'Trunk Group Table' page provides you with a table for enabling device channels, by assigning them telephone numbers, Trunk Groups, and Profiles. Trunk Groups are used for routing IP-to-Tel calls with common rules. Channels that are not defined are disabled. You can add up to 24entries in this table.

Note: You can also configure the Trunk Groups using the *ini* file table parameter TrunkGroup_x to (refer to "Number Manipulation and Routing Parameters" on page 313).

➢ To configure the Trunk Group table, take these 4 steps:

1. Open the 'Trunk Group Table' page (**Configuration** tab > **Protocol Configuration** menu > **Trunk/IP Group** submenu > **Trunk Group** page item).

Figure 3-82: Trunk Group Table Page



Add Phone Context As Prefix	Disable
Trunk Group Index	1-12

Group Index	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Profile ID
1	1	2	*	6000	1	2
2	3	3	1-25	7000	2	0
3	3	3	26-30	8000	3	1
4						

2. Configure the Trunk Group according to the table below**.**

3. Click the **Submit** button to save your changes.

4. To save the changes to the flash memory, refer to "Saving Configuration" on page 230.

Table 3-49: Trunk Group Table Description

Parameter	Description
From Trunk **[TrunkGroup_FirstTrunkId]**	Starting physical Trunk number. The number of listed Trunks depends on the device's hardware configuration.
To Trunk **[TrunkGroup_LastTrunkId]**	Ending physical Trunk number. The number of listed Trunks depends on the device's hardware configuration.
Channels **[TrunkGroup_FirstBChannel], [TrunkGroup_LastBChannel]**	The device's Trunk B-channels. To enable the channels, enter the channel numbers. You can enter a range of channels by using the format [n-m], where *n* represents the lower channel number and *m* the higher channel number, e.g., [1-24] specifies channels 1 through 24. **Notes:** ▪ The number of defined channels must not exceed the number of the Trunk's B-channels. ▪ To represent all channels, enter a single asterisk (*).

Parameter	Description
Phone Number **[TrunkGroup_FirstPhoneNumber]**	Enter the first telephone number that you want to assign to the first channel defined in the 'Channels' field. Subsequent channels are assigned the next consecutive phone number. **Notes:** ▪ If the 'Phone Number' field includes alphabetical characters and the phone number is defined for a range of channels (e.g., 1-4), then the phone number must end with a number (e.g., 'user1'). ▪ This field is optional. The logical numbers defined in this field are used when an incoming PSTN / PBX call doesn't contain the calling number or called number (the latter being determined by the parameter ReplaceEmptyDstWithPortNumber); these numbers are used to replace them. These logical numbers are also used for channel allocation for IP-to-Tel calls if the Trunk Group's 'Channel Select Mode' is set to 'By Dest Phone Number'.
Trunk Group ID **[TrunkGroup_TrunkGroupNum]**	The Trunk Group ID (1-99) assigned to the corresponding channels. The same Trunk Group ID can be used for more than one group of channels. Trunk Group ID is used to define a group of common channel behavior that are used for routing IP-to-Tel calls. If an IP-to-Tel call is assigned to a Trunk Group, the call is routed to the channel or channels that correspond to the Trunk Group ID. You can configure the 'Trunk Group Settings' table (refer to "Configuring the Trunk Group Settings" on page 197) to determine the method in which new calls are assigned to channels within the Trunk Groups. **Note:** You must configure the 'IP to Trunk Group Routing Table' page (refer to "IP to Trunk Group Routing" on page 181) to assign incoming IP calls to the appropriate Trunk Group. If you do not configure the 'IP to Trunk Group Routing Table', calls do not complete.
Profile ID **[TrunkGroup_ProfileId]**	The Tel profile ID (refer to "Tel Profile Settings" on page 192) assigned to the channels defined in the 'Channels' field.

3.4.7.6.2 Configuring the Trunk Group Settings

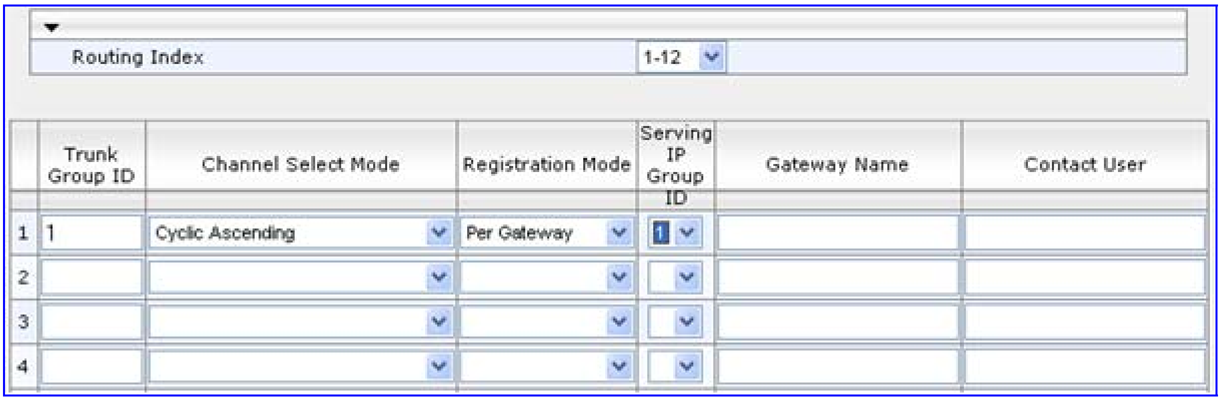
The 'Trunk Group Settings' page is mainly used to select the method for which IP-to-Tel calls are assigned to channels within each Trunk Group. If no method is selected (for a specific Trunk Group), the setting of the global parameter ChannelSelectMode in the 'SIP General Parameters' page (refer to "SIP General Parameters" on page 121) applies. In addition, this page also defines the method for registering Trunk Groups to selected Serving IP Group IDs (if defined). You can add up to 24 entries in this table.

Note: You can also configure the Trunk Group Settings table using the *ini* file table parameter TrunkGroupSettings (refer to "Number Manipulation and Routing Parameters" on page 313).

➢ To configure the Trunk Group Settings table, take these 5 steps:

1. Open the 'Trunk Group Settings' page (**Configuration** tab > **Protocol Configuration** menu > Trunk/**IP Group** submenu > **Trunk Group Settings** page item).

Figure 3-83: Trunk Group Settings Page



Routing Index 1-12

	Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	Cyclic Ascending	Per Gateway	1		
2						
3						
4						

2. From the 'Routing Index' drop-down list, select the range of entries that you want to edit (up to 24 entries can be configured).

3. Configure the Trunk Group according to the table below.

4. Click the **Submit** button to save your changes.

5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-50: Trunk Group Settings Parameters Description

Parameter	Description
Trunk Group ID **[TrunkGroupSettings_TrunkGroupId]**	The Trunk Group ID that you want to configure. The valid range is 1-99. Trunks are assigned to Trunk Groups in the 'Trunk Group Table' page (refer to “Configuring the Trunk Group Table” on page 195).
Channel Select Mode **[TrunkGroupSettings_ChannelSelectMode]**	The method in which IP-to-Tel calls are assigned to channels pertaining to a Trunk Group: ▪ **[0]** By Dest Phone Number = Selects the device's channel according to the called number defined in the 'Trunk Group Table' (refer to “Configuring the Trunk Group Table” on page 195). ▪ **[1]** Cyclic Ascending (default) = Selects the next available channel in an ascending cyclic order. The next highest channel number in the Trunk Group is always selected. When the highest channel number in the Trunk Group is reached, the lowest channel number in the Trunk Group is selected, and then it starts ascending again. ▪ **[2]** Ascending = Selects the lowest available channel. The lowest channel number in the Trunk Group is always first selected, and if that channel is unavailable, the next highest channel is selected. ▪ **[3]** Cyclic Descending = Selects the next available channel in descending cyclic order. The next lowest channel number in the Trunk Group is always first selected. When the lowest channel number in the Trunk Group is reached, it selects the highest channel number in the Trunk Group and then start descending again.

Parameter	Description
	- **[4]** Descending = Selects the highest available channel. The highest channel number in the Trunk Group is always first selected, and if that channel is unavailable, the next lowest channel is selected. - **[5]** Dest Number + Cyclic Ascending = The channel is first selected according to the called number. If the called number isn't found, the next available channel in ascending cyclic order is selected. Note that if the called number is found, but the channel associated with the number is busy, the call is released. - **[6]** By Source Phone Number = Selects the channel according to the calling number. - **[7]** Trunk Cyclic Ascending = The first channel of the next Trunk (i.e., next to the Trunk from which the previous channel was allocated) is selected.
Registration Mode **[TrunkGroupSettings_RegistrationMode]**	Registration mode per Trunk Group: - **[1]** Per Gateway = Single registration for the entire device (default). This mode is applicable only if a default Proxy or Registrar IP are configured, and Registration is enabled (i.e., parameter IsRegisterUsed is set to 1). In this mode, the URI userpart in the From, To, and Contact headers is set to the value of the global registration parameter GWRegistrationName (refer to "Proxy & Registration Parameters" on page 132) or username if GWRegistrationName is not configured. - **[0]** Per Endpoint = Each channel in the Trunk Group registers individually. The registrations are sent to the ServingIPGroupID if defined in the table, otherwise to the default Proxy, and if no default Proxy, then to the Registrar IP. - **[4]** Don't Register = No registrations are sent by endpoints pertaining to the Trunk Group. For example, if the device is configured globally to register all its endpoints (using the parameter ChannelSelectMode), you can exclude some endpoints from being registered by assigning them to a Trunk Group and configuring the Trunk Group registration mode to 'Don't Register'. - **[5]** Per Account = Registrations are sent (or not) to an IP Group, according to the settings in the Account table (refer to "Configuring the Account Table" on page 204). **Notes:** - To enable Trunk Group registrations, configure the global parameter IsRegisterNeeded to 1. This is unnecessary for 'Per Account' registration mode. - If no mode is selected, the registration is performed according to the global registration parameter ChannelSelectMode (refer to "Proxy & Registration Parameters" on page 132). - If the device is configured globally (ChannelSelectMode) to register Per Endpoint, and a Trunk Group comprising four channels is configured to register Per Gateway, the device registers all channels except the first four channels. The Trunk Group of these four channels sends a single registration request.

Parameter	Description
Serving IP Group ID **[TrunkGroupSettings_ServingIPGroup]**	The Serving IP Group ID to where INVITE messages initiated by this Trunk Group's endpoints are sent. The actual destination to where these INVITE messages are sent is to the Proxy Set ID (refer to "Proxy Sets Table" on page 141) associated with this Serving IP Group. The Request URI hostname in the INVITE and REGISTER messages (except for 'Per Account' registration modes) is set to the value of the field 'SIP Group Name' defined in the 'IP Group' table (refer to "Configuring the IP Groups" on page 201). If no Serving IP Group ID is selected, the INVITE messages are sent to the default Proxy or according to the 'Tel to IP Routing Table' (refer to "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing Table' if EnableSBC is set to 1 (refer to “Outbound IP Routing Table” on page 178). **Note:** If the parameter PreferRouteTable is set to 1 (refer to "Proxy & Registration Parameters" on page 132), the routing rules in the 'Tel to IP Routing Table' (or 'Outbound IP Routing Table') prevail over the selected Serving IP Group ID.
Gateway Name **[TrunkGroupSettings_GatewayName]**	The host name used in the From header in INVITE messages, and as a host name in From/To headers in REGISTER requests. If not configured, the global parameter SIPGatewayName is used instead.
Contact User **[TrunkGroupSettings_ContactUser]**	This is used as the user part in the Contact URI in INVITE messages, and as a user part in From, To, and Contact headers in REGISTER requests. This is applicable only if the field 'Registration Mode' is set to 'Per Account', and the Registration through the Account table is successful. **Notes:** ▪ If registration fails, then the userpart in the INVITE Contact header contains the source party number. ▪ The 'ContactUser' parameter in the 'Account Table' page overrides this parameter.

An example is shown below of a REGISTER message for registering endpoint "101" using registration Per Endpoint mode. The "SipGroupName" in the request URI is taken from the IP Group table.

```
REGISTER sip:SipGroupName SIP/2.0
Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac862428454
From: <sip:101@GatewayName>;tag=1c862422082
To: <sip:101@GatewayName>
Call-ID: 9907977062512000232825@10.33.37.78
CSeq: 3 REGISTER
Contact: <sip:101@10.33.37.78>;expires=3600
Expires: 3600
User-Agent: Audiocodes-Sip-Gateway/v.5.40A.008.002
Content-Length: 0
```

3.4.7.6.3 Configuring the IP Groups

The 'IP Group Table' page allows you to create up to nine logical IP entities (IP Groups) that are later used in the call routing tables. The IP Groups are typically implemented in Tel-to-IP call routing. The IP Group can be used as a destination entity in the 'Tel to IP Routing' table (or 'Outbound IP Routing Table'), and Serving IP Group ID in the 'Trunk Group Settings' (refer to "Configuring the Trunk Group Settings" on page 197) and 'Account' (refer to "Configuring the Account Table" on page 204) tables. These call routing tables are used for identifying the IP Group from where the INVITE is sent for obtaining a digest user/password from the 'Account' table if there is a need to authenticate subsequent SIP requests in the call. The IP Group can also be implemented in IP-to-Tel call routing (or inbound IP routing) as a source IP Group.

The IP Groups are assigned various entities such as a Proxy Set ID, which represents an IP address (created in "Proxy Sets Table" on page 141). You can also assign the IP Group with a host name and other parameters that reflect parameters sent in SIP Request From\To.

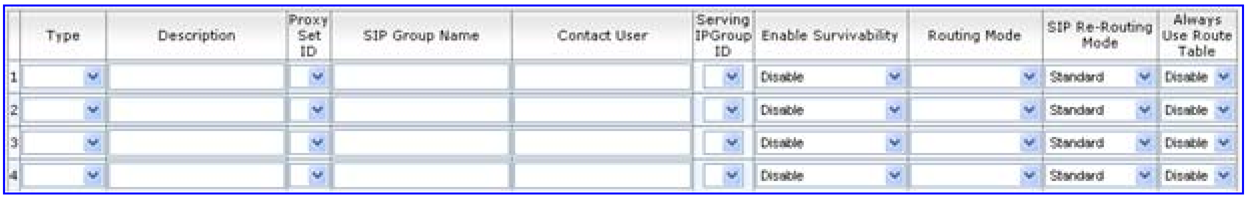
Notes:

- By default, if you disable the use of a proxy (i.e., IsProxyUsed is set to 0), then only one IP Group is defined (and working with multiple IP Groups is not valid).
- You can also configure the IP Groups table using the *ini* file table parameter IPGroup (refer to "SIP Configuration Parameters" on page 284).

➢ To configure IP Groups, take these 4 steps:

1. Open the 'IP Group Table' page (**Configuration** tab > **Protocol Configuration** menu > Trunk**/IP Group** submenu > **IP Group Table** page item).

Figure 3-84: IP Group Table Page



	Type	Description	Proxy Set ID	SIP Group Name	Contact User	Serving IPGroup ID	Enable Survivability	Routing Mode	SIP Re-Routing Mode	Always Use Route Table
1							Disable		Standard	Disable
2							Disable		Standard	Disable
3							Disable		Standard	Disable
4							Disable		Standard	Disable

2. Configure the IP group parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" **on page 230.**

Table 3-51: IP Group Parameters Description

Parameter	Description
Type	The IP Group can be defined as one of the following types: ▪ SERVER = used when the destination address (configured by the Proxy Set) of the IP Group (e.g., ITSP, Proxy, IP-PBX, or Application server) is known. ▪ USER = represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users. Typically, this IP Group is configured with a Serving IP Group that represents an IP-PBX, Application or Proxy server that serves this USER-type IP Group. Each SIP request sent by a user of this IP Group is proxied to the Serving IP Group. For registrations, the device updates its internal database with the AOR and contacts of the users. Digest authentication using SIP 401/407 responses (if needed) is performed by the Serving IP Group. The device forwards these responses directly to the SIP users. To route a call to a registered user, a rule must be configured in the 'Outbound IP Routing' table (refer to "Outbound IP Routing Table" on page 178). The device searches the dynamic database (by using the request URI) for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained from this entry, and a SIP request is sent to the destination. The device also supports NAT traversal for the SIP clients that are behind NAT. In this case, the device must be defined with a global IP address. **Note:** This field is available only if EnableSBC is set to 1 (refer to "SBC Configuration" on page 163).
Description	Brief string description of the IP Group. The value range is a string of up to 29 characters. The default is an empty field.
Proxy Set ID	Selects the Proxy Set ID (defined in "Proxy Sets Table" on page 141) to associate with the IP Group. All INVITE messages configured to be 'sent' to the specific IP Group are in fact sent to the IP address associated with this Proxy Set. The range is 0-5, where 0 is the default Proxy Set. **Note:** The Proxy Set is only defined for SERVER type IP Groups.
SIP Group Name	The request URI host name used in INVITE and REGISTER messages that are sent to this IP Group, or the host name in the From header of INVITE messages received from this IP Group. If not specified, the value of the global parameter ProxyName (refer to "Proxy & Registration Parameters" on page 132) is used instead. The value range is a string of up to 49 characters. The default is an empty field. **Note:** If the IP Group is of type USER, this parameter is used internally as a hostname in the request URI for TDM-to-IP initiated calls. For example, if an incoming call from the device's T1 trunk is routed to a USER-type IP Group, the device first forms the request URI (destination_number@SIPGroupName), and then it searches the User's internal database for a match.
Contact User	Defines the user part for the From, To, and Contact headers of SIP REGISTER messages, and the user part for the Contact header of

Parameter	Description
	INVITE messages that are received from this IP Group and forwarded by the device to another IP Group. **Notes:** ▪ This parameter is applicable only for USER-type IP Groups. ▪ This parameter is overridden by the ‘Contact User’ parameter (if configured) in the ‘Account’ table (refer to "Configuring the Account Table" on page 204).
Serving IP Group ID	If configured, INVITE messages initiated from the IP Group are sent to this Serving IP Group (range 1 to 9). In other words, the INVITEs are sent to the address defined for the Proxy Set associated with this Serving IP Group. The Request URI host name in these INVITE messages are set to the value of the parameter ‘SIP Group Name’ defined for the Serving IP Group. **Notes:** ▪ This field is available only if EnableSBC is set to 1 (refer to “SBC Configuration” on page 163). ▪ If the parameter PreferRouteTable is set to 1, the routing rules in the ‘Outbound IP Routing’ table takes precedence over this ‘Serving IP Group ID’ parameter. ▪ If this parameter is not configured, the INVITE messages are sent to the default Proxy or according to the ‘Outbound IP Routing’ table.
Enable Survivability	Determines whether Survivability mode is enabled for USER-type IP Groups. ▪ Disable (default). ▪ Enable = Survivability mode is enabled. The device records in its local database the registration messages sent by the clients belonging to the USER-type IP Group. If communication with the Serving IP Group (e.g., IP-PBX) fails, the USER-type IP Group enters into Survivability mode in which the device uses its database for routing calls between the clients (e.g., IP phones) of the USER-type IP Group. The RTP packets between the IP phones in Survivability mode always traverse through the device. In Survivability mode, the device is capable of receiving new registrations. When the Serving IP Group is available again, the device returns to normal mode, sending INVITE and REGISTER messages to the Serving IP Group. **Notes:** ▪ This field is available only if EnableSBC is set to 1 (refer to “SBC Configuration” on page 163). ▪ This parameter is applicable only to USER-type IP Groups.
Routing Mode	Defines the routing mode for outgoing SIP INVITE messages. ▪ **[0]** Not Configured = The routing is done according to the selected Serving IP Group. If no Serving IP Group is selected, the device routes the call according to the 'Outbound IP Routing' table (refer to “Outbound IP Routing Table” on page 178). ▪ **[1]** Routing Table = The device routes the call according to the 'Outbound IP Routing' table. ▪ **[2]** Serving IP Group = The device sends the SIP INVITE to the selected Serving IP Group. If no Serving IP Group is selected, the default IP Group is used. If the Proxy server(s) associated with the

Parameter	Description
	destination IP Group is not alive, the device uses the 'Outbound IP Routing' table (if the parameter IsFallbackUsed is set 1, i.e., fallback enabled - refer to Proxy & Registration Parameters on page 132). ▪ **[3]** Request-URI = The device sends the SIP INVITE to the IP address according to the received SIP Request-URI host name. **Note:** This field is available only if EnableSBC is set to 1 (refer to "SBC Configuration" on page 163).
SIP Re Routing Mode	Determines the routing mode after a call redirection (i.e., a 3xx SIP response is received) or transfer (i.e., a SIP REFER request is received). ▪ **[0]** Standard = INVITE messages that are generated as a result of Transfer or Redirect are sent directly to the URI, according to the Refer-To header in the REFER message or Contact header in the 3xx response (default). ▪ **[1]** Proxy = Sends a new INVITE to the Proxy. **Note:** Applicable only if a Proxy server is used and the parameter AlwaysSendtoProxy is set to 0. ▪ **[2]** Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination. **Notes:** ▪ When this parameter is set to [1] and the INVITE sent to the Proxy fails, the device re-routes the call according to the Standard mode [0]. ▪ When this parameter is set to [2] and the INVITE fails, the device re-routes the call according to the Standard mode [0]. If DNS resolution fails, the device attempts to route the call to the Proxy. If routing to the Proxy also fails, the Redirect / Transfer request is rejected. ▪ When this parameter is set to [2], the XferPrefix parameter can be used to define different routing rules for redirected calls. ▪ This parameter is disregarded if the parameter AlwaysSendToProxy is set to 1.
Always Use Route Table	Determines the Request URI host name in outgoing INVITE messages. ▪ Disable (default). ▪ Enable = The device uses the IP address (or domain name) defined in the 'Tel to IP Routing' table ("Tel to IP Routing Table" on page 175) as the Request URI host name in outgoing INVITE messages, instead of the value entered in the 'SIP Group Name' field.

3.4.7.6.4 Configuring the Account Table

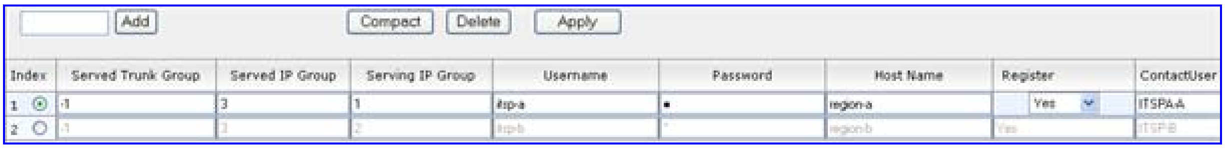
The 'Account Table' page allows you to define *accounts* per Trunk Groups (referred to as *Served Trunk Group*) or to a Served IP Group for registration and/or digest authentication (user name and password) to a destination IP address (Serving IP Group). The Account table can be used, for example, to register to an Internet Telephony Service Provider (ITSP) on behalf of an IP-PBX to which the device is connected. The registrations are sent to the Proxy Set ID (refer to "Proxy Sets Table" on page 141) associated with these Serving IP Groups. A Trunk Group can register to more than one Serving IP Group (e.g., ITSP's), by configuring multiple entries in this Account table with the same Served Trunk Group, but with different Serving IP Groups, user name/password, Host Name, and Contact User parameters.

Note: You can also configure the Account table using the *ini* file table parameter Account (refer to "SIP Configuration Parameters" on page 284).

➢ To configure Accounts, take these 5 steps:

1. Open the 'Account Table' page (**Configuration** tab > **Protocol Configuration** menu > Trunk**/IP Group** submenu > **Account Table** page item).

Figure 3-85: Account Table Page



Index	Served Trunk Group	Served IP Group	Serving IP Group	Username	Password	Host Name	Register	ContactUser
1 ●	-1	3	1	itsp-a	*	region-a	Yes	ITSPA-A
2 ○	-1	3	2	itsp-b	*	region-b	Yes	ITSP-B

2. To add an Account, in the 'Add' field, enter the desired table row index, and then click **Add**. A new row appears.
3. Configure the Account parameters according to the table below.
4. Click the **Apply** button to save your changes.
5. To save the changes, refer to "Saving Configuration" on page 230.

Note: For a description of the Web interface's table command buttons (e.g., **Duplicate** and **Delete**), refer to "Working with Tables" on page 30.

Table 3-52: Account Parameters Description

Parameter	Description
Served Trunk Group	The Trunk Group ID for which the device performs registration and/or authentication to a destination IP Group (i.e., Serving IP Group). For Tel-to-IP calls, the Served Trunk Group is the source Trunk Group from where the call initiated. For IP-to-Tel calls, the Served Trunk Group is the 'Trunk Group ID' defined in the 'IP to Trunk Group Routing' table (refer to "IP to Trunk Group Routing" on page 181). For defining Trunk Groups, refer to “Configuring the Trunk Group Table” on page 195 . **Note:** For IP-to-IP call routing, this parameter must be set to -1 (i.e., no trunk).
Served IP Group	The Source IP Group (e.g., IP-PBX) for which registration and/or authentication is performed.
Serving IP Group	The destination IP Group ID (defined in "Configuring the IP Groups" on page 201) to where the REGISTER requests (if enabled) are sent or Authentication is performed. The actual destination to where the REGISTER requests are sent is the IP address defined for the Proxy Set ID (refer to "Proxy Sets Table" on page 141) associated with this IP Group. This occurs only in the following conditions: ▪ The parameter 'Registration Mode' is set to 'Per Account' in the 'Trunk Group Settings' table (refer to "Configuring the Trunk Group Settings" on page 197).

Parameter	Description
	- The parameter 'Register' in this table is set to 1. In addition, for a SIP call that is identified by both the Served Trunk Group/ Served IP Group and Serving IP Group, the username and password for digest authentication defined in this table is used. For Tel-to-IP calls, the Serving IP Group is the destination IP Group defined in the 'Trunk Group Settings' table or 'Tel to IP Routing' table (refer to "Tel to IP Routing Table" on page 175). For IP-to-Tel calls, the Serving IP Group is the 'Source IP Group ID' defined in the 'IP to Trunk Group Routing' table (refer to "IP to Trunk Group Routing" on page 181). **Note:** If no match is found in this table for incoming or outgoing calls, the username and passwordthe global parameters (UserName and Password) defined on the 'Proxy & Registration' page (refer to "Proxy & Registration Parameters" on page 132) are used.
Username	Digest MD5 Authentication user name (up to 50 characters).
Password	Digest MD5 Authentication password (up to 50 characters).
HostName	Defines the Address of Record (AOR) host name. It appears in REGISTER From/To headers as ContactUser@HostName. For successful registrations, this HostName is also included in the INVITE request's From header URI. If not configured or if registration fails, the 'SIP Group Name' parameter from the 'IP Group' table is used instead. This parameter can be up to 49 characters.

Register	Enables registration.
	- No = Don't register
	- Yes = Register
	When enabled, the device sends REGISTER requests to the Serving IP Group. In addition, to activate registration, you also need to set the parameter 'Registration Mode' to 'Per Account' in the 'Trunk Group Settings' table (refer to "Configuring the Trunk Group Settings" on page 197) for the specific Trunk Group. The Host Name (i.e., host name in SIP From/To headers) and Contact User (user in From/To and Contact headers) are taken from this table upon a successful registration. See the example below:
	`REGISTER sip:audiocodes SIP/2.0`
	`Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac1397582418`
	`From: <sip:ContactUser@HostName>;tag=1c1397576231`
	`To: <sip: ContactUser@HostName >`
	`Call-ID: 1397568957261200022256@10.33.37.78`
	`CSeq: 1 REGISTER`
	`Contact: <sip:ContactUser@10.33.37.78>;expires=3600`
	`Expires: 3600`
	`User-Agent: Audiocodes-Sip-Gateway/v.5.40A.008.002`
	`Content-Length: 0`
	Notes:
	- The Trunk Group account registration is not effected by the parameter IsRegisterNeeded.
	- You can configure this table so that a specific IP Group can register to multiple ITSP's.This is performed by defining several rows in this table containing the same Served IP Group, but with different Serving IP Groups, user/password, Host Name and Contact User parameters.
	- If registration to an IP Group(s) fails for **all** the accounts defined in this table for a specific Trunk Group, and if this Trunk Group includes all the channels in the Trunk (refer to "Configuring the Trunk Group Table" on page 195), the

Parameter	Description
	Trunk Group is set to Out-Of-Service if the parameter OOSOnRegistrationFail is set to 1 (refer to "Proxy & Registration Parameters" on page 132).
Contact User	Defines the AOR user name. It appears in REGISTER From/To headers as ContactUser@HostName, and in INVITE/200 OK Contact headers as ContactUser@<device's IP address>. If not configured, the 'Contact User' parameter from the 'IP Group Table' page is used instead. **Note:** If registration fails, then the userpart in the INVITE Contact header contains the source party number.

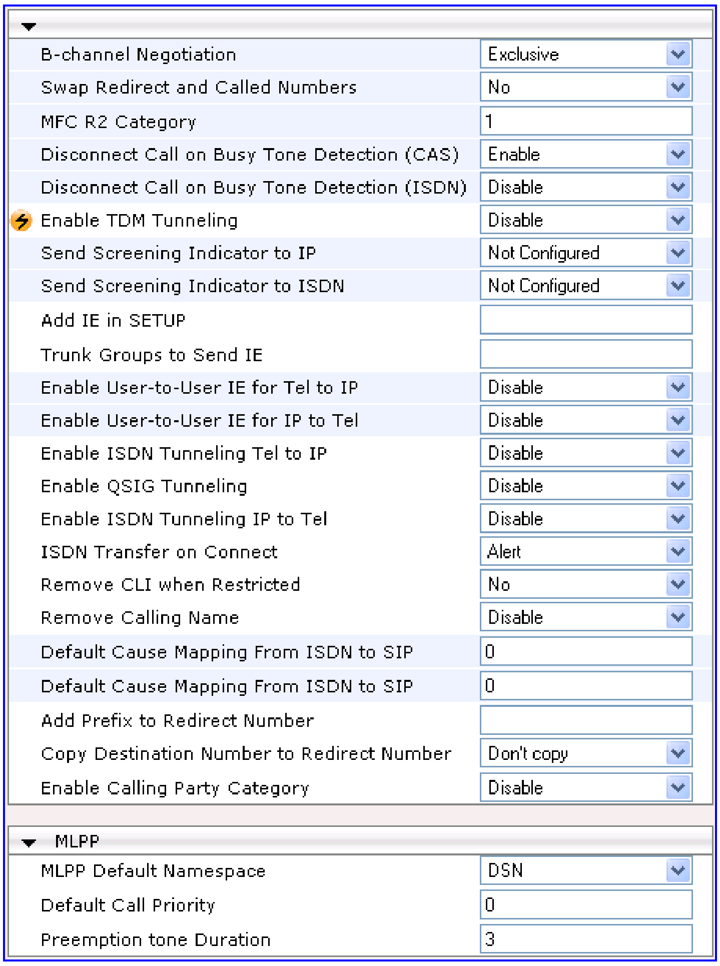
3.4.7.7 Configuring the Digital Gateway Parameters

The 'Digital Gateway Parameters' page allows you to configure miscellaneous digital parameters.

➢ To configure the digital gateway parameters, take these 4 steps:

1. Open the 'Digital Gateway Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **Digital Gateway** submenu > **Digital Gateway Parameters** page item).

Figure 3-86: Digital Gateway Parameters Page



B-channel Negotiation	Exclusive
Swap Redirect and Called Numbers	No
MFC R2 Category	1
Disconnect Call on Busy Tone Detection (CAS)	Enable
Disconnect Call on Busy Tone Detection (ISDN)	Disable
Enable TDM Tunneling	Disable
Send Screening Indicator to IP	Not Configured
Send Screening Indicator to ISDN	Not Configured
Add IE in SETUP	
Trunk Groups to Send IE	
Enable User-to-User IE for Tel to IP	Disable
Enable User-to-User IE for IP to Tel	Disable
Enable ISDN Tunneling Tel to IP	Disable
Enable QSIG Tunneling	Disable
Enable ISDN Tunneling IP to Tel	Disable
ISDN Transfer on Connect	Alert
Remove CLI when Restricted	No
Remove Calling Name	Disable
Default Cause Mapping From ISDN to SIP	0
Default Cause Mapping From ISDN to SIP	0
Add Prefix to Redirect Number	
Copy Destination Number to Redirect Number	Don't copy
Enable Calling Party Category	Disable

MLPP

MLPP Default Namespace	DSN
Default Call Priority	0
Preemption tone Duration	3

2. Configure the Digital Gateway parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-53: Digital Gateway Parameters Description

Parameter	Description
B-channel Negotiation **[BchannelNegotiation]**	Determines the ISDN B-Channel negotiation mode. ▪ **[0]** Preferred. ▪ **[1]** Exclusive (default). ▪ **[2]** Any. **Notes:** ▪ Applicable only to ISDN protocols. ▪ For some ISDN variants, when 'Any' (2) is selected, the SETUP message does not include the Channel Identification IE. ▪ The 'Any' (2) option is applicable only if the parameter 'ISDN Termination Side' is set to 'Use side' (refer to "Configuring the Trunk Settings" on page 82).
Swap Redirect and Called Numbers **[SwapRedirectNumber]**	▪ **[0]** No = Don't change numbers (default). ▪ **[1]** Yes = Incoming ISDN call that includes a redirect number (sometimes referred to as 'original called number') uses the redirect number instead of the called number.
MFC R2 Category **[R2Category]**	Determines the tone for MFC R2 Calling Party Category (CPC). The parameter provides information on the calling party such as National or International call, Operator or Subscriber and Subscriber priority. The value range is 1 to 15 (defining one of the MFC R2 tones). The default value is 1.
Disconnect Call on Busy Tone Detection (CAS) **[DisconnectOnBusyTone]**	Determines whether a call is disconnected upon detection of a busy tone. ▪ **[0]** Disable = Do not disconnect call on detection of busy tone. ▪ **[1]** Enable = Disconnect call on detection of busy tone (default). **Note:** This parameter is applicable only to CAS protocols.
Disconnect Call on Busy Tone Detection (ISDN) **[ISDNDisconnectOnBusyTone]**	Determines whether a call is disconnected upon detection of a busy tone. ▪ **[0]** = Do not disconnect call upon detection of busy tone. ▪ **[1]** = Disconnect call upon detection of busy tone (default). **Note:** This parameter is applicable only to ISDN protocols.
Enable TDM Tunneling **[EnableTDMoverIP]**	Enables TDM tunneling. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = TDM Tunneling is enabled. When TDM Tunneling is enabled, the originating device automatically initiates SIP calls from all enabled B-channels pertaining to E1/T1/J1 spans that are configured with the 'Transparent' protocol. The called number of each call is the internal phone number of the B-channel from where the call

Parameter	Description
	originates. The 'IP to Trunk Group' routing table is used to define the destination IP address of the terminating device. The terminating device automatically answers these calls if its E1/T1 protocol is set to 'Transparent' (ProtocolType = 5).
Send Screening Indicator to IP **[ScreeningInd2IP]**	Overrides the calling party's number (CPN) screening indication in the received ISDN SETUP message for Tel-to-IP calls. ▪ **[-1]** Not Configured = not configured (interworking from ISDN to IP) or set to 0 for CAS (default). ▪ **[0]** User Provided = CPN set by user, but not screened (verified). ▪ **[1]** User Passed = CPN set by user, verified and passed. ▪ **[2]** User Failed = CPN set by user, and verification failed. ▪ **[3]** Network Provided = CPN set by network. **Note:** Applicable only if Remote Party ID (RPID) header is enabled.
Send Screening Indicator to ISDN **[ScreeningInd2ISDN]**	Overrides the screening indicator of the calling party's number for IP-to-Tel ISDN calls. ▪ **[-1]** Not Configured = Not configured (interworking from IP to ISDN) (default). ▪ **[0]** User Provided = user provided, not screened. ▪ **[1]** User Passed = user provided, verified and passed. ▪ **[2]** User Failed = user provided, verified and failed. ▪ **[3]** Network Provided = network provided.
Add IE in SETUP **[AddIEinSetup]**	Adds an optional Information Element (IE) data (in hex format) to ISDN SETUP messages. For example, to add IE '0x20,0x02,0x00,0xe1', enter the following value for this parameter: '200200e1'. **Note:** This IE is sent from the Trunk Group IDs defined by the parameter SendIEonTG.
Trunk Groups to Send IE **[SendIEonTG]**	Defines Trunk Group IDs (up to 50 characters) from where the optional ISDN IE defined by the parameter AddIEinSetup is sent. For example: '1,2,4,10,12,6'.
Enable User-to-User IE for Tel to IP **[EnableUUITel2IP]**	Enables ISDN PRI-to-SIP interworking. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enable transfer of User-to-User Information Element (UUIE) from PRI to SIP. The device supports the following ISDN PRI-to-SIP interworking: SETUP to SIP INVITE, CONNECT to SIP 200 OK, USER INFORMATION to SIP INFO, ALERT to SIP 18x response, and DISCONNECT to SIP BYE response messages. **Note:** The interworking of User-to-User IE to SIP INFO is supported only on the 4ESS PRI variant.

Parameter	Description
Enable User-to-User IE for IP to Tel **[EnableUUIIP2Tel]**	Enables SIP-to-PRI ISDN interworking. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enable transfer of UUIE from SIP INVITE message to PRI SETUP message. The device supports the following SIP-to-PRI ISDN interworking: SIP INVITE to SETUP, SIP 200 OK to CONNECT, SIP INFO to USER INFORMATION, SIP 18x to ALERT, and SIP BYE to DISCONNECT. **Note:** The interworking of User-to-User IE to SIP INFO is supported only on 4ESS PRI variant.
Enable ISDN Tunneling Tel to IP **[EnableISDNTunnelingTel2IP]**	Enables ISDN Tunneling. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Using Header = Enable ISDN Tunneling from ISDN PRI to SIP using a proprietary SIP header. ▪ **[2]** Using Body = Enable ISDN Tunneling from ISDN PRI to SIP using a dedicated message body. When ISDN Tunneling is enabled, the device sends all ISDN PRI messages using the correlated SIP messages. The ISDN SETUP message is tunneled using SIP INVITE, all mid-call messages are tunneled using SIP INFO, and ISDN DISCONNECT / RELEASE is tunneled using SIP BYE messages. The raw data from the ISDN is inserted into a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages. **Note:** It is necessary to set the parameter ISDNDuplicateQ931BuffMode to 128 (i.e., duplicate all messages) for this feature to function.
Enable QSIG Tunneling **[EnableQSIGTunneling]**	Enables QSIG tunneling over SIP according to <draft-elwell-sipping-qsig-tunnel-03>. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Enable = Enable QSIG tunneling from QSIG to SIP and vice versa. When QSIG tunneling is enabled, all QSIG messages are sent as raw data in corresponding SIP messages using a dedicated message body. **Notes:** ▪ QSIG tunneling must be enabled on both originating and terminating devices. ▪ To enable this function, set the parameter ISDNDuplicateQ931BuffMode to 128 (i.e., duplicate all messages).
Enable ISDN Tunneling IP to Tel **[EnableISDNTunnelingIP2Tel]**	▪ **[0]** Disable = Disable (default). ▪ **[1]** Using Header = Enable ISDN Tunneling from SIP to ISDN PRI using a proprietary SIP header. ▪ **[2]** Using Body = Enable ISDN Tunneling from SIP to ISDN PRI using a dedicated message body. When ISDN Tunneling is enabled, the device extracts raw data received in a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages

Parameter	Description
	and sends the data as ISDN messages to the PSTN side.
ISDN Transfer On Connect **[SendISDNTransferOnConnect]**	This parameter is used for the ECT/TBCT/RLT/Path Replacement ISDN Transfer methods. Usually, the device requests the PBX to connect an incoming and outgoing call. This parameter determines if the outgoing call (from the device to the PBX) must be connected before the transfer is initiated. ▪ **[0]** Alert = Enable ISDN Transfer if outgoing call is in Alert or Connect state (default). ▪ **[1]** Connect = Enable ISDN Transfer only if outgoing call is in Connect state.
Remove CLI when Restricted **[RemoveCLIWhenRestricted]**	Determines (for IP-to-Tel calls) whether the Calling Number and Calling Name IEs are removed from the ISDN SETUP message if the presentation is set to Restricted. ▪ **[0]** No = IE aren't removed (default). ▪ **[1]** Yes = IE are removed.
Remove Calling Name **[RemoveCallingName]**	Enables the device to remove the Calling Name from SIP-to-ISDN calls. ▪ **[0]** Disable = Does not remove Calling Name (default). ▪ **[1]** Enable = Remove Calling Name.
Default Cause Mapping From ISDN to SIP **[DefaultCauseMapISDN2IP]**	Defines a single default ISDN release cause that is used (in ISDN-to-IP calls) instead of all received release causes, except when the following Q.931 cause values are received: Normal Call Clearing (16), User Busy (17), No User Responding (18), or No Answer from User (19). The range is valid Q.931 release causes (0 to 127). The default value is 0 (i.e., not configured - static mapping is used).
Add Prefix to Redirect Number **[Prefix2RedirectNumber]**	Defines a string prefix that is added to the Redirect number received from the Tel side. This prefix is added to the Redirect Number in the Diversion header. The valid range is an 8-character string. The default is an empty string.
Copy Destination Number to Redirect Number **[CopyDest2RedirectNumber]**	Determines whether the device copies the received ISDN called number to the outgoing SIP Diversion header for Tel-to-IP calls (even if a Redirecting Number IE is not received in the ISDN Setup message). Therefore, the called number is used as a redirect number. Call redirection information is typically used for Unified Messaging and voice mail services to identify the recipient of a message. ▪ **[0]** Don't copy = Disable (default). ▪ **[1]** Copy after phone number manipulation = Copies the called number after manipulation. The device first performs Tel-to-IP destination phone number manipulation (i.e., on the SIP To header), and only then copies the manipulated called number to the SIP Diversion header for the Tel-to-IP call. Therefore, with this option the called and redirected numbers are identical. ▪ **[2]** Copy before phone number manipulation = Copies the called number before manipulation. The device first copies the original called number to the SIP Diversion header, and then

Parameter	Description
	performs Tel-to-IP destination phone number manipulation. Therefore, this allows you to have different numbers for the called (i.e., SIP To header) and redirected (i.e., SIP Diversion header) numbers. **Notes:** ▪ If the incoming ISDN-to-IP call includes a Redirect Number, this number is overridden by the new called number if this parameter is set to 1 or 2. ▪ This parameter can also be configured for IP Profiles (refer to "IP Profile Settings" on page 193).
Enable Calling Party Category **[EnableCallingPartyCategory]**	Determines whether Calling Party Category (CPC) is mapped between SIP and PRI. ▪ **[0]** Disable = Don't relay the CPC between SIP and PRI (default). ▪ **[1]** Enable = The CPC is relayed between SIP and PRI. If enabled, the CPC received in the Originating Line Information (OLI) IE of an incoming ISDN SETUP message is relayed to the From / P-Asserted-Identity headers using the 'cpc' parameter, in the outgoing INVITE message, and vice versa. For example (calling party is a payphone): From:<sip:2000;cpc=payphone@10.8.23.70>;tag=1c1806157451 **Note:** This feature is supported only when using the NI-2 PRI variant.
Digital Out-Of-Service Behavior **[DigitalOOSBehavior]**	Determines the method for setting digital trunks to Out-Of-Service state per device. ▪ **[0]** Default = Uses default behavior for each trunk - see note below (default) ▪ **[1]** Service = Sends ISDN In or Out of Service (only for ISDN protocols that support Service message). ▪ **[2]** D-Channel = Takes D-Channel down or up (ISDN only). ▪ **[3]** Alarm = Sends or clears PSTN AIS Alarm (ISDN and CAS). ▪ **[4]** Block = Blocks trunk (CAS only). **Notes:** ▪ The default behavior (value 0) is as follows: - ISDN: Use Service messages on supporting variants and use Alarm on non-supporting variants. - CAS: Use Alarm. ▪ When updating this parameter value at run-time, you must stop the trunk and then restart it for the update to take effect. ▪ To determine the method for setting Out-Of-Service state per trunk, use the DigitalOOSBehaviorFor Trunk_ID parameter (refer to "Trunk Settings" on page 82).

Parameter	Description
MLPP (Multilevel Precedence and Preemption) (**Note:** For additional MLPP parameters, refer to "Supplementary Services" on page 159.)	
MLPP Default Namespace **[MLPPDefaultNamespace]**	Determines the Namespace used for MLPP calls received from the ISDN side and destined for the Application server. The Namespace value is not present in the Precedence IE of the PRI SETUP message. Therefore, the value is used in the Resource-Priority header of the outgoing SIP INVITE request. ▪ **[1]** DSN = DSN (default) ▪ **[2]** DOD = DOD ▪ **[3]** DRSN = DRSN
Default Call Priority **[SIPDefaultCallPriority]**	Defines the default call priority for MLPP calls. ▪ **[0]** 0 = ROUTINE (default) ▪ **[2]** 2 = PRIORITY ▪ **[6]** 6 = IMMEDIATE ▪ **[8]** 8 = FLASH-OVERRIDE ▪ **[9]** 9 = FLASH-OVERRIDE-OVERRIDE If the incoming SIP INVITE request doesn't contain a valid priority value in the SIP Resource-Priority header, the default value is used in the Precedence IE (after translation to the relevant ISDN Precedence value) of the outgoing PRI SETUP message. If the incoming PRI SETUP message doesn't contain a valid Precedence Level value, the default value is used in the Resource-Priority header of the outgoing SIP INVITE request. In this scenario, the character string is sent without translation to a numerical value.
Preemption Tone Duration **[PreemptionToneDuration]**	Defines the duration (in seconds) in which the device plays a preemption tone to both the Tel and IP sides if a call is preempted. The valid range is 0 to 60. The default is 3. **Note:** If set to 0, no preemption tone is played.

3.4.8 Advanced Applications

The **Advanced Applications** menu allows you to configure advanced SIP-based applications. This menu includes the following page items:

- Voice Mail Settings (refer to "Configuring the Voice Mail Parameters" on page 214)
- RADIUS Parameters (refer to "Configuring RADIUS Accounting Parameters" on page 217)

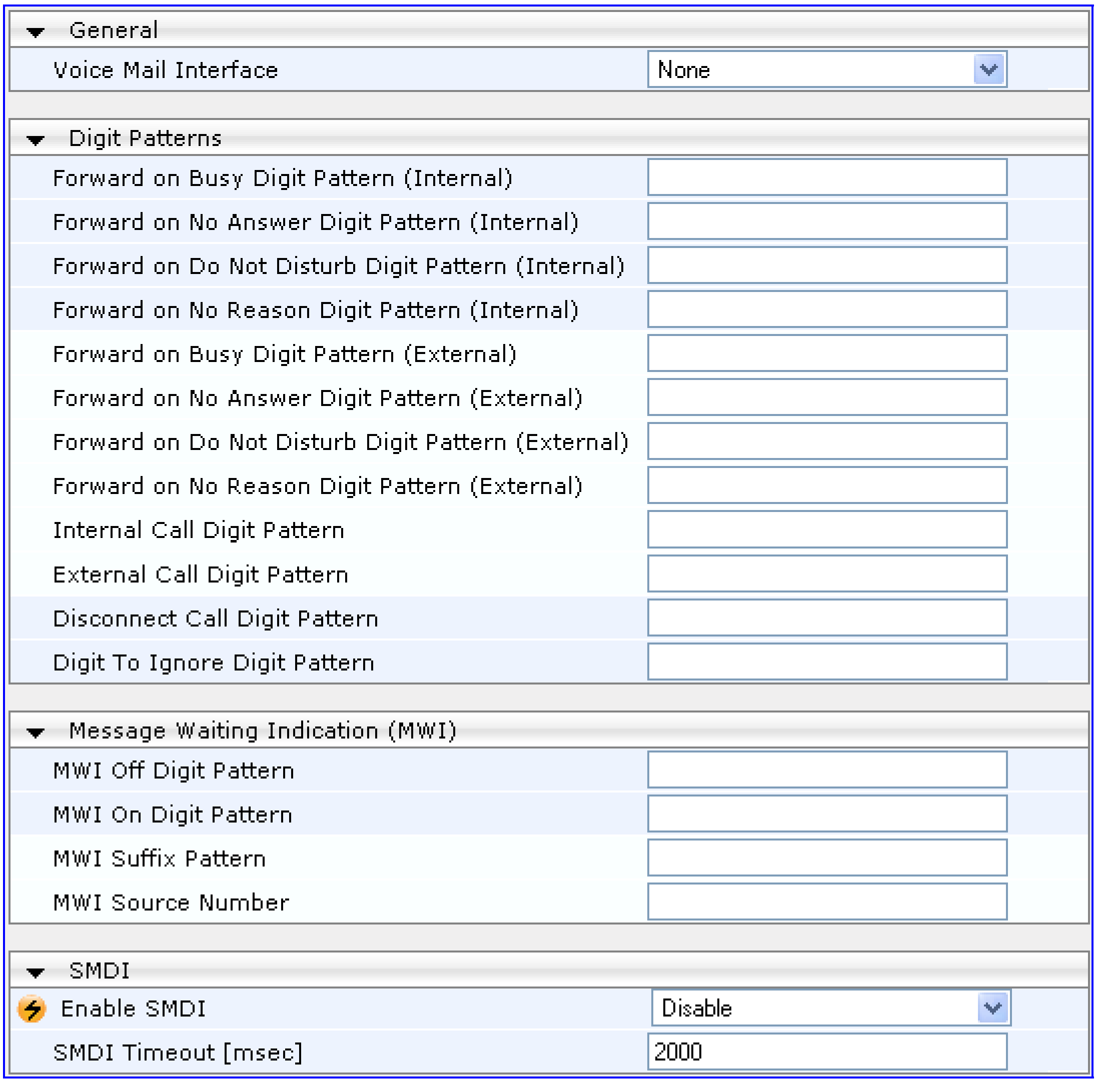
3.4.8.1 Configuring the Voice Mail (VM) Parameters

The 'Voice Mail Settings' page allows you to configure the voice mail parameters. The voice mail application applies only to CAS interfaces. For detailed information on voice mail, refer to the *CPE Configuration Guide for Voice Mail User's Manual*.

➢ To configure the Voice Mail parameters, take these 4 steps:

1. Open the 'Voice Mail Settings' page (**Configuration** tab > **Advanced Applications** menu > **Voice Mail Settings** page item).

Figure 3-87: Voice Mail Settings Page



General

Voice Mail Interface	None

Digit Patterns

Forward on Busy Digit Pattern (Internal)	
Forward on No Answer Digit Pattern (Internal)	
Forward on Do Not Disturb Digit Pattern (Internal)	
Forward on No Reason Digit Pattern (Internal)	
Forward on Busy Digit Pattern (External)	
Forward on No Answer Digit Pattern (External)	
Forward on Do Not Disturb Digit Pattern (External)	
Forward on No Reason Digit Pattern (External)	
Internal Call Digit Pattern	
External Call Digit Pattern	
Disconnect Call Digit Pattern	
Digit To Ignore Digit Pattern	

Message Waiting Indication (MWI)

MWI Off Digit Pattern	
MWI On Digit Pattern	
MWI Suffix Pattern	
MWI Source Number	

SMDI

Enable SMDI	Disable
SMDI Timeout [msec]	2000

2. Configure the voice mail parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-54: Voice Mail Parameters

Parameter	Description
General	
Voice Mail Interface **[VoiceMailInterface]**	Enables the voice mail application on the device and determines the communication method used between the PBX and the device. ▪ **[0]** None (default) ▪ **[1]** DTMF ▪ **[2]** SMDI ▪ **[3]** QSIG ▪ **[4]** SETUP Only (ISDN) ▪ **[5]** MATRA/AASTRA QSIG
Digit Patterns The following digit pattern parameters apply only to voice mail applications that use the DTMF communication method. For the available patterns' syntaxes, refer to the *CPE Configuration Guide for Voice Mail*.	
Forward on Busy Digit Pattern (Internal) **[DigitPatternForwardOnBusy]**	Determines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an internal extension. The valid range is a 120-character string.
Forward on No Answer Digit Pattern (Internal) **[DigitPatternForwardOnNoAnswer]**	Determines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an internal extension. The valid range is a 120-character string.
Forward on Do Not Disturb Digit Pattern (Internal) **[DigitPatternForwardOnDND]**	Determines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an internal extension. The valid range is a 120-character string.
Forward on No Reason Digit Pattern (Internal) **[DigitPatternForwardNoReason]**	Determines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an internal extension. The valid range is a 120-character string.
Forward on Busy Digit Pattern (External) **[DigitPatternForwardOnBusyExt]**	Determines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Forward on No Answer Digit Pattern (External) **[DigitPatternForwardOnNoAnswerExt]**	Determines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.

Parameter	Description
Forward on Do Not Disturb Digit Pattern (External) **[DigitPatternForwardOnDNDExt]**	Determines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Forward on No Reason Digit Pattern (External) **[DigitPatternForwardNoReasonExt]**	Determines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Internal Call Digit Pattern **[DigitPatternInternalCall]**	Determines the digit pattern used by the PBX to indicate an internal call. The valid range is a 120-character string.
External Call Digit Pattern **[DigitPatternExternalCall]**	Determines the digit pattern used by the PBX to indicate an external call. The valid range is a 120-character string.
Disconnect Call Digit Pattern **[TelDisconnectCode]**	Determines a digit pattern that when received from the Tel side, indicates the device to disconnect the call. The valid range is a 25-character string.
Digit To Ignore Digit Pattern **[DigitPatternDigitToIgnore]**	A digit pattern that if received as Src (S) or Redirect (R) numbers is ignored and not added to that number. The valid range is a 25-character string.
Message Waiting Indication (MWI)	
MWI Off Digit Pattern **[MWIOffCode]**	Determines the digit code used by the device to notify the PBX that there aren't any messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.
MWI On Digit Pattern **[MWIOnCode]**	Determines the digit code used by the device to notify the PBX of messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.
MWI Suffix Pattern **[MWISuffixCode]**	Determines the digit code used by the device as a suffix for 'MWI On Digit Pattern' and 'MWI Off Digit Pattern'. This suffix is added to the generated DTMF string after the extension number. The valid range is a 25-character string.
MWI Source Number **[MWISourceNumber]**	Determines the calling party's phone number used in the Q.931 MWI SETUP message to PSTN. If not configured, the channel's phone number is used as the calling number.
SMDI	
Enable SMDI **[SMDI]**	Enables Simplified Message Desk Interface (SMDI) interface on the device. ▪ **[0]** Disable = Normal serial (default). ▪ **[1]** Enable (Bellcore) ▪ **[2]** Ericsson MD-110 ▪ **[3]** NEC (ICS) **Note:** When the RS-232 connection is used for SMDI messages (Serial SMDI), it cannot be used for other

Parameter	Description
	applications, for example, to access the Command Line Interface (CLI).
SMDI Timeout **[SMDITimeOut]**	Determines the time (in msec) that the device waits for an SMDI Call Status message before or after a SETUP message is received. This parameter synchronizes the SMDI and analog CAS interfaces. If the timeout expires and only an SMDI message is received, the SMDI message is dropped. If the timeout expires and only a SETUP message is received, the call is established. The valid range is 0 to 10000 (i.e., 10 seconds). The default value is 2000.

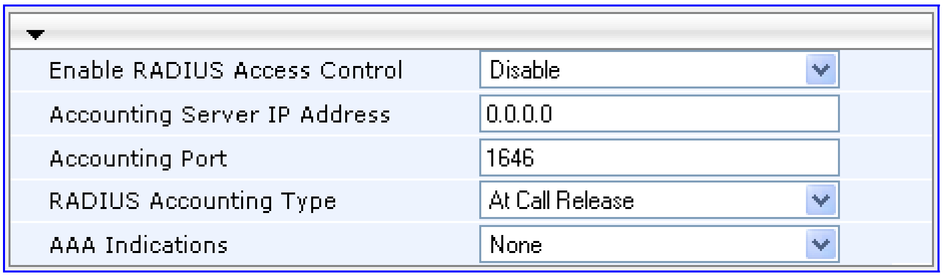
3.4.8.2 Configuring RADIUS Accounting Parameters

The 'RADIUS Parameters' page is used for configuring the Remote Authentication Dial In User Service (RADIUS) accounting parameters.

➢ To configure the RADIUS parameters, take these 4 steps:

1. Open the ‘RADIUS Parameters' page (**Configuration** tab > **Advanced Applications** menu > **RADIUS Parameters** page item).

Figure 3-88: RADIUS Parameters Page



Enable RADIUS Access Control	Disable
Accounting Server IP Address	0.0.0.0
Accounting Port	1646
RADIUS Accounting Type	At Call Release
AAA Indications	None

2. Configure the RADIUS accounting parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-55: RADIUS Parameters Description

Parameter	Description
Enable RADIUS Access Control **EnableRADIUS**	Enables or disables the RADIUS application. ▪ **[0]** Disable = disables RADIUS application (default) ▪ **[1]** Enable = enables RADIUS application
Accounting Server IP Address **[RADIUSAccServerIP]**	IP address of the RADIUS accounting server.
Accounting Port **[RADIUSAccPort]**	Port of the RADIUS accounting server. The default value is 1646.

Parameter	Description
RADIUS Accounting Type **[RADIUSAccountingType]**	Determines when the RADIUS accounting messages are sent to the RADIUS accounting server. ▪ **[0]** At Call Release = Sent at call release only (default). ▪ **[1]** At Connect & Release = Sent at call connect and release. ▪ **[2]** At Setup & Release = Sent at call setup and release.
AAA Indications **[AAAIndications]**	Determines the Authentication, Authorization and Accounting (AAA) indications. ▪ **[0]** None = No indications (default). ▪ **[3]** Accounting Only = Only accounting indications are used.

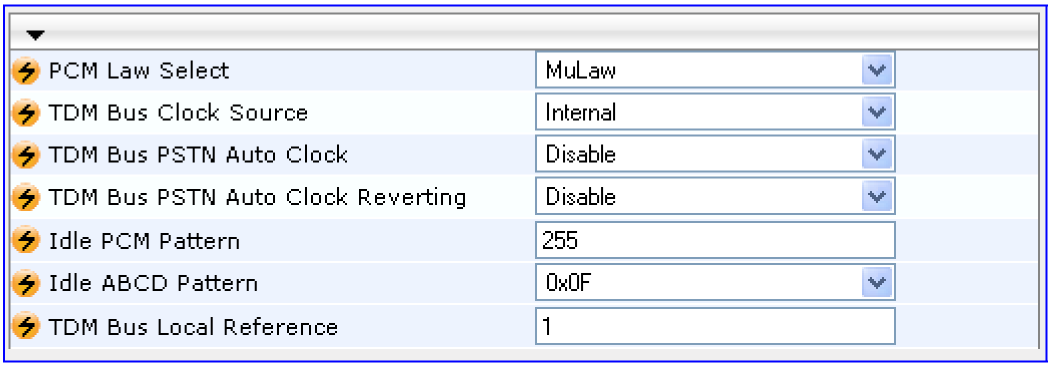
3.4.9 Configuring the TDM Bus Settings

The device's Time-Division Multiplexing (TDM) bus settings can be performed in the 'TDM Bus Settings' page, as described in the procedure below.

➢ To configure the TDM Bus settings, take these 5 steps:

1. Open the 'TDM Bus Settings' page (**Configuration** tab > **TDM Configuration** menu > **TDM Bus Settings** page item).

Figure 3-89: TDM Bus Settings Page



PCM Law Select	MuLaw
TDM Bus Clock Source	Internal
TDM Bus PSTN Auto Clock	Disable
TDM Bus PSTN Auto Clock Reverting	Disable
Idle PCM Pattern	255
Idle ABCD Pattern	0x0F
TDM Bus Local Reference	1

2. Configure the TDM bus parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. Save the changes to flash memory, refer to "Saving Configuration" on page 230.
5. Reset the device (refer to "Resetting the Device" on page 228).

Table 3-56: TDM Bus Settings Parameters Description

Parameter	Description
PCM Law Select **[PCMLawSelect]**	Determines the type of PCM companding law in input/output TDM bus. ▪ **[1]** Alaw = Alaw (default) ▪ **[3]** MuLaw = MuLaw **Note:** Typically, A-Law is used for E1 spans and µ-Law for T1/J1 spans.

Parameter	Description
Idle PCM Pattern **[IdlePCMPattern]**	Defines the PCM Pattern that is applied to the E1/T1 timeslot (B-channel) when the channel is idle. The range is 0 to 255. The default is set internally according to the Law select 1 (0xFF for Mu-Law; 0x55 for A-law).
Idle ABCD Pattern **[IdleABCDPattern]**	Defines the ABCD (CAS) Pattern that is applied to the CAS signaling bus when the channel is idle. The valid range is 0x0 to 0xF. The default is -1 (i.e., default pattern = 0000). **Note:** This parameter is applicable only when using PSTN interface with CAS protocols.
TDM Bus Local Reference **[TDMBusLocalReference]**	Physical Trunk ID from which the device recovers (receives) its clock synchronization. The range is 0 to the maximum number of Trunks. The default is Trunk ID 1. **Note:** This parameter is applicable only if the parameter TDMBusClockSource is set to 4 and the parameter TDMBusPSTNAutoClockEnable is set to 0.
TDM Bus PSTN Auto Clock **[TDMBusPSTNAutoClockEnable]**	Enables or disables the PSTN trunk Auto-Fallback Clock feature. ▪ **[0]** Disable (default) = Recovers the clock from the E1/T1 line defined by the parameter TDMBusLocalReference. ▪ **[1]** Enable = Recovers the clock from any connected synchronized slave E1/T1 line. If this trunk loses its synchronization, the device attempts to recover the clock from the next trunk. Note that initially, the device attempts to recover the clock from the trunk defined by the parameter TDMBusLocalReference. **Note:** This parameter is relevant only if the parameter TDMBusClockSource is set to 4.
TDM Bus PSTN Auto Clock Reverting **[TDMBusPSTNAutoClockRevertingEnable]**	Enables or disables the PSTN trunk auto-fallback reverting feature. If enabled and a trunk returning to service has an AutoClockTrunkPriority parameter value (refer to "Configuring the Trunk Settings" on page 82) that is higher than the priority of the local reference trunk (set in the TDMBusLocalReference parameter), the local reference reverts to the trunk with the higher priority that has returned to service for the device's clock source. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** This parameter is applicable only when the TDMBusPSTNAutoClockEnable parameter is set to 1.
TDM Bus Clock Source **[TDMBusClockSource]**	Selects the clock source to which the device synchronizes. ▪ **[1]** Internal = Generate clock from local source (default). ▪ **[4]** Network = Recover clock from PSTN line. For detailed information on configuring the device's clock settings, refer to "Clock Settings" on page 393.

3.5 Management Tab

The **Management** tab on the Navigation bar displays all menus related to device management. These menus appear in the Navigation tree and include the following:

- Management Configuration (refer to "Management Configuration" on page 220)
- Software Update (refer to "Software Update" on page 231)

3.5.1 Management Configuration

The **Management Configuration** menu allows you to configure the device's management parameters. This menu contains the following page items:

- Management Settings (refer to "Configuring the Management Settings" on page 220)
- Regional settings (refer to "Configuring the Regional Settings" on page 227)
- Maintenance Actions (refer to "Maintenance Actions" on page 228)

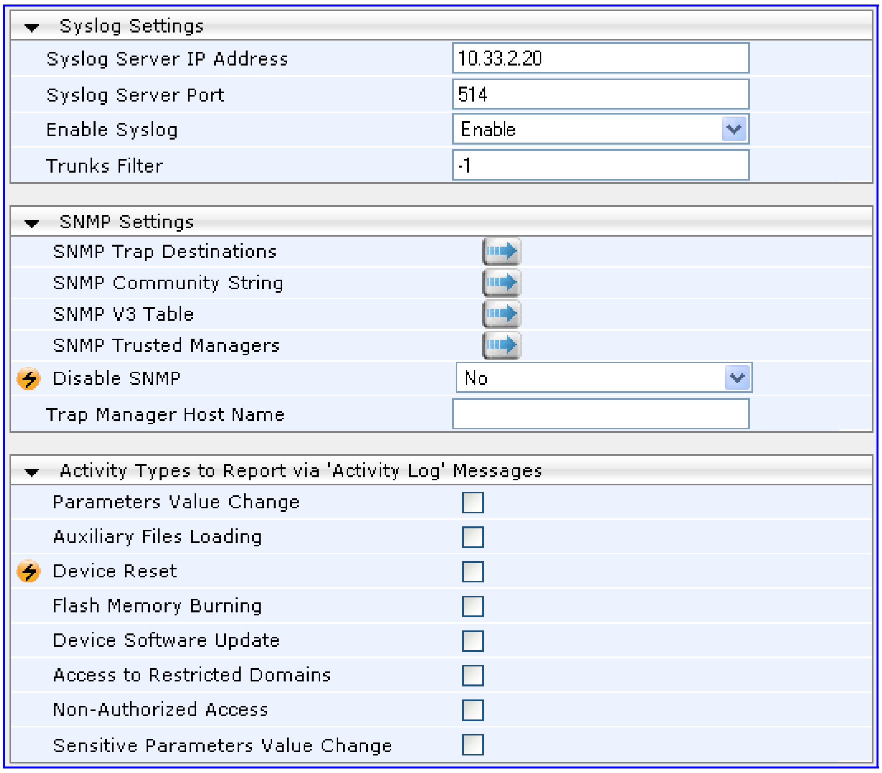
3.5.1.1 Configuring the Management Settings

The 'Management Settings' page allows you to configure the device's management parameters.

➢ To configure the Management parameters, take these 4 steps:

1. Open the 'Management Settings' page (**Management** tab > **Management Configuration** menu > **Management Settings** page item).

Figure 3-90: Management Settings Page



▼ Syslog Settings	
Syslog Server IP Address	10.33.2.20
Syslog Server Port	514
Enable Syslog	Enable
Trunks Filter	-1
▼ SNMP Settings	
SNMP Trap Destinations	➡
SNMP Community String	➡
SNMP V3 Table	➡
SNMP Trusted Managers	➡
⚡ Disable SNMP	No
Trap Manager Host Name	
▼ Activity Types to Report via 'Activity Log' Messages	
Parameters Value Change	□
Auxiliary Files Loading	□
⚡ Device Reset	□
Flash Memory Burning	□
Device Software Update	□
Access to Restricted Domains	□
Non-Authorized Access	□
Sensitive Parameters Value Change	□

2. Configure the Management Settings according to the table below.

3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Table 3-57: Management Settings Parameters

Parameter	Description
Syslog Settings	
Syslog Server IP Address **[SyslogServerIP]**	IP address (in dotted-decimal notation) of the computer you are using to run the Syslog server. The Syslog server is an application designed to collect the logs and error messages generated by the device. Default IP address is 0.0.0.0. For information on Syslog, refer to the *Product Reference Manual*.
Syslog Server Port **[SyslogServerPort]**	Defines the UDP port of the Syslog server. The valid range is 0 to 65,535. The default port is 514. For information on the Syslog, refer to the *Product Reference Manual*.
Enable Syslog **[EnableSyslog]**	Sends the logs and error message generated by the device to the Syslog server. ▪ **[0]** Disable = Logs and errors are not sent to the Syslog server (default). ▪ **[1]** Enable = Enables the Syslog server. **Notes:** ▪ If you enable Syslog, you must enter an IP address and a port number (using SyslogServerIP and SyslogServerPort parameters). ▪ You can configure the device to send Syslog messages implementing Debug Recording (refer to Debug Recording (DR)), by using the SyslogOutputMethod *ini* file parameter. ▪ Syslog messages may increase the network traffic. ▪ To configure Syslog logging levels, use the parameter GwDebugLevel, as described in "Advanced Parameters" on page 151. ▪ For information on the Syslog, refer to the *Product Reference Manual*.
SNMP Settings For detailed information on the SNMP parameters that can be configured via the *ini* file, refer to "SNMP Parameters" on page 282. For detailed information on developing an SNMP-based program to manage your device, refer to the *Product Reference Manual*.	
SNMP Trap Destinations	Click the arrow ➡ button to configure the SNMP trap destinations (refer to "Configuring the SNMP Trap Destinations Table" on page 222).
SNMP Community String	Click the arrow ➡ button to configure the SNMP community strings (refer to "Configuring the SNMP Community Strings" on page 224).
SNMP V3 Table	Click the arrow ➡ button to configure the SNMP V3 users (refer to "Configuring SNMP V3 Table" on page 225).

Parameter	Description
SNMP Trusted Managers	Click the arrow ➡ button to configure the SNMP Trusted Managers (refer to "Configuring SNMP Trusted Managers" on page 226).
Enable SNMP **[DisableSNMP]**	▪ **[0]** Enable = SNMP is enabled (default). ▪ **[1]** Disable = SNMP is disabled and no traps are sent.
Trap Manager Host Name **[SNMPTrapManagerHostName]**	Defines an FQDN of a remote host that is used as an SNMP manager. The resolved IP address replaces the last entry in the Trap Manager table (defined by the parameter SNMPManagerTableIP_x) and the last trap manager entry of snmpTargetAddrTable in the snmpTargetMIB. For example: 'mngr.corp.mycompany.com'. The valid range is a 99-character string.
Activity Types to Report via 'Activity Log' Messages The Activity Log mechanism enables the device to send log messages (to a Syslog server) for reporting on certain types of Web operations according to the below user-defined filters.	
Parameters Value Change **[ActivityListToLog = PVC]**	Changes made on-the-fly to parameters.
Auxiliary Files Loading **[ActivityListToLog = AFL]**	Loading of auxiliary files (e.g., via 'Certificate' page).
Device Reset **[ActivityListToLog = DR]**	Reset of device via the 'Maintenance Actions' page.
Flash Memory Burning **[ActivityListToLog = FB]**	Burning of files / parameters to flash (e.g., 'Maintenance Actions' page).
Device Software Update **[ActivityListToLog = SWU]**	*cmp* loading via the Software Upgrade Wizard.
Access to Restricted Domains **[ActivityListToLog = ARD]**	Access to Restricted Domains, which includes the following pages: ▪ *ini* parameters (AdminPage) ▪ General Security Settings ▪ Configuration File ▪ IPSec/IKE tables ▪ Software Upgrade Key ▪ Internal Firewall ▪ Web Access List ▪ Web User Accounts
Non-Authorized Access **[ActivityListToLog = NAA]**	Attempt to access the Web interface with a false / empty user name or password.
Sensitive Parameters Value Change **[ActivityListToLog = SPC]**	Changes made to sensitive parameters: (1) IP Address (2) Subnet Mask (3) Default Gateway IP Address (4) ActivityListToLog

3.5.1.1.1 Configuring the SNMP Trap Destinations Table

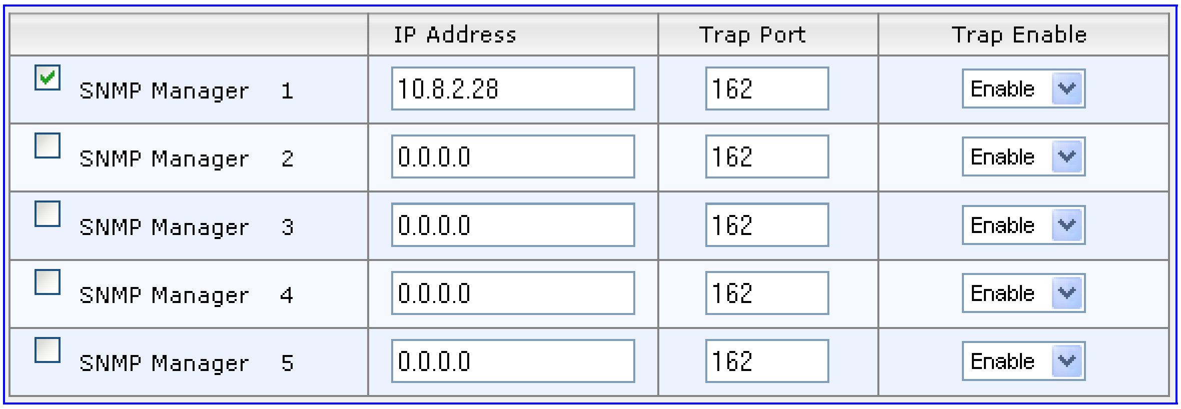
The 'SNMP Trap Destinations' page allows you to configure up to five SNMP trap managers.

➢ To configure the SNMP Trap Destinations table, take these 5 steps:

1. Access the 'Management Settings' page, as described in "Configuring the Management Settings" on page 220.

2. In the 'SNMP Trap Destinations' field, click the right-pointing arrow ➡ button; the 'SNMP Trap Destinations' page appears.

Figure 3-91: SNMP Trap Destinations Page



	IP Address	Trap Port	Trap Enable
☑ SNMP Manager 1	10.8.2.28	162	Enable
□ SNMP Manager 2	0.0.0.0	162	Enable
□ SNMP Manager 3	0.0.0.0	162	Enable
□ SNMP Manager 4	0.0.0.0	162	Enable
□ SNMP Manager 5	0.0.0.0	162	Enable

3. Configure the SNMP trap managers parameters according to the table below.

4. Click the **Submit** button to save your changes.

5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Note: Only table row entries whose corresponding check boxes are selected are applied when clicking **Submit**; otherwise, settings revert to their defaults.

Table 3-58: SNMP Trap Destinations Parameters Description

Parameter	Description
SNMP Manager **[SNMPManagerIsUsed_x]**	Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps. ▪ **[0]** (Check box cleared) = Disabled (default) ▪ **[1]** (Check box selected) = Enabled
IP Address **[SNMPManagerTableIP_x]**	IP address of the remote host used as an SNMP Manager. The device sends SNMP traps to these IP addresses. Enter the IP address in dotted-decimal notation, e.g., 108.10.1.255.
Trap Port **[SNMPManagerTrapPort_x]**	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to these ports. The valid SNMP trap port range is 100 to 4000. The default port is 162.

Parameter	Description
Trap Enable **[SNMPManagerTrapSendingEnable_x]**	Activates or de-activates the sending of traps to the corresponding SNMP Manager. ▪ **[0]** Disable = Sending is disabled. ▪ **[1]** Enable = Sending is enabled (default).

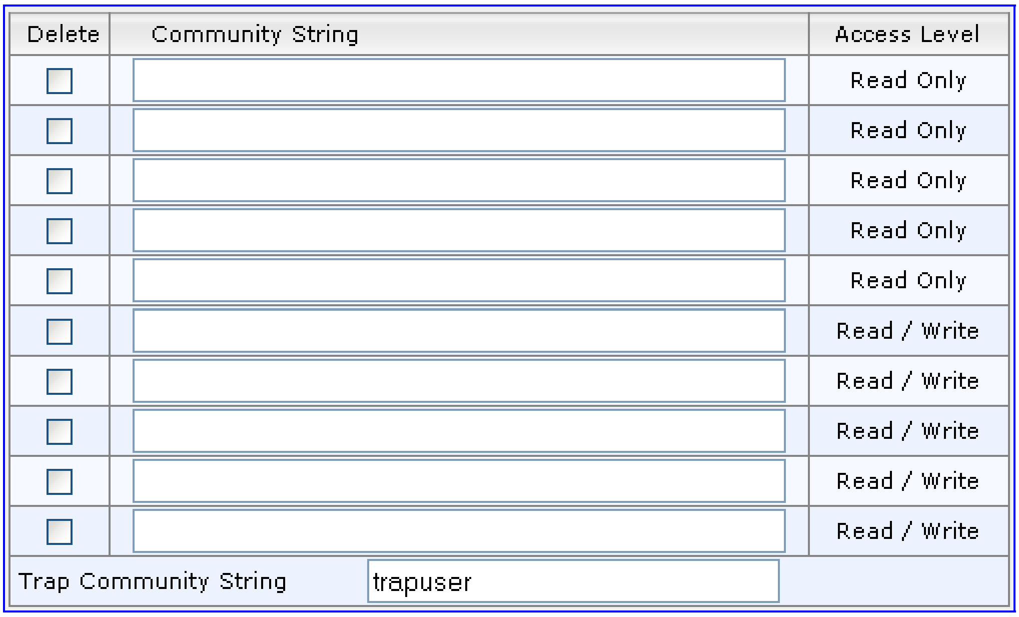
3.5.1.1.2 Configuring the SNMP Community Strings

The 'SNMP Community String' page allows you to configure up to five read-only and up to five read-write SNMP community strings, and to configure the community string that is used for sending traps. For detailed information on SNMP community strings, refer to the *Product Reference Manual*.

➢ To configure the SNMP community strings, take these 5 steps:

1. Access the 'Management Settings' page, as described in "Configuring the Management Settings" on page 220.
2. In the 'SNMP Community String' field, click the right-pointing arrow ➡ button; the 'SNMP Community String' page appears.

Figure 3-92: SNMP Community Strings Page



Delete	Community String	Access Level
□		Read Only
□		Read Only
□		Read Only
□		Read Only
□		Read Only
□		Read / Write
□		Read / Write
□		Read / Write
□		Read / Write
□		Read / Write
Trap Community String	trapuser	

3. Configure the SNMP community strings parameters according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, refer to "Saving Configuration" on page 230.

Note: To delete a community string, select the **Delete** check box corresponding to the community string that you want to delete, and then click **Submit**.

Table 3-59: SNMP Community Strings Parameters Description

Parameter	Description
Community String	▪ Read Only **[SNMPReadOnlyCommunityString_x]:** Up to five read-only community strings (up to 19 characters each). The default string is 'public'. ▪ Read / Write **[SNMPReadWriteCommunityString_x]:** Up to five read / write community strings (up to 19 characters each). The default string is 'private'.
Trap Community String **[SNMPTrapCommunityString]**	Community string used in traps (up to 19 characters). The default string is 'trapuser'.

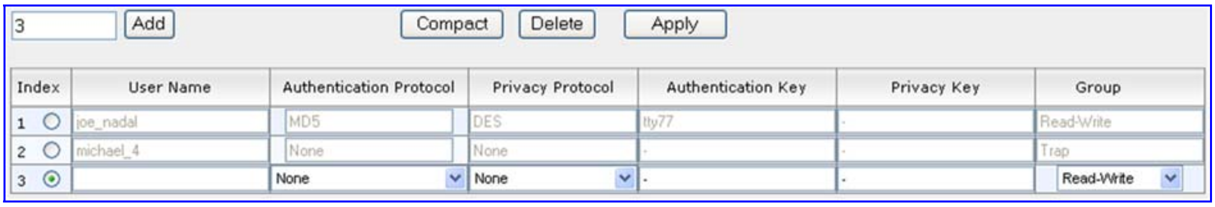
3.5.1.1.3 Configuring SNMP V3 Users

The 'SNMP V3 Settings' page allows you to configure authentication and privacy for up to 10 SNMP v3 users.

➢ To configure the SNMP v3 users, take the following 6 steps:

1. Access the 'Management Settings' page, as described in "Configuring the Management Settings" on page 220.
2. In the 'SNMP V3 Table' field, click the right-pointing arrow ➡ button; the 'SNMP V3 Settings' page appears.

Figure 3-93: SNMP V3 Setting Page



Index		User Name	Authentication Protocol	Privacy Protocol	Authentication Key	Privacy Key	Group
1	○	joe_nadal	MD5	DES	tty77	-	Read-Write
2	○	michael_4	None	None	-	-	Trap
3	●		None	None	-	-	Read-Write

3. To add an SNMP v3 user, in the 'Add' field, enter the desired row index, and then click **Add**. A new row appears.
4. Configure the SNMP V3 Setting parameters according to the table below.
5. Click the **Apply** button to save your changes.
6. To save the changes, refer to "Saving Configuration" on page 230.

Notes:

- For a description of the web interface's table command buttons (e.g., **Duplicate** and **Delete**), refer to "Working with Tables" on page 30.
- You can also configure SNMP v3 users using the *ini* file table parameter SNMPUsers (refer to "SNMP Parameters" on page 282).

Table 3-60: SNMP V3 Users Parameters

Parameter	Description
Index **[SNMPUsers_Index]**	The table index. The valid range is 0 to 9.
User Name **[SNMPUsers_Username]**	Name of the SNMP v3 user. This name must be unique.
Authentication Protocol **[SNMPUsers_AuthProtocol]**	Authentication protocol of the SNMP v3 user. ▪ **[0]** None (default) ▪ **[1]** MD5 ▪ **[2]** SHA-1
Privacy Protocol **[SNMPUsers_PrivProtocol]**	Privacy protocol of the SNMP v3 user. ▪ **[0]** None (default) ▪ **[1]** DES ▪ **[2]** 3DES ▪ **[3]** AES-128 ▪ **[4]** AES-192 ▪ **[5]** AES-256
Authentication Key **[SNMPUsers_AuthKey]**	Authentication key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
Privacy Key **[SNMPUsers_PrivKey]**	Privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
Group **[SNMPUsers_Group]**	The group with which the SNMP v3 user is associated. ▪ **[0]** Read-Only (default) ▪ **[1]** Read-Write ▪ **[2]** Trap **Note:** All groups can be used to send traps.

3.5.1.1.4 Configuring SNMP Trusted Managers

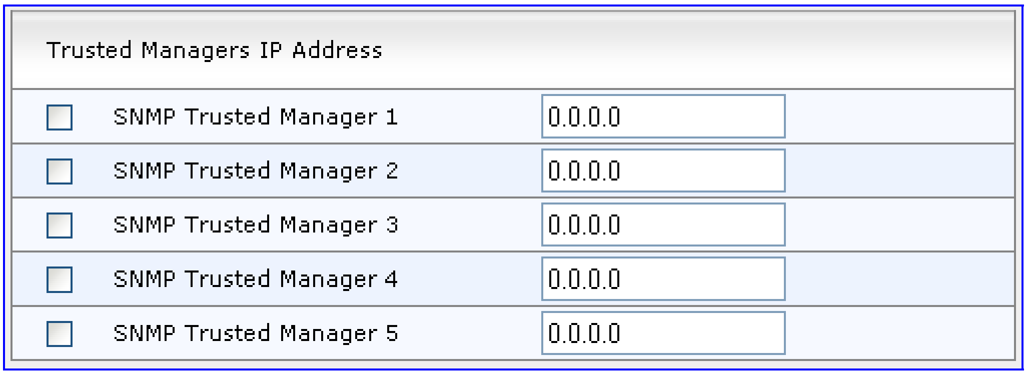
The 'SNMP Trusted Managers' page allows you to configure up to five SNMP Trusted Managers, based on IP addresses. By default, the SNMP agent accepts SNMP Get and Set requests from any IP address, as long as the correct community string is used in the request. Security can be enhanced by using Trusted Managers, which is an IP address from which the SNMP agent accepts and processes SNMP requests.

➢ **To configure the SNMP Trusted Managers, take the following 6 steps:**

1. Access the 'Management Settings' page, as described in "Configuring the Management Settings" on page 220.

2. In the 'SNMP Trusted Managers' field, click the right-pointing arrow ➡ button; the 'SNMP Trusted Managers' page appears.

Figure 3-94: SNMP Trusted Managers



Trusted Managers IP Address		
□	SNMP Trusted Manager 1	0.0.0.0
□	SNMP Trusted Manager 2	0.0.0.0
□	SNMP Trusted Manager 3	0.0.0.0
□	SNMP Trusted Manager 4	0.0.0.0
□	SNMP Trusted Manager 5	0.0.0.0

3. Select the check box corresponding to the SNMP Trusted Manager that you want to enable and for whom you want to define an IP address.
4. Define an IP address in dotted-decimal notation.
5. Click the **Submit** button to apply your changes.
6. To save the changes, refer to "Saving Configuration" on page 230.

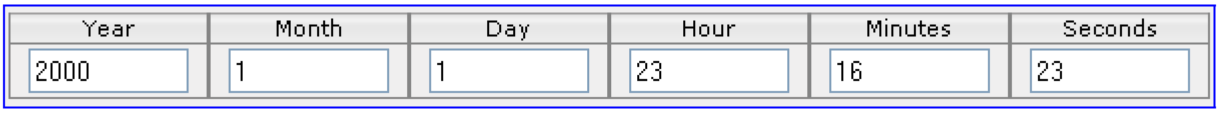
3.5.1.2 Configuring the Regional Settings

The 'Regional Settings' page allows you to define and view the device's internal date and time.

➢ To configure the device's date and time, take these 3 steps:

1. Open the 'Regional Settings' page (**Management** tab > **Management Configuration** menu > **Regional Settings** page item).

Figure 3-95: Regional Settings Page



Year	Month	Day	Hour	Minutes	Seconds
2000	1	1	23	16	23

2. Enter the current date and time in the geographical location in which the device is installed.
3. Click the **Submit** button; the date and time are automatically updated.

Notes:

- If the device is configured to obtain the date and time from an SNTP server (refer to "Configuring the Application Settings" on page 57), the fields on this page are read-only and cannot be modified. For an explanation on SNTP, refer to "Simple Network Time Protocol Support" on page 383.
- After performing a hardware reset, the date and time are returned to their defaults and therefore, should be updated.

3.5.1.3 Maintenance Actions

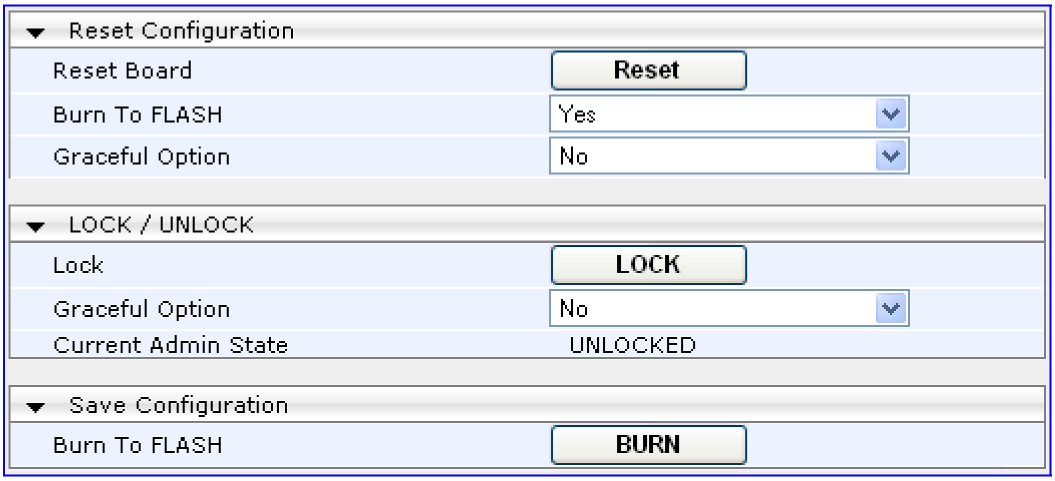
The 'Maintenance Actions' page allows you to perform the following operations:

- Reset the device (refer to "Resetting the Device" on page 228)
- Lock and unlock the device (refer to "Locking and Unlocking the Device" on page 229)
- Save the configuration to the device's flash memory (refer to "Saving Configuration" on page 230)

➢ To access the 'Maintenance Actions' page, take this step:

- On the Navigation bar, click the **Management** tab, and then in the Navigation tree, select the **Management Configuration** menu, and then choose the **Maintenance Actions** page item.

Figure 3-96: Maintenance Actions Page



Reset Configuration
Reset Board: Reset
Burn To FLASH: Yes
Graceful Option: No

LOCK / UNLOCK
Lock: LOCK
Graceful Option: No
Current Admin State: UNLOCKED

Save Configuration
Burn To FLASH: BURN

3.5.1.3.1 Resetting the Device

The 'Maintenance Actions' page allows you to remotely reset the device. In addition, before resetting the device, you can choose the following options:

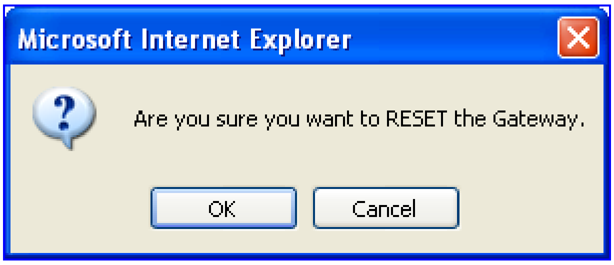
- Save the device's current configuration to the device's flash memory (non-volatile).
- Perform a graceful shutdown, i.e., device reset starts only after a user-defined time expires (i.e., timeout) or after no more active traffic exists (the earliest thereof).

➢ To reset the device, take these 6 steps:

1. Open the 'Maintenance Actions' page (refer to "Maintenance Actions" on page 228).
2. Under the 'Reset Configuration' group, from the 'Burn To FLASH' drop-down list, select one of the following options:
   - 'Yes': The device's current configuration is saved (*burned*) to the flash memory prior to reset (default).
   - 'No': Resets the device without saving the current configuration to flash (discards all unsaved modifications).

3. Under the 'Reset Configuration' group, from the 'Graceful Option' drop-down list, select one of the following options:
   - 'Yes': Reset starts only after the user-defined time in the 'Shutdown Timeout' field (refer to Step 4) expires or after no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
   - 'No': Reset starts regardless of traffic, and any existing traffic is terminated at once.
4. In the 'Shutdown Timeout' field (relevant only if the 'Graceful Option' in the previous step is set to 'Yes'), enter the time after which the device resets. Note that if no traffic exists and the time has not yet expired, the device resets.
5. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.

Figure 3-97: Reset Confirmation Message Box



Are you sure you want to RESET the Gateway.

6. Click **OK** to confirm device reset; if the parameter 'Graceful Option' is set to 'Yes' (in Step 3), the reset is delayed and a screen displaying the number of remaining calls and time is displayed. When the device begins to reset, a message appears notifying you of this.

Notes:

- Throughout the Web interface, parameters preceded by the lightning ⚡ symbol are not applied on-the-fly to the device and require that you reset the device for them to take effect.
- If you modify parameters that only take effect after a device reset, after you click the **Submit** button, the toolbar displays the word 'Reset' (refer to "Toolbar" on page 21) to remind you to later reset the device.

3.5.1.3.2 Locking and Unlocking the Device

The Lock and Unlock options allow you to lock the device so that it doesn't accept any new incoming calls. This is useful when, for example, you are uploading new software files to the device and you don't want any traffic to interfere with the process.

➢ To lock the device, take these 5 steps:

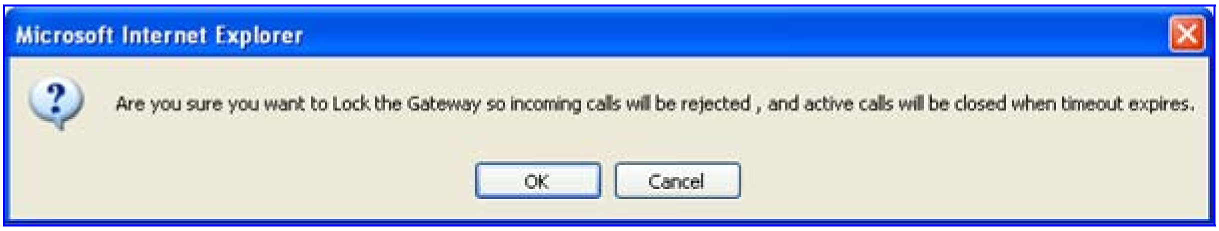
1. Open the 'Maintenance Actions' page (refer to "Maintenance Actions" on page 228).
2. Under the 'LOCK / UNLOCK' group, from the 'Graceful Option' drop-down list, select one of the following options:
   - 'Yes': The device is 'locked' only after the user-defined time in the 'Lock Timeout' field (refer to Step 3) expires or no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.

- 'No': The device is 'locked' regardless of traffic. Any existing traffic is terminated immediately.

Note: These options are only available if the current status of the device is in the Unlock state.

3. In the 'Lock Timeout' field (relevant only if the parameter 'Graceful Option' in the previous step is set to 'Yes'), enter the time (in seconds) after which the device locks. Note that if no traffic exists and the time has not yet expired, the device locks.
4. Click the **LOCK** button; a confirmation message box appears requesting you to confirm device Lock.

Figure 3-98: Device Lock Confirmation Message Box



Microsoft Internet Explorer

Are you sure you want to Lock the Gateway so incoming calls will be rejected , and active calls will be closed when timeout expires.

5. Click **OK** to confirm device Lock; if 'Graceful Option' is set to 'Yes', the lock is delayed and a screen displaying the number of remaining calls and time is displayed. Otherwise, the lock process begins immediately. The 'Current Admin State' field displays the current state: LOCKED or UNLOCKED.

➢ To unlock the device, take these 2 steps:

1. Open the 'Maintenance Actions' page (refer to "Maintenance Actions" on page 228).
2. Under the 'LOCK / UNLOCK' group, click the **UNLOCK** button. Unlock starts immediately and the device accepts new incoming calls.

3.5.1.3.3 Saving Configuration

The 'Maintenance Actions' page allows you to save (*burn*) the current parameter configuration (including loaded auxiliary files) to the device's *non-volatile* memory (i.e., flash). The parameter modifications that you make throughout the Web interface's pages are temporarily saved (to the *volatile* memory - RAM) when you click the **Submit** button on these pages. Parameter settings that are only saved to the device's RAM revert to their previous settings after a hardware/software reset (or power failure). Therefore, to ensure that your configuration changes are retained, you must save them to the device's flash memory using the burn option described below.

➢ To save the changes to the non-volatile flash memory , take these 2 steps:

1. Open the 'Maintenance Actions' page (refer to "Maintenance Actions" on page 228).
2. Under the 'Save Configuration' group, click the **BURN** button; a confirmation message appears when the configuration successfully saves.

Notes:

- Saving configuration to the *non-volatile* memory may disrupt traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (refer to "Locking and Unlocking the Device" on page 229).
- Throughout the Web interface, parameters preceded by the lightning ⚡ symbol are not applied on-the-fly to the device and require that you reset the device (refer to "Resetting the Device" on page 228) for them to take effect.

3.5.2 Software Update

The **Software Update** menu allows you to upgrade the device's software by loading a new *cmp* file (compressed firmware) along with the *ini* file and a suite of auxiliary files, or to update existing auxiliary files.

The **Software Update** menu includes the following page items:

- Load Auxiliary Files (refer to "Loading Auxiliary Files" on page 231)
- Software Update Key (refer to “Upgrading the Software Upgrade Key” on page 233)
- Software Upgrade Wizard (refer to "Software Upgrade Wizard" on page 236)
- Configuration File (refer to "Backing Up and Restoring Configuration" on page 240)

3.5.2.1 Loading Auxiliary Files

The 'Load Auxiliary Files' page allows you to load to the device various auxiliary files (described in the table below). For detailed information on these files, refer to "Auxiliary Configuration Files" on page 335. For information on deleting these files from the device, refer to "Device Information" on page 244.

Table 3-61: Auxiliary Files Descriptions

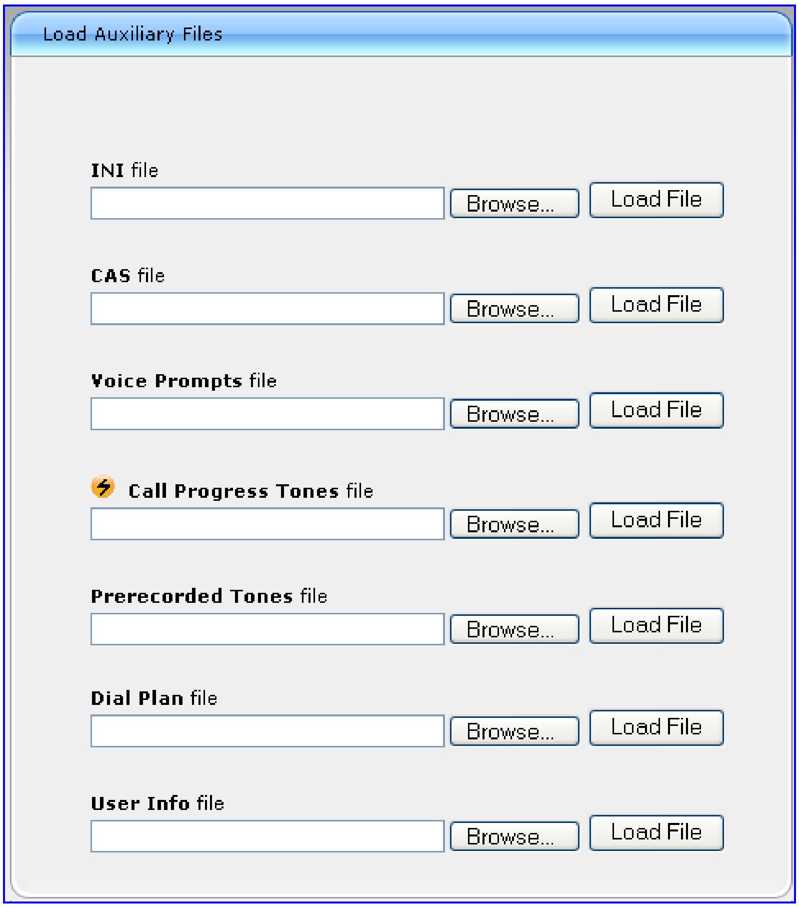
File Type	Description
ini	Provisions the device’s parameters. The Web interface enables practically full device provisioning, but customers may occasionally require new feature configuration parameters in which case this file is loaded. **Note:** Loading this file only provisions those parameters that are included in the *ini* file. Parameters that are not specified in the *ini* file are reset to factory default values.
CAS	Up to eight different CAS files containing specific CAS protocol definitions for digital modules. These files are provided to support various types of CAS signaling.
Voice Prompts	The voice announcement file contains a set of Voice Prompts (VP) that are played by the device during operation.
Dial Plan	Dial plan file.
Call Progress Tones	This is a region-specific, telephone exchange-dependent file that contains the Call Progress Tones (CPT) levels and frequencies that the device uses. The default CPT file is: U.S.A.

File Type	Description
Prerecorded Tones	The *dat* PRT file enhances the device's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the Call Progress Tones file.
User Info	The User Information file maps PBX extensions to IP numbers. This file can be used to represent PBX extensions as IP phones in the global 'IP world'.

➢ To load an auxiliary file to the device using the Web interface, take these 6 steps:

1. Open the 'Load Auxiliary Files' page (**Management** tab > **Software Update** menu > **Load Auxiliary Files** page item).

Figure 3-99: Load Auxiliary Files Page



2. Click the **Browse** button corresponding to the file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
3. Click the **Load File** button corresponding to the file you want to load.
4. Repeat steps 2 through 3 for each file you want to load.
5. To save the loaded auxiliary files to flash memory, refer to "Saving Configuration" on page 230.
6. To reset the device (if you have loaded a Call Progress Tones file), refer to "Resetting the Device" on page 228.

Notes:

- Saving an auxiliary file to flash memory may disrupt traffic on the device. To avoid this, disable all traffic on the device by performing a graceful lock (refer to "Locking and Unlocking the Device" on page 229).
- You can schedule automatic loading of updated auxiliary files using HTTP, HTTPS, FTP, or NFS (refer to the *Product Reference Manual*).

You can also load the Auxiliary files using the *ini* file. Before you load the files to the device, in the *ini* file you need to include certain *ini* file parameters associated with these files. These *ini* file parameters specify the files that you want loaded and whether they must be stored in the non-volatile memory. For a description of the *ini* file parameters associated with the auxiliary files, refer to "Configuration Files Parameters" on page 331.

➢ **To load the auxiliary files via the *ini* file, take these 3 steps:**

1. In the *ini* file, define the auxiliary files to be loaded to the device. You can also define in the *ini* file whether the loaded files must be stored in the non-volatile memory so that the TFTP process is not required every time the device boots up.
2. Save the auxiliary files you want to load and the *ini* file in the same directory on your PC.
3. Invoke a BootP/TFTP session; the *ini* and auxiliary files are loaded to the device.

3.5.2.2 Upgrading the Software Upgrade Key

The device is supplied with a Software Upgrade Key for each of its TrunkPack Modules (TPM). You can upgrade the device's features, capabilities, and quantity of available resources by by purchasing a new key to match your requirements. The Software Upgrade Key is provided in string format in a text file, which is loaded to the device's non-volatile flash memory. The string defines the device's allowed features and capabilities. A new key overwrites a previously installed key.

You can load a Software Upgrade Key using one of the following:

- Web interface
- BootP/TFTP configuration utility (refer to "Loading via BootP/TFTP" on page 235)
- AudioCodes' EMS (refer to *AudioCodes' EMS User's Manual* or *EMS Product Description*)

Warning: Don't modify the contents of the Software Upgrade Key file.

Notes:

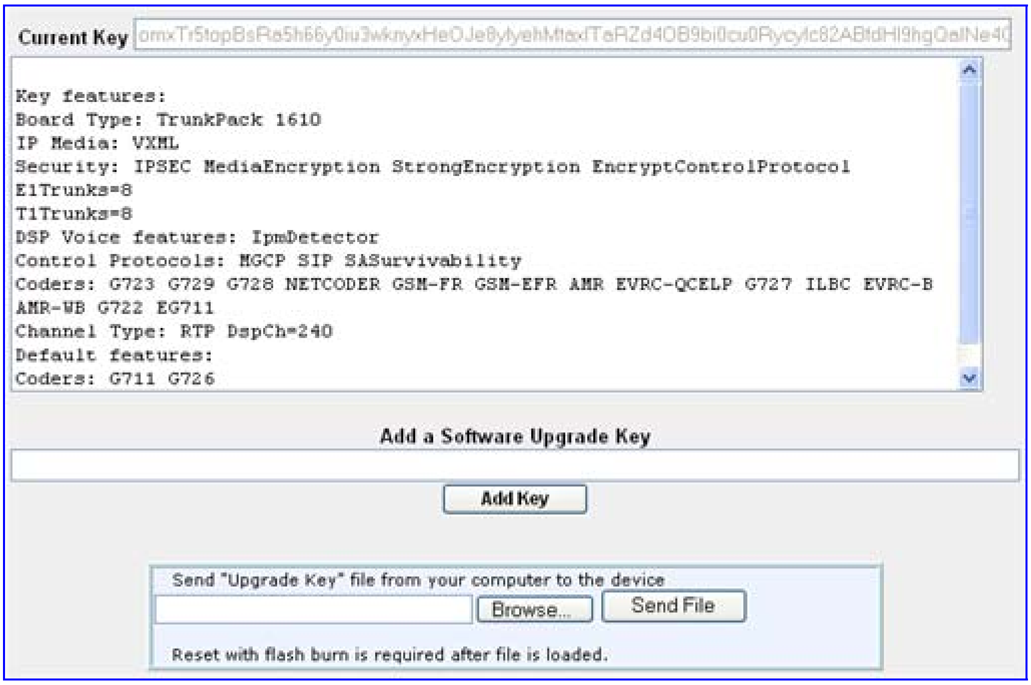
- The Software Upgrade Key is an encrypted key. Each TPM utilizes a unique key.
- The Software Upgrade Key is provided only by AudioCodes.

The procedure below describes how to load a Software Upgrade Key to the device using the Web interface.

➢ To load a Software Upgrade Key, take these 6 steps:

1. Open the 'Software Upgrade Key Status' page (**Management** tab > **Software Update** menu > **Software Upgrade Key** page item).

Figure 3-100: Software Upgrade Key Status Page



Current Key omxTr5topBsRa5h66y0iu3wknyxHeOJe8ylyehMtaxlTaRZd4OB9bi0cu0Rycylc82ABtdHI9hgQalNe4

```
Key features:
Board Type: TrunkPack 1610
IP Media: VXML
Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
E1Trunks=8
T1Trunks=8
DSP Voice features: IpmDetector
Control Protocols: MGCP SIP SASurvivability
Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B
AMR-WB G722 EG711
Channel Type: RTP DspCh=240
Default features:
Coders: G711 G726
```

Add a Software Upgrade Key
Add Key
Send "Upgrade Key" file from your computer to the device
Browse...
Send File
Reset with flash burn is required after file is loaded.

2. Backup your current Software Upgrade Key as a precaution so that you can re-load this backup key to restore the device's original capabilities if the new key doesn't comply with your requirements:

   a. In the 'Current Key' field, copy the string of text and paste it in any standard text file.

   b. Save the text file to a folder on your PC with a name of your choosing.

3. Open the new Software Upgrade Key file and ensure that the first line displays '[LicenseKeys]' and that it contains one or more lines in the following format: S/N<serial number of the first or second module> = <long Software Upgrade Key>

   For example: S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj...

   One S/N must match the serial number of your device. The device's serial number can be viewed in the 'Device Information' page (refer to "Device Information" on page 244).

4. Follow one of the following procedures, depending on whether you are loading a single or multiple key S/N lines:

   - **Single key S/N line:**

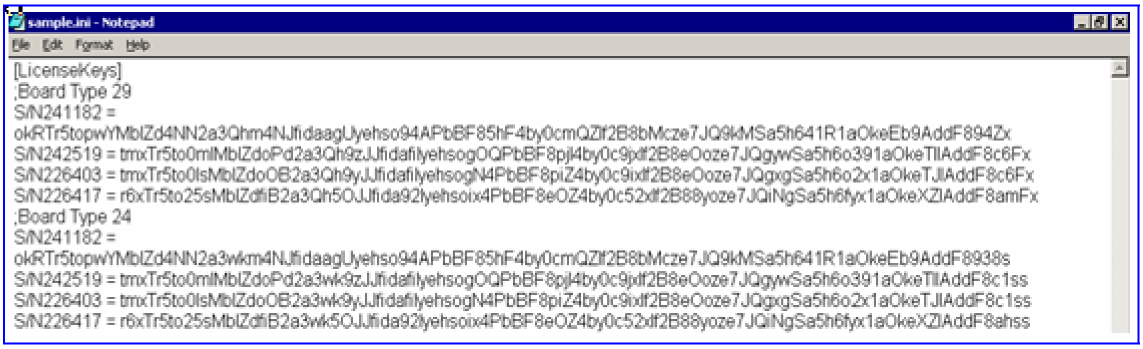
     a. Open the Software Upgrade Key text file (using, for example, Microsoft® Notepad).

     b. Select and copy the key string of the device's S/N and paste it into the field 'Add a Software Upgrade Key'.

     c. Click the **Add Key** button.

- **Multiple S/N lines (as shown below):**

Figure 3-101: Software Upgrade Key with Multiple S/N Lines



```
[LicenseKeys]
;Board Type 29
S/N241182 =
okRTr5topwYMblZd4NN2a3Qhm4NJfidaagUyehso94APbBF85hF4by0cmQZlf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF894Zx
S/N242519 = tmxTr5to0mlMblZdoPd2a3Qh9zJJfidafilyehsogOQPbBF8pjl4by0c9jxlf2B8eOoze7JQgywSa5h6o391aOkeTllAddF8c6Fx
S/N226403 = tmxTr5to0lsMblZdoOB2a3Qh9yJJfidafilyehsogN4PbBF8piZ4by0c9ixlf2B8eOoze7JQgxgSa5h6o2x1aOkeTJlAddF8c6Fx
S/N226417 = r6xTr5to25sMblZdfiB2a3Qh5OJJfida92lyehsoix4PbBF8eOZ4by0c52xlf2B88yoze7JQiNgSa5h6fyx1aOkeXZlAddF8amFx
;Board Type 24
S/N241182 =
okRTr5topwYMblZd4NN2a3wkm4NJfidaagUyehso94APbBF85hF4by0cmQZlf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF8938s
S/N242519 = tmxTr5to0mlMblZdoPd2a3wk9zJJfidafilyehsogOQPbBF8pjl4by0c9jxlf2B8eOoze7JQgywSa5h6o391aOkeTllAddF8c1ss
S/N226403 = tmxTr5to0lsMblZdoOB2a3wk9yJJfidafilyehsogN4PbBF8piZ4by0c9ixlf2B8eOoze7JQgxgSa5h6o2x1aOkeTJlAddF8c1ss
S/N226417 = r6xTr5to25sMblZdfiB2a3wk5OJJfida92lyehsoix4PbBF8eOZ4by0c52xlf2B88yoze7JQiNgSa5h6fyx1aOkeXZlAddF8ahss
```

a. in the 'Send Upgrade Key file' field, click the **Browse** button and navigate to the folder in which the Software Upgrade Key text file is located on your PC.

b. Click the **Send File** button; the new key is loaded to the device and validated. If the key is valid, it is burned to memory and displayed in the 'Current Key' field.

5. Verify that the Software Upgrade Key file was successfully loaded to the device, by using one of the following methods:

   - In the ‘Key features’ group, ensure that the features and capabilities activated by the installed string match those that were ordered.

   - Access the Syslog server (refer to the *Product Reference Manual*) and ensure that the following message appears in the Syslog server:
     "S/N___ Key Was Updated. The Board Needs to be Reloaded with ini file\n".

6. Reset the device; the new capabilities and resources are active.

Note: If the Syslog server indicates that the Software Upgrade Key file was unsuccessfully loaded (i.e., the 'SN_' line is blank), perform the following preliminary troubleshooting procedures:

1. Open the Software Upgrade Key file and check that the S/N line appears. If it does not appear, contact AudioCodes.

2. Verify that you’ve loaded the correct file. Open the file and ensure that the first line displays [LicenseKeys].

3. Verify that the contents of the file has not been altered in any way.

3.5.2.2.1 Loading via BootP/TFTP

The procedure below describes how to load a Software Upgrade Key to the device using AudioCodes' BootP/TFTP Server utility (for a detailed description on the BootP utility, refer to the *Product Reference Manual*).

➢ To load a Software Upgrade Key file using BootP/TFTP, take these 6 steps:

1. Place the Software Upgrade Key file (typically, a *.txt file) in the same folder in which the device's *cmp* file is located.

2. Start the BootP/TFTP Server utility.

3. From the **Services** menu, choose **Clients**; the 'Client Configuration' screen is displayed.

4. From the 'INI File' drop-down list, select the Software Upgrade Key file. Note that the device's *cmp* file must be specified in the 'Boot File' field.

5. Configure the initial BootP/TFTP parameters as required, and then click **OK**.

6. Reset the device; the *cmp* and Software Upgrade Key files are loaded to the device.

Note: To load the Software Upgrade Key using BootP/TFTP, the extension name of the key file must be **.ini*.

3.5.2.3 Software Upgrade Wizard

The Software Upgrade Wizard guides you through the process of software upgrade: selecting files and loading them to the device. The wizard also enables you to upgrade software while maintaining the existing configuration. Using the wizard obligates you to load and burn a *cmp* file to the device. You can choose to also use the wizard to load the *ini* and auxiliary files (e.g., Call Progress Tones*)*, but this option cannot be pursued without loading the *cmp* file. For the *ini* and each auxiliary file type, you can choose to reload an existing file, load a new file, or not load a file at all.

The Software Upgrade Wizard allows you to load the following files:

- cmp (mandatory) - compressed firmware file
- *ini* - configuration file
- Auxiliary files: CPT (Call Progress Tone), VP (Voice Prompts), PRT (Prerecorded Tones), CAS, and USRINF (User Info)

Warnings:

- Before upgrading the device to a new major software version (e.g., from version 5.4 to 5.6), save a copy of the device's configuration settings (i.e., *ini* file) to your PC (refer to "Backing Up and Restoring Configuration" on page 240) and ensure that you have all the original auxiliary files (e.g., CPT file) currently being used by the device. After you have upgraded the device, upload these files to the device.
- The Software Upgrade Wizard requires the device to be reset at the end of the process, which may disrupt its traffic. To avoid this, disable all traffic on the device before initiating the wizard by performing a graceful lock (refer to "Locking and Unlocking the Device" on page 229).

Notes:

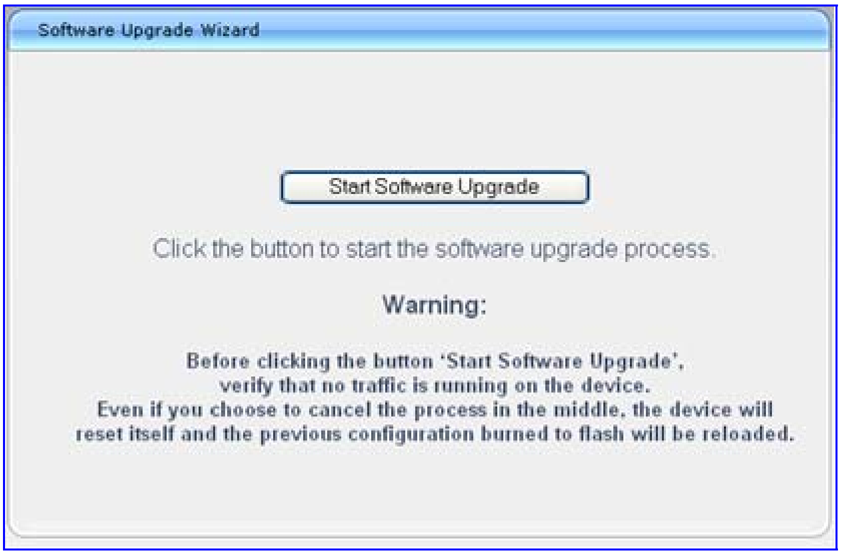
- Before you can load an *ini* or any auxiliary file, you must first load a *cmp* file.
- When you activate the wizard, the rest of the Web interface is unavailable. After you load the desired files, access to the full Web interface is restored.
- You can schedule automatic loading of *cmp, ini,* and auxiliary files using HTTP, HTTPS, FTP, or NFS. (Refer to the *Product Reference Manual*).

➢ To use the Software Upgrade Wizard, take these 11 steps:

1. Stop all traffic on the device (refer to the note above).

2. Open the 'Software Upgrade Wizard' (**Management** tab > **Software Update** menu > **Software Upgrade Wizard**); the 'Software Upgrade Wizard' page appears.

Figure 3-102: Start Software Upgrade Wizard Screen



Software Upgrade Wizard

Start Software Upgrade

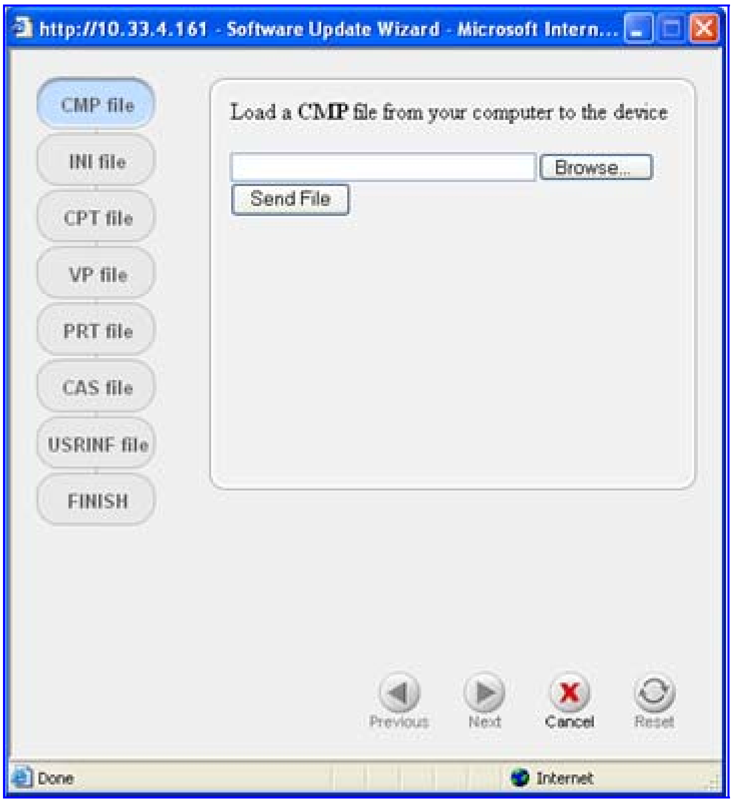
Click the button to start the software upgrade process.

Warning:

Before clicking the button 'Start Software Upgrade', verify that no traffic is running on the device. Even if you choose to cancel the process in the middle, the device will reset itself and the previous configuration burned to flash will be reloaded.

3. Click the **Start Software Upgrade** button; the 'Load a CMP file' Wizard page appears.

Figure 3-103: Load CMP File Wizard Page



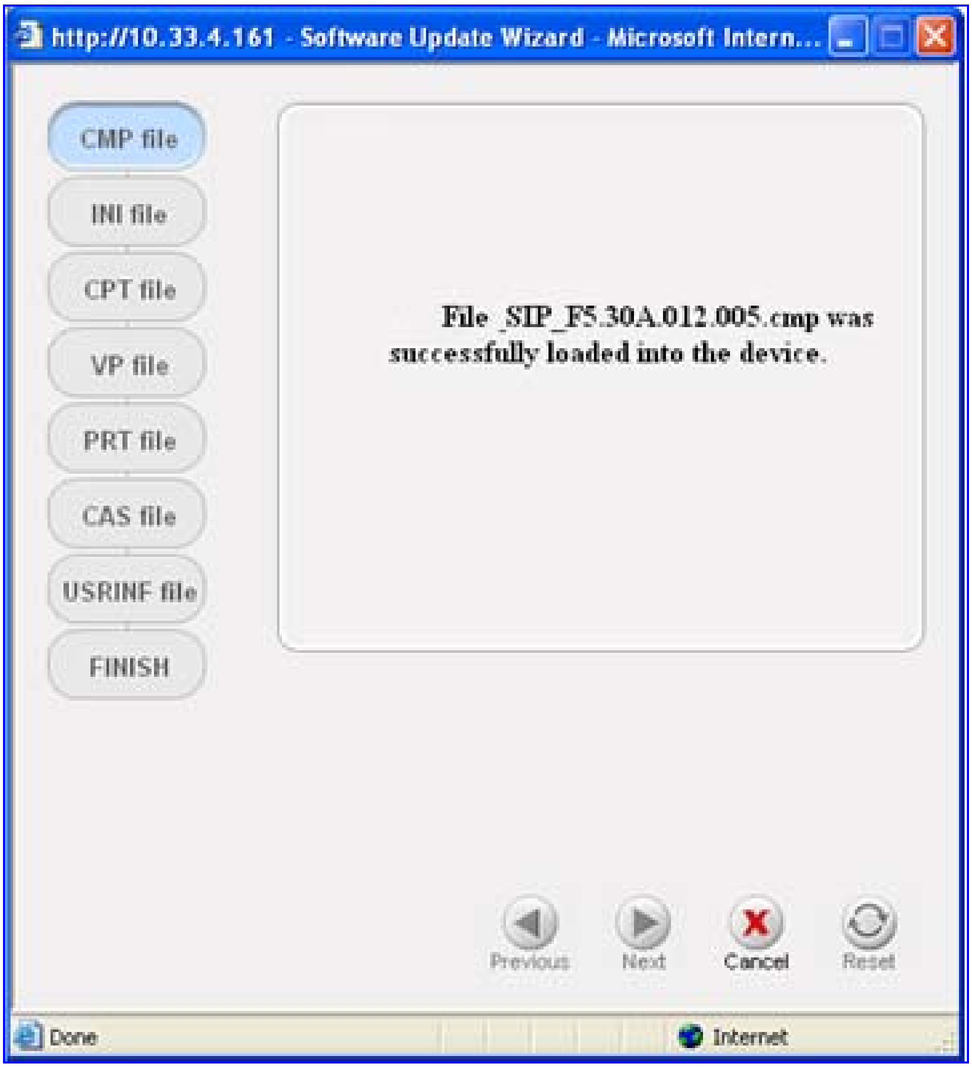
http://10.33.4.161 - Software Update Wizard - Microsoft Intern...

Load a CMP file from your computer to the device

Note: At this stage, you can quit the Software Update Wizard, by clicking **Cancel** ☒, without requiring a device reset. However, once you start uploading a cmp file, the process must be completed with a device reset.

4. Click the **Browse** button, navigate to the *cmp* file, and then click **Send File**; the *cmp* file is loaded to the device and you're notified as to a successful loading, as shown below.

Figure 3-104: CMP File Successfully Loaded Message



File SIP_F5.30A.012.005.cmp was successfully loaded into the device.

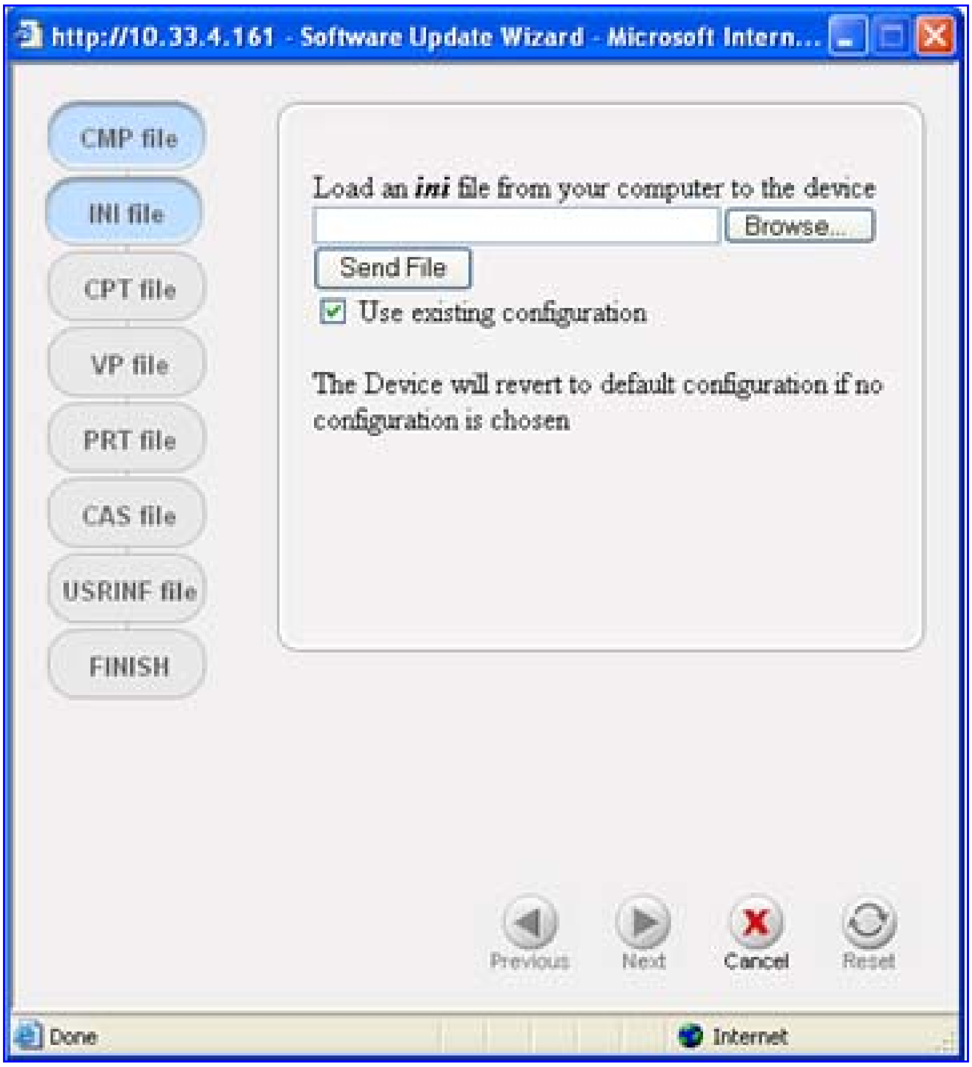
5. Click one of the following buttons:

- **Reset**; the device resets with the newly loaded *cmp,* and utilizing the current configuration and auxiliary files.
- **Next**; the 'Load an *ini* File' wizard page opens.

Note that as you progress by clicking **Next**, the relevant file name corresponding to the applicable Wizard page is highlighted in the file list on the left.

6. In the 'Load an *ini* File' page, you can now choose to either:
   - Click **Browse**, navigate to the *ini* file, and then click **Send File**; the *ini* file is loaded to the device and you're notified as to a successful loading.
   - Use the *ini* file currently used by the device, by not selecting an *ini* file and by ensuring that the 'Use existing configuration' check box is marked (default).
   - Return the device's configuration settings to factory defaults, by not selecting an *ini* file and by clearing the 'Use existing configuration' check box.

Figure 3-105: Load an ini File Wizard Page



Load an *ini* file from your computer to the device

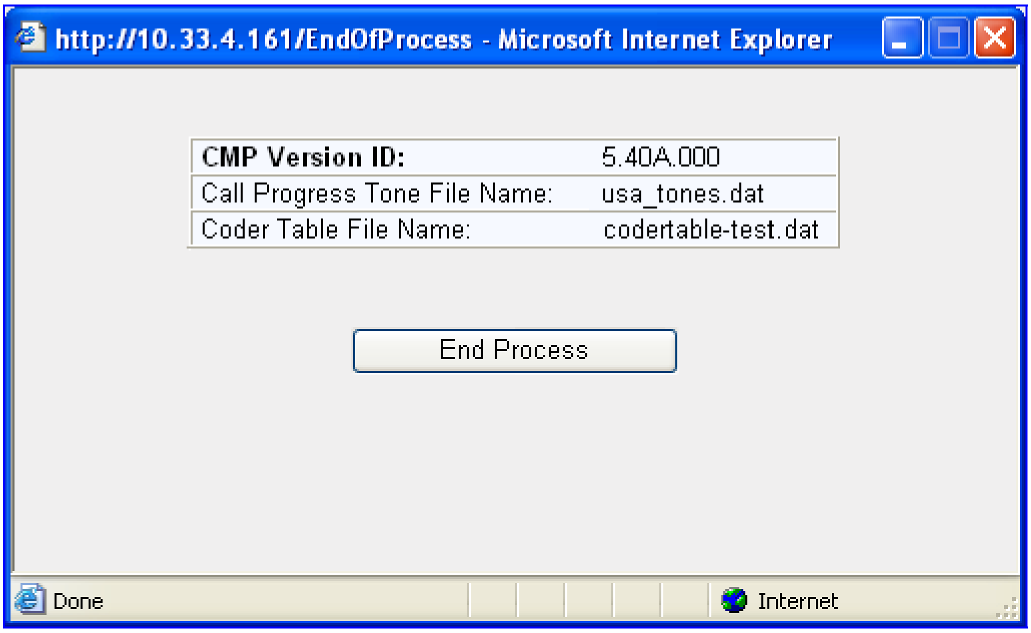
☑ Use existing configuration

The Device will revert to default configuration if no configuration is chosen

7. You can now choose to either:
   - Click **Reset**; the device resets, utilizing the new *cmp* and *ini* file you loaded up to now as well as utilizing the other auxiliary files.
   - Click **Back**; the 'Load a *cmp* file' page is opened again.
   - Click **Next**; the next page opens for loading the next consecutive auxiliary file listed in the Wizard.
8. Follow the same procedure as for loading the *ini* file (Step 6) for loading the auxiliary files.

9. In the 'FINISH' page, complete the upgrade process by clicking **Reset;** the device 'burns' the newly loaded files to flash memory and then resets t.he device. After the device resets, the 'End Process' screen appears displaying the burned configuration files (refer to the figure below).

Figure 3-106: End Process Wizard Page

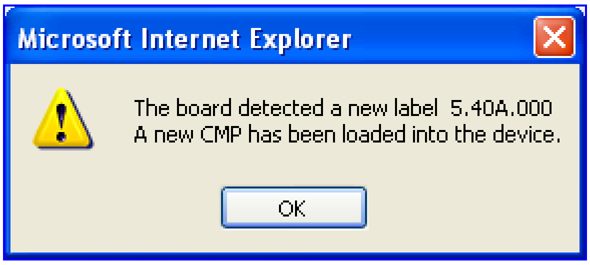


http://10.33.4.161/EndOfProcess - Microsoft Internet Explorer
End Process
Done
Internet

CMP Version ID:	5.40A.000
Call Progress Tone File Name:	usa_tones.dat
Coder Table File Name:	codertable-test.dat

10. Click **End Process** to close the wizard, and then in the 'Enter Network Password' dialog box, enter your login user name and password (described in "Accessing the Web Interface" on page 20) and click **OK**; a message box appears informing you of the new CMP file:

Figure 3-107: Message Box Informing of Upgraded CMP File



The board detected a new label 5.40A.000
A new CMP has been loaded into the device.

11. Click **OK**; the Web interface now becomes active and reflecting the upgraded device.

3.5.2.4 Backing Up and Restoring Configuration

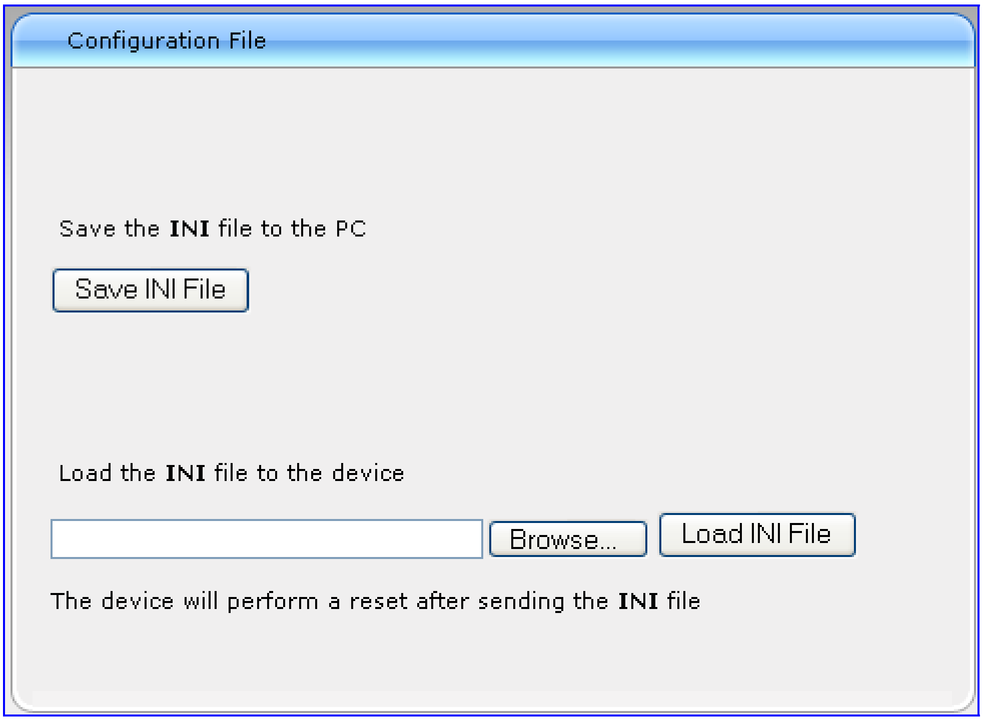
The 'Configuration File' page allows you to save a copy of the device's current configuration file modifications as an *ini* file to a PC. This is useful for backing up your configuration to protect your device configuration. The saved *ini* file includes only those parameters that were modified as well as parameters with other than default values.

In addition, this page allows you to load an *ini* file to the device. If the device has lost its configuration, you can restore the device's configuration by loading the previously saved *ini* file, or by simply loading a newly created *ini* file.

➢ To save and restore the *ini* file, take these 3 steps:

1. Open the 'Configuration File' page (**Management** tab > **Software Update** menu > **Configuration File**).

Figure 3-108: Configuration File Page



Configuration File

Save the INI file to the PC

Load the INI file to the device

The device will perform a reset after sending the INI file

2. To save the *ini* file to a PC, perform the following:
   a. Click the **Save INI File** button; the 'File Download' dialog box opens.
   b. Click the **Save** button, navigate to the folder in which you want to save the *ini* file on your PC, and then click **Save**; the device copies the *ini* file to the selected folder.
3. To load an *ini* file to the device, perform the following:
   a. Click the **Browse** button, navigate to the folder in which the *ini* file is located, select the file, and then click **Open**; the name and path of the file appear in the field beside the **Browse** button.
   b. Click the **Load INI File** button, and then at the prompt, click **OK;** the device uploads the *ini* file and then resets (from the *cmp* version stored on the flash memory). Once complete, the 'Enter Network Password' dialog box appears, requesting you to enter your user name and password.

3.6 Status & Diagnostics Tab

The **Status & Diagnostics** tab on the Navigation bar displays all menus related to the operating status of the device and device diagnostics. These menus appear in the Navigation tree and include the following:

- Status & Diagnostics (refer to "Status & Diagnostics" on page 242)
- Gateway Statistics (refer to "Gateway Statistics" on page 248)

3.6.1 Status & Diagnostics

The **Status & Diagnostics** menu is used to view and monitor the device's channels, Syslog messages, hardware and software product information, and to assess the device's statistics and IP connectivity information. This menu includes the following page items:

- Message Log (refer to "Viewing the Device's Syslog Messages" on page 242)
- Ethernet Port Information (refer to "Viewing Ethernet Port Information" on page 243)
- Active IP Interfaces (refer to "Viewing Active IP Interfaces" on page 244)
- Device Information (refer to "Viewing Device Information" on page 244)
- Performance Statistics (refer to "Viewing Performance Statistics" on page 245)
- Active Alarms (refer to "Viewing Active Alarms" on page 245)
- Trunks & Channels Status (refer to “Viewing Trunks & Channels Status” on page 246)

3.6.1.1 Viewing the Device's Syslog Messages

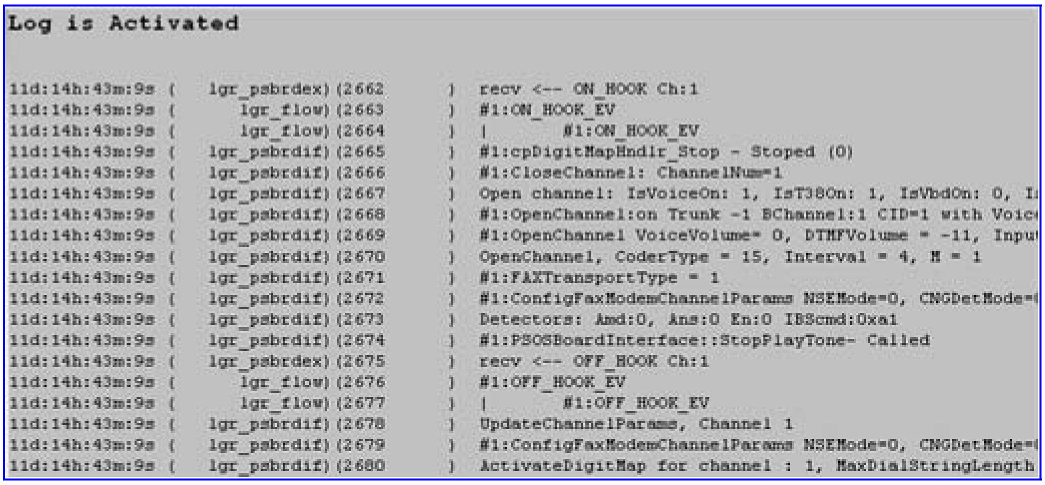
The 'Message Log' page displays Syslog debug messages sent by the device. You can select the Syslog messages in this page, and then copy and paste them into a text editor such as Notepad. This text file (*txt*) can then be sent to AudioCodes Technical Support for diagnosis and troubleshooting.

Note: It's not recommended to keep a Message Log session open for a prolonged period. This may cause the device to overload. For prolonged (and detailed) debugging, use an external Syslog server (refer to the *Product Reference Manual*).

➢ To activate the Message Log, take these 3 steps:

1. In the 'Advanced Parameters' page (refer "Advanced Parameter" on page 151), set the parameter 'Debug Level' (or *ini* file parameter GwDebugLevel) to 6. This parameter determines the Syslog logging level in the range 0 to 6, where 6 is the highest level.
2. Open the 'Message Log' page (**Status & Diagnostics** tab > **Status & Diagnostics** menu > **Message Log** page item); the 'Message Log' page is displayed and the log is activated.

Figure 3-109: Message Log Screen



```
Log is Activated


11d:14h:43m:9s (   lgr_psbrdex)(2662      )  recv <-- ON_HOOK Ch:1
11d:14h:43m:9s (      lgr_flow)(2663      )  #1:ON_HOOK_EV
11d:14h:43m:9s (      lgr_flow)(2664      )  |       #1:ON_HOOK_EV
11d:14h:43m:9s (   lgr_psbrdif)(2665      )  #1:cpDigitMapHndlr_Stop - Stoped (0)
11d:14h:43m:9s (   lgr_psbrdif)(2666      )  #1:CloseChannel: ChannelNum=1
11d:14h:43m:9s (   lgr_psbrdif)(2667      )  Open channel: IsVoiceOn: 1, IsT38On: 1, IsVbdOn: 0, I
11d:14h:43m:9s (   lgr_psbrdif)(2668      )  #1:OpenChannel:on Trunk -1 BChannel:1 CID=1 with Voic
11d:14h:43m:9s (   lgr_psbrdif)(2669      )  #1:OpenChannel VoiceVolume= 0, DTMFVolume = -11, Inpu
11d:14h:43m:9s (   lgr_psbrdif)(2670      )  OpenChannel, CoderType = 15, Interval = 4, M = 1
11d:14h:43m:9s (   lgr_psbrdif)(2671      )  #1:FAXTransportType = 1
11d:14h:43m:9s (   lgr_psbrdif)(2672      )  #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=
11d:14h:43m:9s (   lgr_psbrdif)(2673      )  Detectors: Amd:0, Ans:0 En:0 IBScmd:0xa1
11d:14h:43m:9s (   lgr_psbrdif)(2674      )  #1:PSOSBoardInterface::StopPlayTone- Called
11d:14h:43m:9s (   lgr_psbrdex)(2675      )  recv <-- OFF_HOOK Ch:1
11d:14h:43m:9s (      lgr_flow)(2676      )  #1:OFF_HOOK_EV
11d:14h:43m:9s (      lgr_flow)(2677      )  |       #1:OFF_HOOK_EV
11d:14h:43m:9s (   lgr_psbrdif)(2678      )  UpdateChannelParams, Channel 1
11d:14h:43m:9s (   lgr_psbrdif)(2679      )  #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=
11d:14h:43m:9s (   lgr_psbrdif)(2680      )  ActivateDigitMap for channel : 1, MaxDialStringLength
```

The displayed logged messages are color coded as follows:

- Yellow - fatal error message
- Blue - recoverable error message (i.e., non-fatal error)
- Black - notice message

3. To clear the page of Syslog messages, in the Navigation tree, click the page item **Message Log** again; the page is cleared and new messages begin appearing.

➢ To stop the Message Log, take this step:

- Close the page by accessing any another page in the Web interface.

3.6.1.2 Viewing the Ethernet Port Information

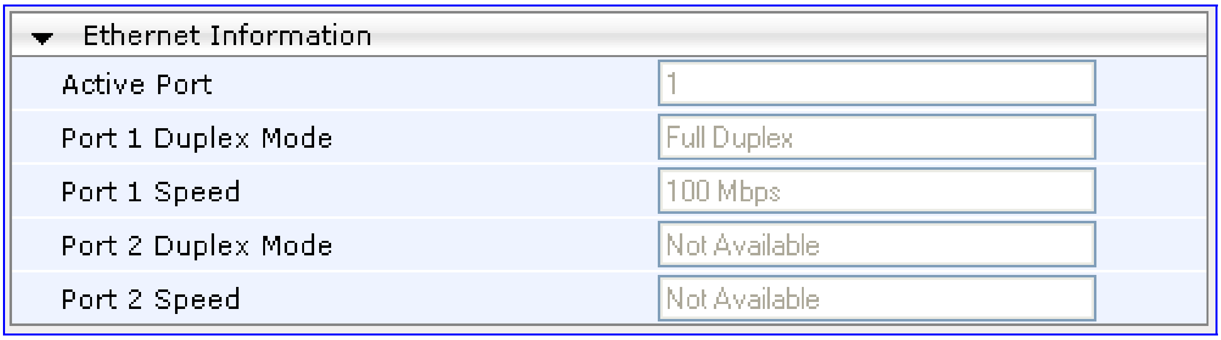
The 'Ethernet Port Information' page displays read-only information on the Ethernet connection used by the device. This includes indicating the active port, duplex mode, and speed. You can also access this page from the 'Home' page (refer to "Using the Home Page" on page 46).

For detailed information on the Ethernet redundancy scheme, refer to "Ethernet Interface Redundancy" on page 380. For detailed information on the Ethernet interface configuration, refer to "Ethernet Interface Configuration" on page 379.

➢ To view Ethernet port information, take the following step:

- Open the ‘Ethernet Port Information’ page (**Status & Diagnostics** tab > **Status & Diagnostics** menu > **Ethernet Port Information** page item).

Figure 3-110: Ethernet Port Information Page



Ethernet Information

Active Port	1
Port 1 Duplex Mode	Full Duplex
Port 1 Speed	100 Mbps
Port 2 Duplex Mode	Not Available
Port 2 Speed	Not Available

Table 3-62: Ethernet Port Information Parameters

Parameter	Description
Active Port	Displays the active Ethernet port (1 or 2).
Port Duplex Mode	Displays the Duplex mode of the Ethernet port (Half Duplex or Full Duplex).
Port Speed	Displays the speed (in Mbps) of the Ethernet port (10 Mbps; 100 Mbps).

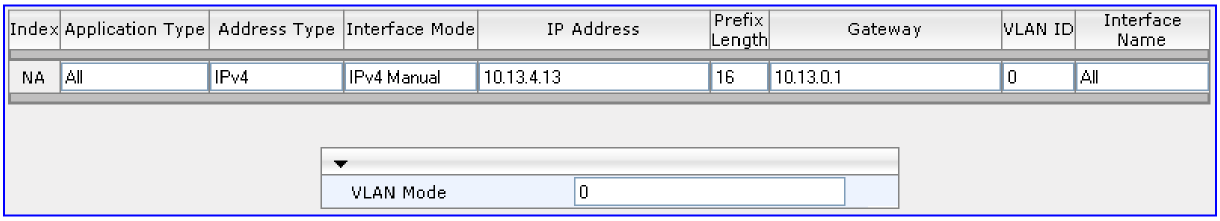
3.6.1.3 Viewing Active IP Interfaces

The 'Active IP Interfaces' page displays the device's IP interfaces, which you configured in the 'Multiple Interface Table' page (refer to "Configuring the Multiple Interface Table" on page 53) and that are currently active.

➢ To view the 'Active IP Interfaces' page, take this step:

- Open the 'Active IP Interfaces' page (**Status & Diagnostics** tab > **Status & Diagnostics** menu > **Active IP Interfaces** page item).

Figure 3-111: Active IP Interfaces Page



Index	Application Type	Address Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
NA	All	IPv4	IPv4 Manual	10.13.4.13	16	10.13.0.1	0	All

VLAN Mode	0

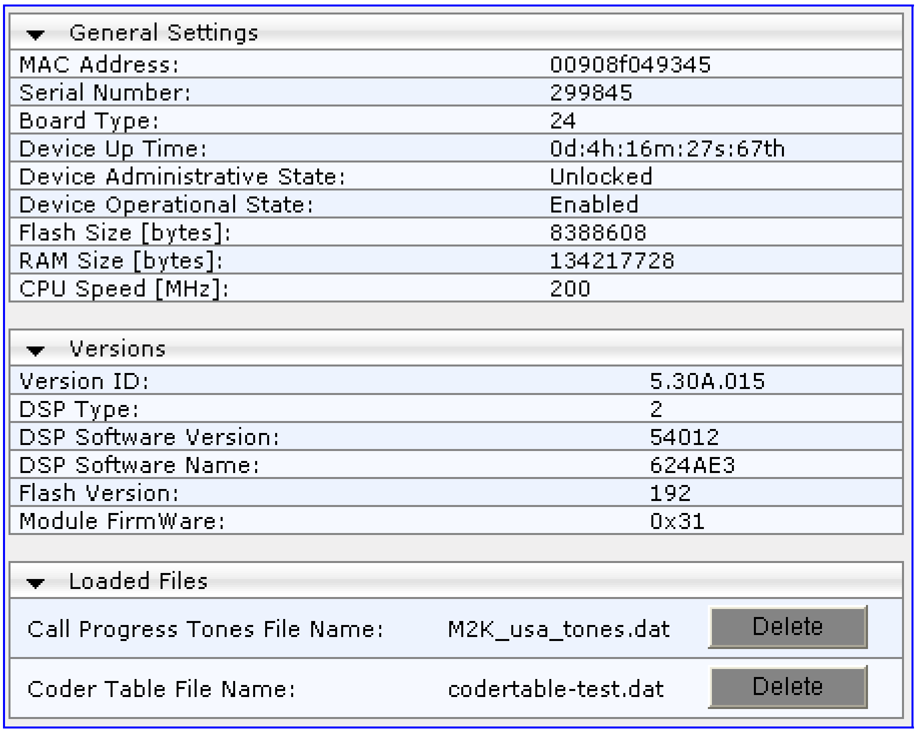
3.6.1.4 Viewing Device Information

The 'Device Information' page displays the device's specific hardware and software product information. This information can help you to expedite troubleshooting. Capture the page and e-mail it to AudioCodes Technical Support personnel to ensure quick diagnosis and effective corrective action. This page also displays any loaded files used by the device (stored in the RAM) and allows you to remove them.

➢ To access the 'Device Information' page, take this step:

- Open the 'Device Information' page (**Status & Diagnostics** tab > **Status & Diagnostics** menu > **Device Information** page item).

Figure 3-112: Device Information Page



General Settings

MAC Address:	00908f049345
Serial Number:	299845
Board Type:	24
Device Up Time:	0d:4h:16m:27s:67th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [bytes]:	8388608
RAM Size [bytes]:	134217728
CPU Speed [MHz]:	200

Versions

Version ID:	5.30A.015
DSP Type:	2
DSP Software Version:	54012
DSP Software Name:	624AE3
Flash Version:	192
Module FirmWare:	0x31

Loaded Files

Call Progress Tones File Name:	M2K_usa_tones.dat	Delete
Coder Table File Name:	codertable-test.dat	Delete

The 'Board Type' field number depicts the following devices:

- Mediant 2000 = 31
- TP-1610 = 24

➢ To delete any of the loaded files, take this step:

- Click the **Delete** button corresponding to the files that you want to delete. Deleting a file takes effect only after the device is reset (refer to "Resetting the Device" on page 228).

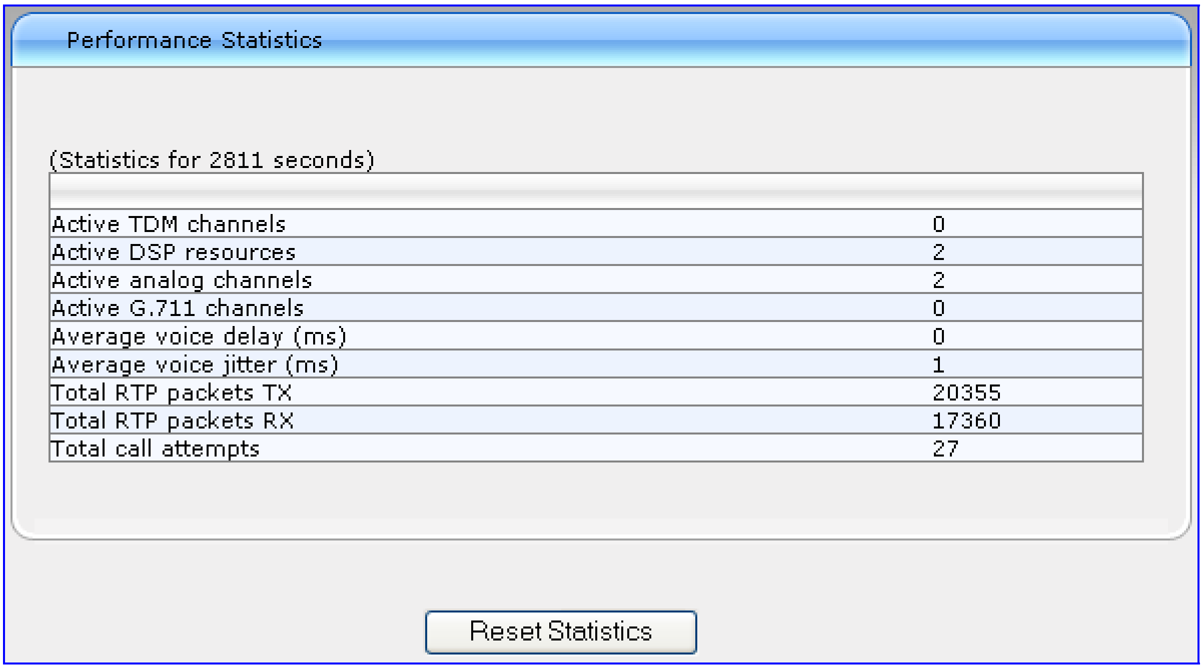
3.6.1.5 Viewing Performance Statistics

The 'Performance Statistics' page provides read-only, device performance statistics. This page is refreshed with new statistics every 60 seconds. The duration that the current statistics has been collected, is displayed above the statistics table.

➢ To view performance statistics, take the following step:

- Open the 'Performance Statistics' page (**Status & Diagnostics** tab > **Status & Diagnostics** menu > **Performance Statistics** page item)**.**

Figure 3-113: Performance Statistics Page



Performance Statistics

(Statistics for 2811 seconds)

Active TDM channels	0
Active DSP resources	2
Active analog channels	2
Active G.711 channels	0
Average voice delay (ms)	0
Average voice jitter (ms)	1
Total RTP packets TX	20355
Total RTP packets RX	17360
Total call attempts	27

➢ To reset the performance statistics to zero, take the following step:

- Click the **Reset Statistics** button.

3.6.1.6 Viewing Active Alarms

The 'Active Alarms' page displays a list of currently active alarms. For each alarm, the following information is provided:

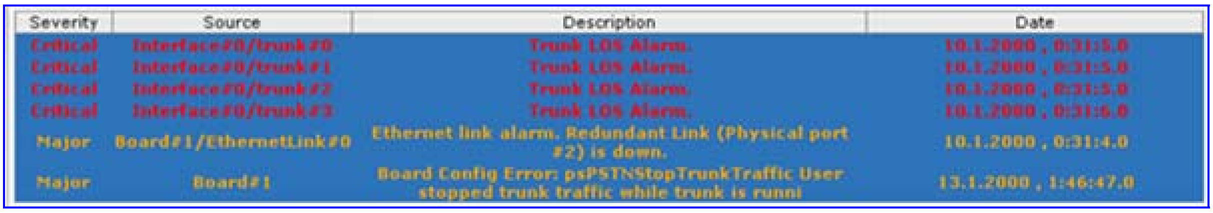
- **Severity:** severity level of the alarm:
  - Critical - alarm displayed in red
  - Major - alarm displayed in orange
  - Minor - alarm displayed in yellow
- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

You can also access this page from the 'Home' page (refer to "Using the Home Page" on page 46).

➢ To view the list of alarms, take this step:

- Open the 'Active Alarms' page (**Status & Diagnostics** tab > **Status & Diagnostics** menu > **Active Alarms** page item)**.**

Figure 3-114: Active Alarms Page



Severity	Source	Description	Date
Critical	Interface#0/trunk#0	Trunk LOS Alarm.	10.1.2000 , 0:31:5.0
Critical	Interface#0/trunk#1	Trunk LOS Alarm.	10.1.2000 , 0:31:5.0
Critical	Interface#0/trunk#2	Trunk LOS Alarm.	10.1.2000 , 0:31:5.0
Critical	Interface#0/trunk#3	Trunk LOS Alarm.	10.1.2000 , 0:31:6.0
Major	Board#1/EthernetLink#0	Ethernet link alarm. Redundant Link (Physical port #2) is down.	10.1.2000 , 0:31:4.0
Major	Board#1	Board Config Error: psPSTNStopTrunkTraffic User stopped trunk traffic while trunk is runni	13.1.2000 , 1:46:47.0

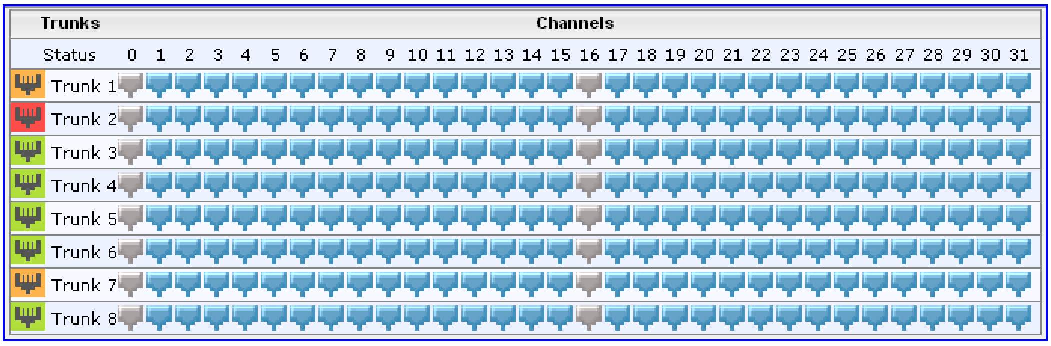
3.6.1.7 Viewing Trunks & Channels Status

The 'Trunks & Channels Status' page displays the status of the device's Trunks and the channels pertaining to these trunks.

➢ To view the status of the device's trunks and the trunks' channels, take the following step:

- Open the 'Trunks & Channels Status' page (**Status & Diagnostics** tab > **Status & Diagnostics** menu > **Trunks & Channels Status** page item).

Figure 3-115: Trunks & Channels Status Page



Trunks	Channels																															
Status	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
🟧 Trunk 1	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟥 Trunk 2	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩 Trunk 3	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩 Trunk 4	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩 Trunk 5	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩 Trunk 6	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟧 Trunk 7	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩 Trunk 8	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	⬜	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

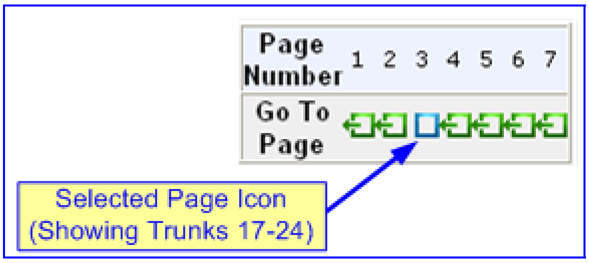
Note: The number of trunks and channels displayed on the page depends on the system configuration.

The page initially displays the first eight trunks and their channels. The page displays eight consecutive trunks at a time. You can view the next eight trunks, by performing the procedure below.

➢ To view the next eight trunks, take this step:

- Click the **Go To Page** ⇦ icon.

Figure 3-116: Example of a Selected Page Icon for Displaying Trunks 17-24



The 'Trunks and Channels Status' page uses the following color-coding icons to indicate the status of the trunks and channels:

Table 3-63: Color-Coding Icons for Trunk and Channel Status

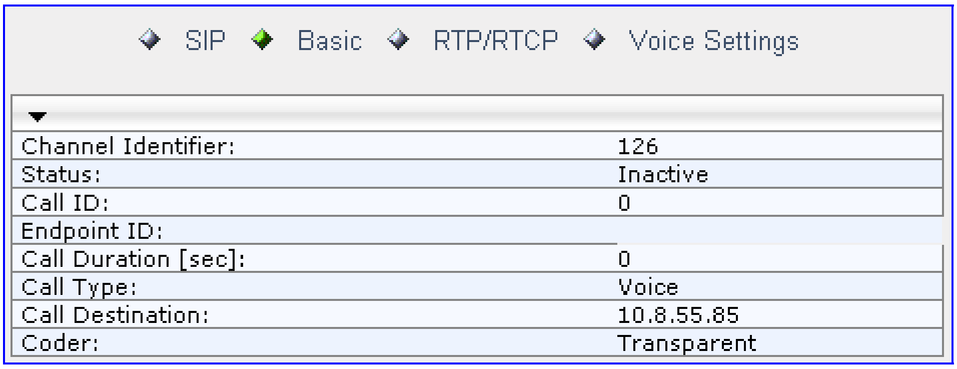
		Trunk	Channel		
Icon	**Color**	**Description**	**Icon**	**Color**	**Description**
⬜	Gray	Disabled	🟦	Light Blue	Inactive
🟩	Green	Active - OK	🟩	Green	Active
🟨	Yellow	RAI Alarm	🟪	Purple	SS7
🟥	Red	LOS/LOF Alarm	⬜	Gray	Non Voice
🟦	Blue	AIS Alarm	🟦	Blue	ISDN Signaling
🟧	Orange	D-Channel Alarm	🟨	Yellow	CAS Blocked

The 'Trunks & Channels Status' page also allows you to view detailed information regarding a selected trunk channel, as described in the procedure below.

➢ To view detailed channel information of a trunk's channel, take these 2 steps:

1. Click a required channel pertaining to a trunk for which you want to view information; the 'Basic Channel Information' page appears, displaying basic information about the channel:

Figure 3-117: Basic Channel Information Page



Channel Identifier:	126
Status:	Inactive
Call ID:	0
Endpoint ID:	
Call Duration [sec]:	0
Call Type:	Voice
Call Destination:	10.8.55.85
Coder:	Transparent

2. To view additional channel information, click the buttons (**SIP**, **Basic**, **RTP/RTCP**, and **Voice Settings**) located above on the page.

3.6.2 Gateway Statistics

The 'Gateway Statistics' page allows you to monitor real-time activity such as IP connectivity information, call details and call statistics, including the number of call attempts, failed calls, fax calls, etc. This menu includes the following page items:

- IP to Tel Calls Count and Tel to IP Calls Count (refer to "Call Counters" on page 248)
- Call Routing Status (refer to "Call Routing Status" on page 250)
- SAS/SBC Registered Users (refer to “SAS/SBC Registered Users” on page 251)
- IP Connectivity (refer to "IP Connectivity" on page 252)

Note: The 'Gateway Statistics' pages don't refresh automatically. To view updated information, re-access the required page.

3.6.2.1 Call Counters

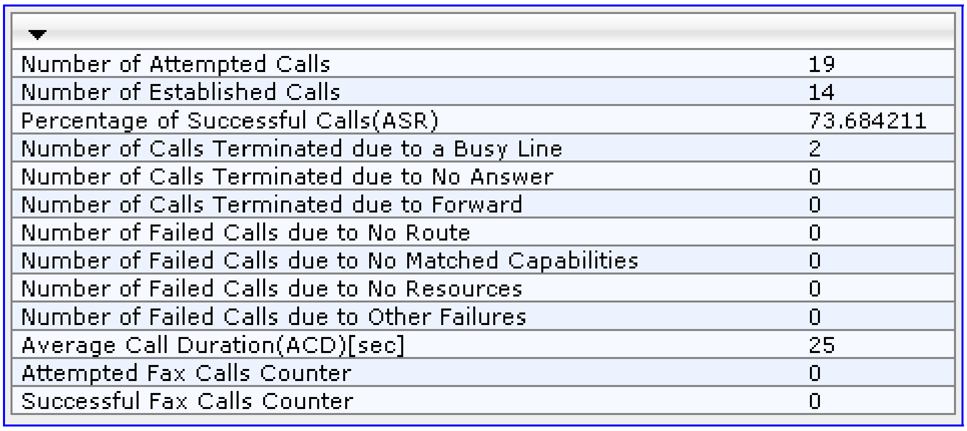
The 'IP to Tel Calls Count' and 'Tel to IP Calls Count' pages provide you with statistical information on incoming (IP-to-Tel) and outgoing (Tel-to-IP) calls. The statistical information is updated according to the release reason that is received after a call is terminated (during the same time as the end-of-call Call Detail Record or CDR message is sent). The release reason can be viewed in the 'Termination Reason' field in the CDR message.

You can reset the statistical data displayed on the page (i.e., refresh the display), by clicking the **Reset Counters** button located on the page.

➢ To view the IP-to-Tel and Tel-to-IP Call Counters pages, take this step:

- Open the Call Counters page that you want to view (**Status & Diagnostics** tab > **Gateway Statistics** menu > **IP to Tel Calls Count** or **Tel to IP Calls Count** page item); the figure below shows the 'IP to Tel Calls Count' page.

Figure 3-118: Calls Count Page



Number of Attempted Calls	19
Number of Established Calls	14
Percentage of Successful Calls(ASR)	73.684211
Number of Calls Terminated due to a Busy Line	2
Number of Calls Terminated due to No Answer	0
Number of Calls Terminated due to Forward	0
Number of Failed Calls due to No Route	0
Number of Failed Calls due to No Matched Capabilities	0
Number of Failed Calls due to No Resources	0
Number of Failed Calls due to Other Failures	0
Average Call Duration(ACD)[sec]	25
Attempted Fax Calls Counter	0
Successful Fax Calls Counter	0

Table 3-64: Call Counters Description

Counter	Description
Number of Attempted Calls	Indicates the number of attempted calls. It is composed of established and failed calls. The number of established calls is represented by the 'Number of Established Calls' counter. The number of failed calls is represented by the failed-call counters. Only one of the established / failed call counters is incremented every time.
Number of Established Calls	Indicates the number of established calls. It is incremented as a result of one of the following release reasons if the duration of the call is greater than zero: ▪ GWAPP_REASON_NOT_RELEVANT (0) ▪ GWAPP_NORMAL_CALL_CLEAR (16) ▪ GWAPP_NORMAL_UNSPECIFIED (31) And the internal reasons: ▪ RELEASE_BECAUSE_UNKNOWN_REASON ▪ RELEASE_BECAUSE_REMOTE_CANCEL_CALL ▪ RELEASE_BECAUSE_MANUAL_DISC ▪ RELEASE_BECAUSE_SILENCE_DISC ▪ RELEASE_BECAUSE_DISCONNECT_CODE **Note:** When the duration of the call is zero, the release reason GWAPP_NORMAL_CALL_CLEAR increments the 'Number of Failed Calls due to No Answer' counter. The rest of the release reasons increment the 'Number of Failed Calls due to Other Failures' counter.
Percentage of Successful Calls (ASR)	The percentage of established calls from attempted calls.

Counter	Description
Number of Calls Terminated due to a Busy Line	Indicates the number of calls that failed as a result of a busy line. It is incremented as a result of the following release reason: GWAPP_USER_BUSY (17)
Number of Calls Terminated due to No Answer	Indicates the number of calls that weren't answered. It's incremented as a result of one of the following release reasons: ▪ GWAPP_NO_USER_RESPONDING (18) ▪ GWAPP_NO_ANSWER_FROM_USER_ALERTED (19) ▪ GWAPP_NORMAL_CALL_CLEAR (16) (when the call duration is zero)
Number of Calls Terminated due to Forward	Indicates the number of calls that were terminated due to a call forward. The counter is incremented as a result of the following release reason: RELEASE_BECAUSE_FORWARD
Number of Failed Calls due to No Route	Indicates the number of calls whose destinations weren't found. It is incremented as a result of one of the following release reasons: ▪ GWAPP_UNASSIGNED_NUMBER (1) ▪ GWAPP_NO_ROUTE_TO_DESTINATION (3)
Number of Failed Calls due to No Matched Capabilities	Indicates the number of calls that failed due to mismatched device capabilities. It is incremented as a result of an internal identification of capability mismatch. This mismatch is reflected to CDR via the value of the parameter DefaultReleaseReason (default is GWAPP_NO_ROUTE_TO_DESTINATION (3)) or by the GWAPP_SERVICE_NOT_IMPLEMENTED_UNSPECIFIED (79) reason.
Number of Failed Calls due to No Resources	Indicates the number of calls that failed due to unavailable resources or a device lock. The counter is incremented as a result of one of the following release reasons: ▪ GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED ▪ RELEASE_BECAUSE_GW_LOCKED
Number of Failed Calls due to Other Failures	This counter is incremented as a result of calls that failed due to reasons not covered by the other counters.
Average Call Duration (ACD) [sec]	The average call duration (ACD) in seconds of established calls. The ACD value is refreshed every 15 minutes and therefore, this value reflects the average duration of all established calls made within a 15 minute period.
Attempted Fax Calls Counter	Indicates the number of attempted fax calls.
Successful Fax Calls Counter	Indicates the number of successful fax calls.

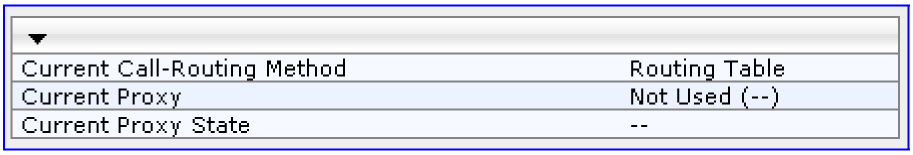
3.6.2.2 Call Routing Status

The 'Call Routing Status' page provides you with information on the current routing method used by the device. This information includes the IP address and FQDN (if used) of the Proxy server with which the device currently operates.

➢ To view the call routing status, take this step:

- Open the 'Call Routing Status' page (**Status & Diagnostics** tab > **Gateway Statistics** menu > **Calls Routing Status** page item).

Figure 3-119: Call Routing Status Page



Current Call-Routing Method	Routing Table
Current Proxy	Not Used (--)
Current Proxy State	--

Table 3-65: Call Routing Status Parameters

Parameter	Description
Current Call-Routing Method	▪ Proxy = Proxy server is used to route calls. ▪ Routing Table preferred to Proxy = The 'Tel to IP Routing' table (or 'Outbound IP Routing Table' if EnableSBC is set to 1) takes precedence over a Proxy for routing calls ('Prefer Routing Table' parameter is set to 'Yes' as described in "Proxy & Registration Parameters" on page 132).
Current Proxy	▪ Not Used = Proxy server isn't defined. ▪ IP address and FQDN (if exists) of the Proxy server with which the device currently operates.
Current Proxy State	▪ N/A = Proxy server isn't defined. ▪ OK = Communication with the Proxy server is in order. ▪ Fail = No response from any of the defined Proxies.

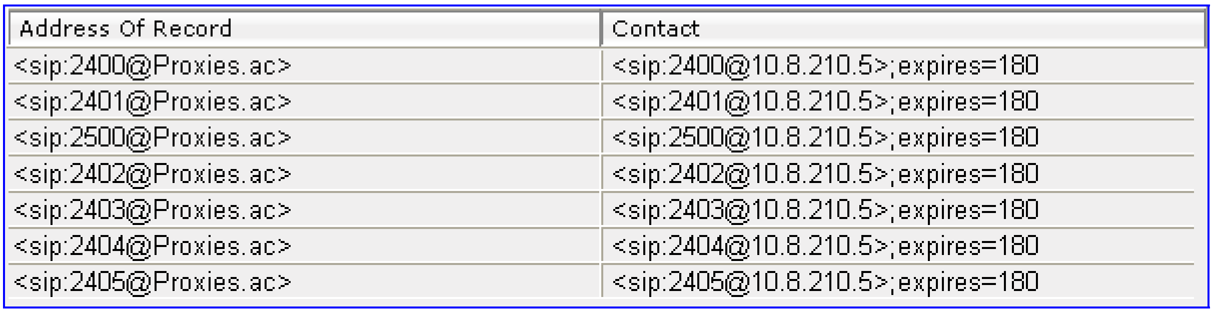
3.6.2.3 SAS/SBC Registered Users

The 'SAS Registered Users' page displays a list of up to 250 Stand Alone Survivability (SAS) and/or IP-to-IP registered users. The SAS feature is configured in the 'SAS Configuration' page (refer to "Stand-Alone Survivability" on page 161). The IP-to-IP feature is configured (enabled) in the 'SBC Configuration' page (refer to “SBC Configuration” on page 163).

➢ To view the SAS registered users, take this step:

- Open the 'SAS Registered Users' page (**Status & Diagnostics** tab > **Gateway Statistics** menu > **SAS/SBC Registered Users** page item).

Figure 3-120: SAS Registered Users Page



Address Of Record	Contact
<sip:2400@Proxies.ac>	<sip:2400@10.8.210.5>;expires=180
<sip:2401@Proxies.ac>	<sip:2401@10.8.210.5>;expires=180
<sip:2500@Proxies.ac>	<sip:2500@10.8.210.5>;expires=180
<sip:2402@Proxies.ac>	<sip:2402@10.8.210.5>;expires=180
<sip:2403@Proxies.ac>	<sip:2403@10.8.210.5>;expires=180
<sip:2404@Proxies.ac>	<sip:2404@10.8.210.5>;expires=180
<sip:2405@Proxies.ac>	<sip:2405@10.8.210.5>;expires=180

Table 3-66: SAS Registered Users Parameters

Column Name	Description
Address of Record	An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI (Contact) where the user might be available.
Contact	SIP URI that can be used to contact that specific instance of the User Agent for subsequent requests.

3.6.2.4 IP Connectivity

The 'IP Connectivity' page displays online, read-only network diagnostic connectivity information on all destination IP addresses configured in the 'Tel to IP Routing' page (refer to "Tel to IP Routing Table" on page 175) or 'Outbound IP Routing Table' page if EnableSBC is set to 1 (refer to “Outbound IP Routing Table” on page 178).

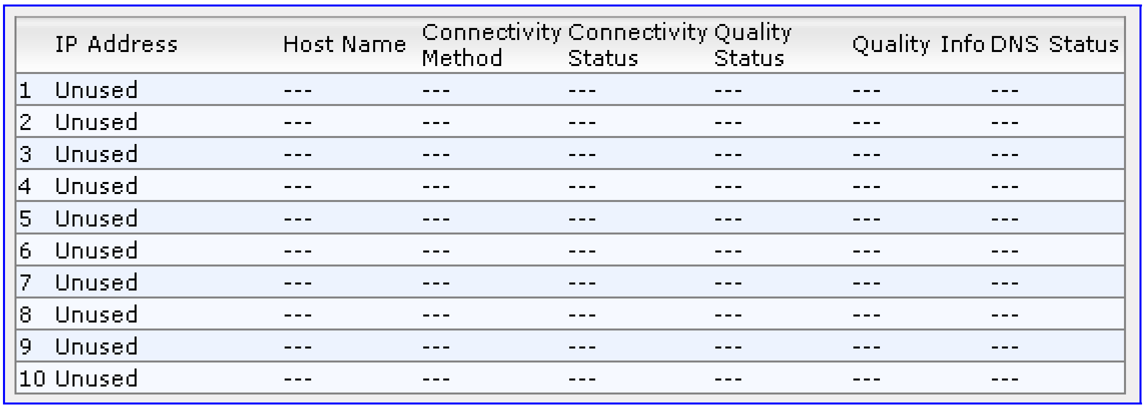
Notes:

- This information is available only if the parameter 'Enable Alt Routing Tel to IP' (refer to "Routing General Parameters" on page 171) is set to 1 (Enable) or 2 (Status Only).
- The information in columns 'Quality Status' and 'Quality Info' (per IP address) is reset if two minutes elapse without a call to that destination.

➢ To view the IP connectivity information, take these 2 steps:

1. In the 'Routing General Parameters' page, set the parameter 'Enable Alt Routing Tel to IP' (or *ini* file parameter AltRoutingTel2IPEnable) to Enable **[1]** or Status Only **[2]**.
2. Open the 'IP Connectivity' page (**Status & Diagnostics** tab > **Gateway Statistics** menu > **IP Connectivity** page item).

Figure 3-121: IP Connectivity Page



	IP Address	Host Name	Connectivity Method	Connectivity Status	Quality Status	Quality Info	DNS Status
1	Unused	---	---	---	---	---	---
2	Unused	---	---	---	---	---	---
3	Unused	---	---	---	---	---	---
4	Unused	---	---	---	---	---	---
5	Unused	---	---	---	---	---	---
6	Unused	---	---	---	---	---	---
7	Unused	---	---	---	---	---	---
8	Unused	---	---	---	---	---	---
9	Unused	---	---	---	---	---	---
10	Unused	---	---	---	---	---	---

Table 3-67: IP Connectivity Parameters

Column Name	Description
IP Address	The IP address can be one of the following: ▪ IP address defined as the destination IP address in the 'Tel to IP Routing' table (or 'Outbound IP Routing Table' page). ▪ IP address resolved from the host name defined as the destination IP address in the 'Tel to IP Routing' table (or 'Outbound IP Routing Table' page).
Host Name	Host name (or IP address) as defined in the 'Tel to IP Routing' table (or 'Outbound IP Routing Table' page).
Connectivity Method	The method according to which the destination IP address is queried periodically (ICMP ping or SIP OPTIONS request).
Connectivity Status	The status of the IP address' connectivity according to the method in the 'Connectivity Method' field. ▪ OK = Remote side responds to periodic connectivity queries. ▪ Lost = Remote side didn't respond for a short period. ▪ Fail = Remote side doesn't respond. ▪ Init = Connectivity queries not started (e.g., IP address not resolved). ▪ Disable = The connectivity option is disabled, i.e., parameter 'Alt Routing Tel to IP Mode' (AltRoutingTel2IPMode *ini*) is set to 'None' or 'QoS' (refer to "Routing General Parameters" on page 171).
Quality Status	Determines the QoS (according to packet loss and delay) of the IP address. ▪ Unknown = Recent quality information isn't available. ▪ OK ▪ Poor **Notes:** ▪ This parameter is applicable only if the parameter 'Alt Routing Tel to IP Mode' is set to 'QoS' or 'Both' (AltRoutingTel2IPMode = 2 or 3). ▪ This parameter is reset if no QoS information is received for 2 minutes.
Quality Info.	Displays QoS information: delay and packet loss, calculated according to previous calls. **Notes:** ▪ This parameter is applicable only if the parameter 'Alt Routing Tel to IP Mode' is set to 'QoS' or 'Both' (AltRoutingTel2IPMode = 2 or 3). ▪ This parameter is reset if no QoS information is received for 2 minutes.
DNS Status	DNS status can be one of the following: ▪ DNS Disable ▪ DNS Resolved ▪ DNS Unresolved

Reader’s Notes

4 ini File Configuration

As an alternative to configuring the device using the Web interface (as described in "Web-Based Management" on page 19), you can configure the device by loading an *ini* file containing user-defined parameters. The *ini* file can be loaded using the following methods:

- AudioCodes' BootP/TFTP utility (refer to the *Product Reference Manual*)
- Any standard TFTP server
- Web interface (refer to "Backing Up and Restoring Configuration" on page 240)

The *ini* file configuration parameters are saved in the device's non-volatile memory after the file is loaded to the device. When a parameter is absent from the *ini* file, the default value is assigned to that parameter (according to the *cmp* file loaded to the device) and stored in the non-volatile memory (thereby, overriding the value previously defined for that parameter).

Some of the device's parameters are configurable only through the *ini* file (and not the Web interface). These parameters usually determine a low-level functionality and are seldom changed for a specific application.

Notes:

- For a list of the *ini* file parameters, refer to "The ini File Parameter Reference" on page 260. The *ini* file parameters that are configurable in the Web interface are described in "Web-Based Management" on page 19. The *ini* parameters that can't be configured using the Web interface are described in this section.
- To define or restore default settings using the *ini* file, refer to "Default Settings" on page 333.

4.1 Secured Encoded ini File

The *ini* file contains sensitive information that is required for the functioning of the device. Typically, it is loaded to or retrieved from the device using TFTP or HTTP. These protocols are not secure and vulnerable to potential hackers.

To overcome this security threat, the AudioCodes' TrunkPack Downloadable Conversion Utility (DConvert) allows you to binary-encode the *ini* file before loading it to the device (refer to the *Product Reference Manual)*. If you retrieve an *ini* file from the device using the Web interface (refer to Backing Up and Restoring Configuration) that was initially loaded as encoded to the device, the file is retrieved as encoded and vice versa.

Note: The procedure for loading an encoded *ini* file is identical to the procedure for loading an unencoded *ini* file.

4.2 The ini File Structure

The *ini* file can contain any number of parameters. The *ini* file can contain the following types of parameters:

- Individual parameters, which are conveniently grouped (optional) by their functionality (refer to "Structure of Individual ini File Parameters" on page 256)
- Table parameters, which include multiple individual parameters (refer to "Structure of ini File Table Parameters" on page 257)

4.2.1 Structure Rules

The *ini* file must adhere to the following format rules:

- The *ini* file name must not include hyphens (-) or spaces; if necessary, use an underscore (_) instead.
- Lines beginning with a semi-colon (;) are ignored. These can be used for adding remarks in the *ini* file.
- A carriage return (i.e., Enter) must be done at the end of each line.
- The number of spaces before and after the equals sign (=) is irrelevant.
- Subsection names for grouping parameters are optional.
- If there is a syntax error in the parameter name, the value is ignored.
- Syntax errors in the parameter's value can cause unexpected errors (parameters may be set to the incorrect values).
- Parameter string values that denote file names (e.g., CallProgressTonesFileName), must be enclosed with inverted commas ('…'), e.g., CallProgressTonesFileName = 'cpt_usa.dat'
- The parameter name is not case-sensitive.
- The parameter value is not case-sensitive, except for coder names.
- The *ini* file must end with at least one carriage return.

4.2.2 Structure of Individual ini File Parameters

The structure of individual *ini* file parameters in an *ini* file is shown below:

```
[Subsection Name]
Parameter Name = Parameter Value
Parameter Name = Parameter Value
; REMARK
```

An example of an *ini* file containing individual *ini* file parameters is shown below:

```
[SYSTEM Params]
SyslogServerIP = 10.13.2.69
EnableSyslog = 1
; These are a few of the system-related parameters.
[WEB Params]
LogoWidth = '339'
WebLogoText = 'My Device'
UseWeblogo = 1
; These are a few of the Web-related parameters.
[Files]
CallProgressTonesFileName = 'cpusa.dat'
```

4.2.3 Structure of ini File Table Parameters

You can use an*ini* file to configure table parameters, which include several parameters (table *columns*) grouped according to the applications they configure (e.g., NFS and IPSec). When loading an *ini* file to the device, it's recommended to include only tables that belong to applications that are to be configured (dynamic tables of other applications are empty, but static tables are not).

A table is defined as a *secret* table (i.e., concealed) if it contains at least one secret data field or if it depends on another secret table. For example, in the IPSec application, IPSec tables are defined as secret tables as the IKE table contains a pre-shared key that must be concealed. Therefore, the SPD table that depends on the IKE table is defined as a secret table as well. Secret tables are always concealed when loading an *ini* file to the device. However, there is a commented title that states that the secret table exists in the device, but is not to be revealed. Secret tables are always stored in the device's non-volatile memory and can be overwritten by new tables that are provided in a new *ini* file. If a secret table appears in an *ini* file, it replaces the current table regardless of its content. To delete a secret table from the device, include an empty table of the same type (with no data lines) as part of a new *ini* file.

The *ini* file table parameter is composed of the following elements:

- **Title of the table:** The name of the table in square brackets (e.g., [MY_TABLE_NAME]).
- **Format line:** Specifies the columns (parameters) of the table (by their string names) that are to be configured.
    - The first word of the Format line must be 'FORMAT', followed by the Index field name, and then an equal (=) sign. After the equal sign, the names of the parameters (*items*) are listed.
    - Items must be separated by a comma (,).
    - The Format line must only include columns that can be modified (i.e., parameters that are not specified as read-only). An exception is Index fields that are always mandatory.
    - The Format line must end with a semicolon (;).
- **Data line(s):** Contain the actual values of the parameters. The values are interpreted according to the Format line.
    - The first word of the Data line must be the table's string name followed by the Index field.
    - Items must be separated by a comma (,).
    - A Data line must end with a semicolon (;).
- **End-of-Table Mark:** Indicates the end of the table. The same string used for the table's title, preceded by a backslash (\), e.g., [\MY_TABLE_NAME].

The following displays an example of the structure of an *ini* file table parameter.

```
[Table Title]
; This is the title of the table.
FORMAT Item Index = Item Name1, Item Name2, Item Name3;
; This is the Format line.
Item 0 = value1, value2, value3;
Item 1 = value1, $$, value3;
; These are the Data lines.
[\Table Title]
; This is the end-of-the-table-mark.
```

Refer to the following notes:

- Indices (in both the Format and the Data lines) must appear in the same order. The Index field must never be omitted.
- The Format line can include a subset of the configurable fields in a table. In this case, all other fields are assigned with the pre-defined default values for each configured line.
- The order of the fields in the Format line isn't significant (as opposed to the Index fields). The fields in the Data lines are interpreted according to the order specified in the Format line.
- The double dollar sign ($$) in a Data line indicates the default value for the parameter.
- The order of the 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 must be in exactly the same order.
- A line in a table is identified by its table name and Index fields. Each such line may appear only once in the *ini* file.
- Table dependencies: Certain tables may depend on other tables. For example, one table may include a field that specifies an entry in another table. This method is used 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 the order of their dependency (i.e., if Table X is referred to by Table Y, Table X must appear in the *ini* file before Table Y).

The table below displays an example of an *ini* file table parameter:

```
[ PREFIX ]
FORMAT PREFIX Index = PREFIX DestinationPrefix,
PREFIX DestAddress, PREFIX SourcePrefix, PREFIX ProfileId,
PREFIX MeteringCode, PREFIX DestPort;
PREFIX 0 = 10, 10.13.83.5, *, 0, 255, 0;
PREFIX 1 = 20, 10.13.83.7, *, 0, 255, 0;
PREFIX 2 = 30, 10.13.83.6, *, 0, 255, 0;
PREFIX 3 = 20, 10.13.83.2, *, 0, 255, 0;
[ \PREFIX ]
```

Note: Do not include read-only parameters in the *ini* file table parameter, as this can cause an error when trying to load the file to the device.

4.2.4 Example of an ini File

Below is an example of an *ini* file for the VoIP device.

```
;Channel Params
DJBufMinDelay = 75
RTPRedundancyDepth = 1
IsProxyUsed = 1
ProxyIP = 192.168.122.179
[CoderName]
FORMAT CoderName Index = CoderName Type, CoderName PacketInterval,
CoderName rate, CoderName PayloadType, CoderName Sce;
CoderName 1= g7231,90
[\CoderName]
;List of serial B-channel numbers
[TrunkGroup]
FORMAT TrunkGroup Index = TrunkGroup TrunkGroupNum,
TrunkGroup FirstTrunkId,TrunkGroup LastTrunkId,
TrunkGroup FirstBChannel, TrunkGroup LastBChannel,
TrunkGroup FirstPhoneNumber, TrunkGroup ProfileId,
TrunkGroup Module;
TrunkGroup 1 = 0,0,0,1,24,1000;
TrunkGroup 2 = 0,1,1,1,24,2000;
TrunkGroup 3 = 0,2,2,1,24,3000;
TrunkGroup 4 = 0,3,3,1,24,4000;
[\TrunkGroup]
CallProgressTonesFilename = 'CPUSA.dat'
SaveConfiguration = 1
```

4.3 Modifying an ini File

You can modify an *ini* file currently used by a device. Modifying an *ini* file instead of loading an entirely new *ini* file preserves the device's current configuration, including factory default values.

➢ To modify an *ini* file, take these 4 steps:

1. Save the *ini* file from the device to your PC using the Web interface (refer to "Backing Up and Restoring Configuration" on page 240).
2. Open the *ini* file (using a text file editor such as Microsoft Notepad), and then modify the *ini* file parameters according to your requirements.
3. Save the modified *ini* file, and then close the file.
4. Load the modified *ini* file to the device, using either the BootP/TFTP utility or the Web interface (refer to "Backing Up and Restoring Configuration" on page 240).

Tip: Before loading the *ini* file to the device, verify that the file extension of the *ini* file saved on your PC is correct, i.e., **.ini*.

4.4 Reference for ini File Parameters

This subsection lists all the *ini* file parameters. References to their descriptions in the Web interface are provided except for those *ini* file parameters that can only be configured using the *ini* file.

4.4.1 Networking Parameters

The networking-related *ini* file configuration parameters are described in the table below.

Table 4-1: Networking ini File Parameters

Parameter	Description
EthernetPhyConfiguration	Defines the Ethernet connection mode type. ▪ **[0]** = 10Base-T half-duplex ▪ **[1]** = 10Base-T full-duplex ▪ **[2]** = 100Base-TX half-duplex ▪ **[3]** = 100Base-TX full-duplex ▪ **[4]** = Auto-negotiate (default) For detailed information on Ethernet interface configuration, refer to "Ethernet Interface Configuration" on page 379.
DHCPEnable	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
DHCPSpeedFactor	Determines the DHCP renewal speed. ▪ **[0]** = Disable ▪ **[1]** = Normal (default) ▪ **[2]** to **[10]** = Fast When set to 0, the DHCP lease renewal is disabled. Otherwise, the renewal time is divided by this factor. Some DHCP-enabled routers perform better when set to 4.
EnableDHCPLeaseRenewal	Enables or disables DHCP renewal support. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable This parameter is applicable only if DHCPEnable is set to 0 for cases where booting up the device via DHCP is not desirable, but renewing DHCP leasing is. When the device is powered up, it attempts to communicate with a BootP server. If there is no response and if DHCP is disabled, the device boots from flash. It then attempts to communicate with the DHCP server to renew the lease.
EnableLANWatchDog	For a description of this parameter, refer to "General Parameters" on page 151.
DNSPriServerIP	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
DNSSecServerIP	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.

Parameter	Description
DNS2IP	This *ini* file table parameter configures the internal DNS table for resolving host names into IP addresses. Up to four different IP addresses (in dotted-decimal notation) can be assigned to a host name. The format of this parameter is as follows: [Dns2Ip] FORMAT Dns2Ip_**Index** = Dns2Ip_**DomainName**, Dns2Ip_**FirstIpAddress**, Dns2Ip_**SecondIpAddress**, Dns2Ip_**ThirdIpAddress**, Dns2Ip_**FourthIpAddress**; [\Dns2Ip] For example: [Dns2Ip] Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4; [\Dns2Ip] **Notes:** ▪ This parameter can include up to 20 indices. ▪ If the internal DNS table is used, the device first attempts to resolve a domain name using this table. If the domain name isn't found, the device performs a DNS resolution using an external DNS server. ▪ To configure the internal DNS table using the Web interface and for a description of the parameters in this *ini* file table parameter, refer to "Internal DNS Table" on page 186. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
SRV2IP	This *ini* file table parameter defines the internal SRV table for resolving host names to DNS A-Records. Three different A-Records can be assigned to a host name. Each A-Record contains the host name, priority, weight, and port. The format of this parameter is as follows: [SRV2IP] FORMAT SRV2IP_**Index** = SRV2IP_**InternalDomain**, SRV2IP_**TransportType**, SRV2IP_**Dns1**, SRV2IP_**Priority1**, SRV2IP_**Weight1**, SRV2IP_**Port1**, SRV2IP_**Dns2**, SRV2IP_**Priority2**, SRV2IP_**Weight2**, SRV2IP_**Port2**, SRV2IP_**Dns3**, SRV2IP_**Priority3**, SRV2IP_**Weight3**, SRV2IP_**Port3**; [\SRV2IP] For example: [SRV2IP] SRV2IP 0 = SrvDomain,0,Dnsname1,1,1,500,Dnsname2,2,2,501,$$,0,0,0; [\SRV2IP] **Notes**: ▪ This parameter can include up to 10 indices. ▪ If the Internal SRV table is used, the device first attempts to resolve a domain name using this table. If the domain name isn't located, the device performs an SRV resolution using an external DNS server. ▪ To configure the Internal SRV table using the Web interface and for a description of the parameters in this *ini* file table parameter, refer to "Internal SRV Table" on page 187.

Parameter	Description
	▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
EnableSTUN	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
STUNServerPrimaryIP	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
STUNServerSecondaryIP	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
STUNServerDomainName	Defines the domain name for the Simple Traversal of User Datagram Protocol (STUN) server's address (used for retrieving all STUN servers with an SRV query). The STUN client can perform the required SRV query to resolve this domain name to an IP address and port, sort the server list, and use the servers according to the sorted list. **Note:** Use either the STUNServerPrimaryIP or the STUNServerDomainName parameter, with priority to the first one.
NATBindingDefaultTimeout	Defines the default NAT binding lifetime in seconds. STUN is used to refresh the binding information after this time expires. The valid range is 0 to 2,592,000. The default value is 30.
DisableNAT	Enables / disables the Network Address Translation (NAT) mechanism. ▪ **[0]** = Enabled. ▪ **[1]** = Disabled (default). **Note:** The compare operation that is performed on the IP address is enabled by default and is controlled by the parameter EnableIPAddrTranslation. The compare operation that is performed on the UDP port is disabled by default and is controlled by the parameter EnableUDPPortTranslation.
EnableIPAddrTranslation	Enables IP address translation. ▪ **[0]** = Disable IP address translation. ▪ **[1]** = Enable IP address translation for RTP, RTCP and T.38 packets (default). ▪ [2] = Enable IP address translation for RTP Multiplexing (ThroughPacket™). ▪ [3] = Enable IP address translation for all protocols (RTP, RTCP, T.38 and RTP Multiplexing). When enabled, the device compares the source IP address of the first incoming packet to the remote IP address stated in the opening of the channel. If the two IP addresses don't match, the NAT mechanism is activated. Consequently, the remote IP address of the outgoing stream is replaced by the source IP address of the first incoming packet. **Notes:** ▪ The NAT mechanism must be enabled for this parameter to take effect (DisableNAT set to 0). ▪ For information on RTP Multiplexing, refer to "RTP Multiplexing (ThroughPacket)" on page 360.

Parameter	Description
EnableUDPPortTranslation	▪ **[0]** = Disable UDP port translation (default). ▪ **[1]** = Enable UDP port translation. When enabled, the device compares the source UDP port of the first incoming packet, to the remote UDP port stated in the opening of the channel. If the two UDP ports don't match, the NAT mechanism is activated. Consequently, the remote UDP port of the outgoing stream is replaced by the source UDP port of the first incoming packet. **Note:** The NAT mechanism and the IP address translation must be enabled for this parameter to take effect (DisableNAT = 0, EnableIpAddrTranslation = 1).
NoOpEnable	Enables or disables the transmission of RTP or T.38 No-Op packets. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.
NoOpInterval	Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP / T.38 traffic) when No-Op packet transmission is enabled. The valid range is 20 to 65,000 msec. The default is 10,000. **Note:** To enable No-Op packet transmission, use the NoOpEnable parameter.
RTPNoOpPayloadType	Determines the payload type of No-Op packets. The valid range is 96 to 127 (for the range of Dynamic RTP Payload Type for all types of non hard-coded RTP Payload types, refer to RFC 3551). The default value is 120. **Note:** When defining this parameter, ensure that it doesn't cause collision with other payload types.
EnableDetectRemoteMACChange	Changes the RTP packets according to the MAC address of received RTP packets and according to Gratuitous Address Resolution Protocol (GARP) messages. ▪ **[0]** = nothing is changed. ▪ **[1]** = If the device receives RTP packets with a different source MAC address (than the MAC address of the transmitted RTP packets), then it sends RTP packets to this MAC address and removes this IP entry from the device's ARP cache table. ▪ **[2]** = The device uses the received GARP packets to change the MAC address of the transmitted RTP packets. ▪ **[3]** = both 1 and 2 options above are used (default).
StaticNatIP	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
SyslogServerIP	For a description of this parameter, refer to "Configuring the Management Settings" on page 220.
SyslogServerPort	For a description of this parameter, refer to "Configuring the Management Settings" on page 220.
EnableSyslog	For a description of this parameter, refer to "Configuring the Management Settings" on page 220.

Parameter	Description
SyslogOutputMethod	Determines the method used for Syslog messages. ▪ **[0]** = Send all Syslog messages to the defined Syslog server (default). ▪ **[1]** = Send all Syslog messages using the Debug Recording mechanism. ▪ **[2]** = Send only Error and Warning level Syslog messages using the Debug Recording mechanism. For a detailed description on Debug Recording, refer to Debug Recording (DR).
BaseUDPport	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
RemoteBaseUDPPort	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
L1L1ComplexTxUDPPort	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
L1L1ComplexRxUDPPort	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
NTPServerIP	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
NTPServerUTCOffset	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
NTPUpdateInterval	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.

IP Routing Table parameters:
The IP routing *ini* file parameters are array parameters. Each parameter configures a specific column in the IP routing table. The first entry in each parameter refers to the first row in the IP routing table, the second entry to the second row and so forth.
In the following example, two rows are configured when the device is in network 10.31.x.x:
RoutingTableDestinationsColumn = 130.33.4.6, 83.4.87.6
RoutingTableDestinationMasksColumn = 255.255.255.255, 255.255.255.0
RoutingTableGatewaysColumn = 10.31.0.1, 10.31.0.112
RoutingTableInterfacesColumn = 0, 1
RoutingTableHopsCountColumn = 20, 20	

RoutingTableDestinationsColumn	For a description of this parameter, refer to "Configuring the IP Routing Table" on page 62.
RoutingTableDestinationMasksColumn	For a description of this parameter, refer to "Configuring the IP Routing Table" on page 62.
RoutingTableGatewaysColumn	For a description of this parameter, refer to "Configuring the IP Routing Table" on page 62.
RoutingTableHopsCountColumn	For a description of this parameter, refer to "Configuring the IP Routing Table" on page 62.
RoutingTableInterfacesColumn	For a description of this parameter, refer to "Configuring the IP Routing Table" on page 62.
VLAN Parameters	
VLANMode	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.

Parameter	Description
VLANNativeVLANID	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
VLANOamVLANID	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
VLANControlVLANID	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
VLANMediaVLANID	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
VLANNetworkServiceClassPriority	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
VLANPremiumServiceClassMediaPriority	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
VLANPremiumServiceClassControlPriority	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
VlanGoldServiceClassPriority	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
VLANBronzeServiceClassPriority	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
EnableDNSasOAM	This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for DNS services. VLAN: Determines the traffic type for DNS services. ▪ **[1]** = OAMP (default) ▪ **[0]** = Control.
EnableNTPasOAM	This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for NTP services. VLAN: Determines the traffic type for NTP services. ▪ **[1]** = OAMP (default) ▪ **[0]** = Control.
VLANSendNonTaggedOnNative	Specify whether to send non-tagged packets on the native VLAN. ▪ **[0]** = Sends priority tag packets (default). ▪ **[1]** = Sends regular packets (with no VLAN tag).
Multiple IPs Parameters	
EnableMultipleIPs	For a description of this parameter, refer to "Configuring the IP Settings" on page 50. **Note:** This parameter is not applicable when configuring multiple interfaces using the *ini* file table parameter InterfaceTable.
LocalMediaIPAddress	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
LocalMediaSubnetMask	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
LocalMediaDefaultGW	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.

Parameter	Description
LocalControlIPAddress	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
LocalControlSubnetMask	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
LocalControlDefaultGW	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
LocalOAMIPAddress	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
LocalOAMSubnetMask	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
LocalOAMDefaultGW	For a description of this parameter, refer to "Configuring the IP Settings" on page 50.
Multiple Interface Table	
InterfaceTable	This *ini* file table parameter configures the Multiple Interface table for configuring logical IP addresses. The format of this parameter is as follows: [InterfaceTable] FORMAT InterfaceTable_**Index** = InterfaceTable_**ApplicationTypes**, InterfaceTable_**IPv6InterfaceMode**, InterfaceTable_**IPAddress**, InterfaceTable_**PrefixLength**, InterfaceTable_**Gateway**, InterfaceTable_**VlanID**, InterfaceTable_**InterfaceName**; InterfaceTable 0 = 6, 0, 192.168.85.14, 16, 192.168.0.1, 1, myAll; [\InterfaceTable] For example: [InterfaceTable] FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_IPv6InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName; InterfaceTable 0 = 0, 0, 192.168.85.14, 16, 0.0.0.0, 1, ManagementIF; InterfaceTable 1 = 2, 0, 200.200.85.14, 24, 0.0.0.0, 200, myControlIF; InterfaceTable 2 = 1, 0, 211.211.85.14, 24, 211.211.85.1, 211, myMediaIF; [\InterfaceTable] The above example, configures three network interfaces (OAMP, Control, and Media applications). **Notes:** ▪ To configure the Multiple Interface table using the Web interface, refer to "Configuring the Multiple Interface Table" on page 53. ▪ For a description of configuring *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

Parameter	Description
Differential Services. For detailed information on IP QoS via Differentiated Services, refer to "IP QoS via Differentiated Services (DiffServ)" on page 384.	
NetworkServiceClassDiffServ	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
PremiumServiceClassMediaDiffServ	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
PremiumServiceClassControlDiffServ	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
GoldServiceClassDiffServ	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
BronzeServiceClassDiffServ	For a description of this parameter, refer to "Configuring the QoS Settings" on page 63.
NFS Table Parameter	
NFSServers	This *ini* file table parameter defines Network File Systems (NFS) so that the device can access a remote server's shared files and directories for loading *cmp*, *ini*, and auxiliary files (using the Automatic Update mechanism). The format of this *ini* file table parameter is as follows: [NFSServers] FORMAT NFSServers_**Index** = NFSServers_**HostOrIP**, NFSServers_**RootPath**, NFSServers_**NfsVersion**, NFSServers_**AuthType**, NFSServers_**UID**, NFSServers_**GID**, NFSServers_**VlanType**; [\NFSServers] For example: [NFSServers] FORMAT NFSServers_Index = NFSServers_HostOrIP, NFSServers_RootPath, NFSServers_NfsVersion, NFSServers_AuthType, NFSServers_UID, NFSServers_GID, NFSServers_VlanType; NFSServers 1 = 101.1.13, /audio1, 3, 1, 0, 1, 1; [\NFSServers] **Notes:** ▪ You can configure up to five NFS file systems (0-4). ▪ The combination of Host / IP and Root Path must be unique for each index in the table. For example, the table must include only one index entry with a Host / IP of '192.168.1.1' and Root Path of '/audio'. ▪ This parameter is applicable only if VLANs are enabled or if Multiple IPs is configured. ▪ To configure NFS using the Web interface and for a description of the parameters of this ini file table parameter, refer to "Configuring the NFS Settings" on page 60. ▪ For a description of configuring *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

4.4.2 System Parameters

The system-related *ini* file configuration parameters are described in the table below.

Table 4-2: System ini File Parameters

Parameter	Description
EnableDiagnostics	Checks the correct functionality of the different hardware components on the device. On completion of the check, if the test fails, the device sends information on the test results of each hardware component to the Syslog server. ▪ **[0]** = Rapid and Enhanced self-test mode (default). ▪ **[1]** = Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY and Flash). ▪ **[2]** = A quicker version of the Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY, but partial test of Flash). For detailed information, refer to the *Product Reference Manual*.
GWAppDelayTime	For a description of this parameter, refer to "Advanced Parameters" on page 151.
ActivityListToLog	The Activity Log mechanism enables the device to send log messages (to a Syslog server) that report certain types of Web actions according to a pre-defined filter. The following filters are available: ▪ **[PVC]** (Parameters Value Change) = Changes made on-the-fly to parameters. ▪ **[AFL]** (Auxiliary Files Loading) = Loading of auxiliary files (e.g., via 'Certificate' screen). ▪ **[DR]** (Device Reset) = Reset of device via the 'Maintenance Actions' screen. ▪ **[FB]** (Flash Memory Burning) = Burning of files / parameters to flash (in 'Maintenance Actions' screen). ▪ **[SWU]** (Device Software Update) = cmp loading via the Software Upgrade Wizard. ▪ **[ARD]** (Access to Restricted Domains) = Access to Restricted Domains. The following screens are restricted: (1) ini parameters (AdminPage) (2) 'General Security Settings' (3) 'Configuration File' (4) 'IPSec/IKE' tables (5) 'Software Upgrade Key' (6) 'Internal Firewall' (7) 'Web Access List' (8) 'Web User Accounts' ▪ **[NAA]** (Non Authorized Access) = Attempt to access the Web interface with a false / empty user name or password. ▪ **[SPC]** (Sensitive Parameters Value Change) = Changes made to sensitive parameters: (1) IP Address (2) Subnet Mask (3) Default Gateway IP Address

Parameter	Description
	(4) ActivityListToLog For example: ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'
ECHybridLoss	Sets the four wire to two wire worst-case Hybrid loss, the ratio between the signal level sent to the hybrid and the echo level returning from the hybrid. ▪ **[0]** = 6 dB (default) ▪ **[1]** = N/A ▪ **[2]** = 0 dB ▪ **[3]** = 3 dB
GwDebugLevel	For a description of this parameter, refer to "Advanced Parameters" on page 151.
CDRReportLevel	For a description of this parameter, refer to "Advanced Parameters" on page 151.
CDRSyslogServerIP	For a description of this parameter, refer to "Advanced Parameters" on page 151.
HeartBeatDestIP	Destination IP address (in dotted format notation) to which the device sends proprietary UDP 'ping' packets. The default IP address is 0.0.0.0.
HeartBeatDestPort	Destination UDP port to which the heartbeat packets are sent. The range is 0 to 64000. The default is 0.
HeartBeatIntervalmsec	Delay (in msec) between consecutive heartbeat packets. ▪ **[10]** = 100000. ▪ **[-1]** = disabled (default).
EnableRAI	▪ **[0]** = Disable RAI (Resource Available Indication) service (default). ▪ **[1]** = Enable RAI service. If RAI is enabled, an SNMP 'acBoardCallResourcesAlarm' Alarm Trap is sent if device's busy endpoints exceed a predefined (configurable) threshold.
RAIHighThreshold	High threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints exceeds this High Threshold, the device sends the SNMP acBoardCallResourcesAlarm Alarm Trap with a 'major' Alarm Status. The range is 0 to 100. The default value is 90. **Note:** The percentage of busy endpoints is calculated by dividing the number of busy endpoints by the total number of “enabled” endpoints(trunks are physically connected and synchronized with no alarms and endpoints are defined in the Trunk Group table).
RAILowThreshold	Low threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints falls below this Low Threshold, the device sends an SNMP acBoardCallResourcesAlarm Alarm Trap with a 'cleared' Alarm Status. The range is 0 to 100%. The default value is 90%.

Parameter	Description
RAILoopTime	Time interval (in seconds) that the device periodically checks call resource availability. The valid range is 1 to 200. The default is 10.
Disconnect Supervision Parameters	
TelConnectCode	For a description of this parameter, refer to "Advanced Parameters" on page 151.
DisconnectOnBrokenConnection	For a description of this parameter, refer to "Advanced Parameters" on page 151.
BrokenConnectionEventTimeout	For a description of this parameter, refer to "Advanced Parameters" on page 151.
EnableSilenceDisconnect	For a description of this parameter, refer to "Advanced Parameters" on page 151.
FarEndDisconnectSilencePeriod	For a description of this parameter, refer to "Advanced Parameters" on page 151.
FarEndDisconnectSilenceMethod	For a description of this parameter, refer to "Advanced Parameters" on page 151.
FarEndDisconnectSilenceThreshold	Threshold of the packet count (in percentages) below which is considered silence by the device. The valid range is 1 to 100%. The default is 8%. **Note:** Applicable only if silence is detected according to packet count (FarEndDisconnectSilenceMethod = 1).
Automatic Update Parameters	
CmpFileURL	Specifies the name of the *cmp* file and the location of the server (IP address or FQDN) from which the device loads a new *cmp* file and updates itself. The *cmp* file can be loaded using HTTP, HTTPS, FTP, FTPS, or NFS. For example: http://192.168.0.1/filename **Notes:** ▪ When this parameter is set in the *ini* file, the device always loads the *cmp* file after it is reset. ▪ The *cmp* file is validated before it's burned to flash. The checksum of the *cmp* file is also compared to the previously-burnt checksum to avoid unnecessary resets. ▪ The maximum length of the URL address is 255 characters.
IniFileURL	Specifies the name of the *ini* file and the location of the server (IP address or FQDN) from which the device loads the *ini* file. The *ini* file can be loaded using: HTTP, HTTPS, FTP, FTPS or NFS. For example: http://192.168.0.1/filename http://192.8.77.13/config<MAC> https://<username>:<password>@<IP address>/<file name> **Notes:** ▪ When using HTTP or HTTPS, the date and time of the *ini* file are validated. Only more recently-dated *ini* files are loaded. ▪ The optional string '<MAC>' is replaced with the device's MAC address. Therefore, the device requests an *ini* file name that contains its MAC address. This option enables loading different configurations for specific devices.

Parameter	Description
	▪ The maximum length of the URL address is 99 characters.
PrtFileURL	Specifies the name of the Prerecorded Tones file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. **Note:** The maximum length of the URL address is 99 characters.
CptFileURL	Specifies the name of the CPT file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. **Note:** The maximum length of the URL address is 99 characters.
VpFileURL	Specifies the name of the Voice Prompts file and the location of the server (IP address or FQDN) from which it is loaded.\ For example: http://server_name/file, https://server_name/file. **Note:** The maximum length of the URL address is 99 characters.
CasFileURL	Specifies the name of the CAS file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file. **Note:** The maximum length of the URL address is 99 characters.
TLSRootFileUrl	Specifies the name of the TLS trusted root certificate file and the location URL from where it's downloaded.
TLSCertFileUrl	Specifies the name of the TLS certificate file and the location URL from where it's downloaded.
UserInfoFileURL	Specifies the name of the User Information file and the location of the server (IP address or FQDN) from which it is loaded. For example: http://server_name/file, https://server_name/file **Note:** The maximum length of the URL address is 99 characters.
AutoUpdateCmpFile	Enables / disables the Automatic Update mechanism for the cmp file. ▪ **[0]** = The Automatic Update mechanism doesn't apply to the cmp file (default). ▪ **[1]** = The Automatic Update mechanism includes the cmp file.
AutoUpdateFrequency	Determines the number of minutes the device waits between automatic updates. The default value is 0 (the update at fixed intervals mechanism is disabled).
AutoUpdatePredefinedTime	Schedules an automatic update to a predefined time of the day. The range is 'HH:MM' (24-hour format). For example: 20:18 **Note:** The actual update time is randomized by five minutes to reduce the load on the Web servers.
ResetNow	Invokes an immediate restart of the device. This option can be used to activate offline (i.e., not on-the-fly) parameters that are loaded via IniFileUrl. ▪ **[0]** = The immediate restart mechanism is disabled (default). ▪ **[1]** = The device immediately restarts after an *ini* file with this parameter set to 1 is loaded.

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td colspan="3"><b>BootP and TFTP Parameters</b></td></tr>
<tr><td colspan="3">The BootP parameters are special 'Hidden' parameters. Once defined and saved in the flash memory, they are used even if they don't appear in the <i>ini</i> file.</td></tr>
<tr><td rowspan="2"><b>BootPRetries</b></td><td colspan="2"><b>Note:</b> This parameter only takes effect from the next reset of the device.
This parameter is used to:</td></tr>
<tr><td>Set the number of BootP requests the device sends during start-up. The device stops sending BootP requests when either BootP reply is received or number of retries is reached.
▪ <b>[1]</b> = 1 BootP retry, 1 sec.
▪ <b>[2]</b> = 2 BootP retries, 3 sec.
▪ <b>[3]</b> = 3 BootP retries, 6 sec. (default).
▪ <b>[4]</b> = 10 BootP retries, 30 sec.
▪ <b>[5]</b> = 20 BootP retries, 60 sec.
▪ <b>[6]</b> = 40 BootP retries, 120 sec.
▪ <b>[7]</b> = 100 BootP retries, 300 sec.
▪ <b>[15]</b> = BootP retries indefinitely.</td><td>Set the number of DHCP packets the device sends. After all packets were sent, if there's still no reply, the device loads from flash.
▪ <b>[1]</b> = 4 DHCP packets
▪ <b>[2]</b> = 5 DHCP packets
▪ <b>[3]</b> = 6 DHCP packets (default)
▪ <b>[4]</b> = 7 DHCP packets
▪ <b>[5]</b> = 8 DHCP packets
▪ <b>[6]</b> = 9 DHCP packets
▪ <b>[7]</b> = 10 DHCP packets
▪ <b>[15]</b> = 18 DHCP packets</td></tr>
<tr><td><b>BootPSelectiveEnable</b></td><td colspan="2">Enables the Selective BootP mechanism.
▪ <b>[1]</b> = Enabled.
▪ <b>[0]</b> = Disabled (default).
The Selective BootP mechanism (available from Boot version 1.92) enables the device's integral BootP client to filter unsolicited BootP/DHCP replies (accepts only BootP replies that contain the text 'AUDC' in the vendor specific information field). This option is useful in environments where enterprise BootP/DHCP servers provide undesired responses to the device's BootP requests.
<b>Note:</b> When working with DHCP (DHCPEnable = 1) the selective BootP feature must be disabled.</td></tr>
<tr><td><b>BootPDelay</b></td><td colspan="2">The interval between the device's startup and the first BootP/DHCP request that is issued by the device.
▪ <b>[1]</b> = 1 second (default).
▪ <b>[2]</b> = 3 second.
▪ <b>[3]</b> = 6 second.
▪ <b>[4]</b> = 30 second.
▪ <b>[5]</b> = 60 second.
<b>Note:</b> This parameter only takes effect from the next reset of the device.</td></tr>
</table>

Parameter	Description
ExtBootPReqEnable	▪ **[0]** = Disable (default). ▪ **[1]** = Enable extended information to be sent in BootP request. If enabled, the device uses the vendor specific information field in the BootP request to provide device-related initial startup information such as blade type, current IP address, software version, etc. For a full list of the vendor specific Information fields, refer to the *Product Reference Manual*. The BootP/TFTP configuration utility displays this information in the 'Client Info' column (refer to the *Product Reference Manual*). **Note:** This option is not available on DHCP servers.
Serial Parameters	
DisableRS232	Enables or disables the device's RS-232 port. ▪ **[0]** = RS-232 serial port is enabled (default). ▪ **[1]** = RS-232 serial port is disabled. The RS-232 serial port can be used to change the networking parameters and view error / notification messages. For information on establishing a serial communications link with the device, refer to the device's *Installation Manual*.
SerialBaudRate	Determines the value of the RS-232 baud rate. The valid range is any value. It is recommended to use the following standard values: 1200, 2400, 9600 (default), 14400, 19200, 38400, 57600, 115200.
SerialData	Determines the value of the RS-232 data bit. ▪ **[7]** = 7-bit. ▪ **[8]** = 8-bit (default).
SerialParity	Determines the value of the RS-232 polarity. ▪ **[0]** = None (default). ▪ **[1]** = Odd. ▪ **[2]** = Even.
SerialStop	Determines the value of the RS-232 stop bit. ▪ **[1]** = 1-bit (default). ▪ **[2]** = 2-bit.
SerialFlowControl	Determines the value of the RS-232 flow control. ▪ **[0]** = None (default). ▪ **[1]** = Hardware.

4.4.3 Web and Telnet Parameters

The Web- and Telnet-related *ini* file configuration parameters are described in the table below.

Table 4-3: Web and Telnet ini File Parameters

Parameter	Description
WebAccessList_x	Defines up to ten IP addresses that are permitted to access the device's Web interface and Telnet interfaces. Access from an undefined IP address is denied. This security feature is inactive (i.e., the device can be accessed from any IP address) when the table is empty. For example: WebAccessList_0 = 10.13.2.66 WebAccessList_1 = 10.13.77.7 The default value is 0.0.0.0 (i.e., the device can be accessed from any IP address). For defining the Web and Telnet Access list using the Web interface, refer to "Configuring the Web and Telnet Access List" on page 102.
WebRADIUSLogin	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
DisableWebTask	▪ **[0]** = Enable Web management (default). ▪ **[1]** = Disable Web management.
ResetWebPassword	Resets the username and password of the primary and secondary accounts to their defaults. ▪ **[0]** = Password and username retain their values (default). ▪ **[1]** = Password and username are reset (for the default username and password, refer to User Accounts). **Note:** The username and password cannot be reset from the Web interface (i.e., via AdminPage or by loading an *ini* file).
WelcomeMessage	This *ini* file table parameter configures the Welcome message that appears after a Web interface login. The format of this parameter is as follows: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "..." ; WelcomeMessage 2 = "..." ; WelcomeMessage 3 = "..." ; [\WelcomeMessage] For Example: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "***********************************" ; WelcomeMessage 2 = "********* This is a Welcome message ***" ; WelcomeMessage 3 = "***********************************" ; [\WelcomeMessage] **Notes:** ▪ Each index represents a line of text in the Welcome message box. Up to 20 indices can be defined. ▪ If this parameter is not configured, no Welcome message is

Parameter	Description
	displayed. - For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
DisableWebConfig	Determines whether the entire Web interface is in read-only mode. - **[0]** = Enables modifications of parameters (default). - **[1]** = Web interface in read-only mode. When in read-only mode, parameters can't be modified. In addition, the following pages can't be accessed: 'Web User Accounts', 'Certificates', 'Regional Settings', 'Maintenance Actions' and all file-loading pages ('Load Auxiliary Files', 'Software Upgrade Wizard', and 'Configuration File'). **Note:** To return to read/write after you have applied read-only using this parameter (set to 1), you need to reboot your device with an *ini* file that doesn't include this parameter, using the BootP/TFTP Server utility (refer to the *Product Reference Manual*).
HTTPport	HTTP port used for Web management (default is 80).
ScenarioFileName	Defines the file name of the Scenario file to be loaded to the device. The file name must have the *dat* extension and can be up to 47 characters. For loading a Scenario using the Web interface, refer to "Loading a Scenario to the Device" on page 39.
Telnet Parameters	
TelnetServerEnable	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
TelnetServerPort	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
TelnetServerIdleDisconnect	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
SSHServerEnable	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
SSHServerPort	For a description of this parameter, refer to "Configuring the Application Settings" on page 57.
Customizing the Web Appearance Parameters For detailed information on customizing the Web interface interface, refer to "Customizing the Web Interface" on page 41.	
UseProductName	Determines whether the UserProductName text string is displayed instead of the default product name. - **[0]** = Disabled (default). - **[1]** = Enables the display of the user-defined UserProductName text string (in the Web interface interface and in the extracted *ini* file). If enabled, the UserProductName text string is displayed instead of the default product name.
UserProductName	Text string that replaces the default product name that appears in the Web interface (upper right-hand corner) and the extracted *ini* file. The default is 'Mediant 2000'. The string can be up to 29 characters.

Parameter	Description
UseWebLogo	▪ **[0]** = Logo image is used (default). ▪ **[1]** = Text string is used instead of a logo image. If enabled, AudioCodes' default logo (or any other logo defined by the LogoFileName parameter) is replaced with a text string defined by the WebLogoText parameter.
WebLogoText	Text string that replaces the logo image. The string can be up to 15 characters.
LogoWidth	Width (in pixels) of the logo image. **Note:** The optimal setting depends on the resolution settings. The default value is 441, which is the width of AudioCodes' displayed logo.
LogoFileName	Name of the image file (of type GIF, JPEG, or JPG) containing the user's logo. The logo file name can be used to replace AudioCodes' default Web logo with a user defined logo. The file name can be up to 47 characters.

4.4.4 Security Parameters

The security-related *ini* file configuration parameters are described in the table below.

Table 4-4: Security ini File Parameters

Parameter	Description
EnableMediaSecurity	For a description of this parameter, refer to "Configuring Media Security" on page 80.
MediaSecurityBehaviour	For a description of this parameter, refer to "Configuring Media Security" on page 80.
SRTPTxPacketMKISize	For a description of this parameter, refer to "Configuring Media Security" on page 80.
RTPAuthenticationDisableTx	For a description of this parameter, refer to "Configuring Media Security" on page 80.
RTPEncryptionDisableTx	For a description of this parameter, refer to "Configuring Media Security" on page 80.
RTCPEncryptionDisableTx	For a description of this parameter, refer to "Configuring Media Security" on page 80.
EnableSIPS	For a description of this parameter, refer to "General Parameters" on page 151.
TLSLocalSIPPort	For a description of this parameter, refer to "General Parameters" on page 151.
TLSVersion	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
TLSReHandshakeInterval	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
SIPSRequireClientCertificate	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.

Parameter	Description
PeerHostNameVerificationMode	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
VerifyServerCertificate	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
TLSRemoteSubjectName	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
OCSPEnable	Enables or disables certificate checking using Online Certificate Status Protocol (OCSP). ▪ **[0]** = Disable (default). ▪ **[1]** = Enable.
OCSPServerIP	Defines the IP address of the OCSP server. The default IP address is 0.0.0.0.
OCSPServerPort	Defines the OCSP server's TCP port number. The default port number is 2560.
OCSPDefaultResponse	Determines the default OCSP behavior when the server cannot be contacted. ▪ **[0]** = Rejects peer certificate (default). ▪ **[1]** = Allows peer certificate.
EnableSecureStartup	Enables the Secure Startup mode. In this mode, downloading the *.ini file to the device is restricted to a URL provided in initial configuration (see parameter IniFileURL) or using DHCP. ▪ **[0]** Disable (default). ▪ **[1]** Enable = disables TFTP and allows secure protocols such as HTTPS to fetch the device configuration. **Note:** For a detailed explanation on Secure Startup, refer to the *Product Reference Manual*.
SSHAdminKey	Determines the RSA public key for strong authentication to logging in to the Secure Shell (SSH) interface (if enabled). The value should be a base64-encoded string. The value can be a maximum length of 511 characters. For additional information, refer to the *Product Reference Manual*.
SSHRequirePublicKey	Enables or disables RSA public keys for SSH. ▪ **[0]** = RSA public keys are optional, if a value is configured for the *ini* file parameter SSHAdminKey (default). ▪ **[1]** = RSA public keys are mandatory.
IPSec Parameters	
EnableIPSec	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
IPSecDPDMode	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
IPSEC_SPD_TABLE	This *ini* file table parameter configures the IPSec SPD table. The format of this parameter is as follows: [IPSEC_SPD_TABLE]

Parameter	Description
	Format SPD_INDEX = IPSec**Mode**, IPSec**PolicyRemoteIPAddress**, IPSec**PolicySrcPort**, IPSec**PolicyDStPort**,IPSec**PolicyProtocol**, IPSec**PolicyLifeInSec**, IPSec**PolicyLifeInKB**, IPSec**PolicyProposalEncryption_X**, IPSec**PolicyProposalAuthentication_X**, IPSec**PolicyKeyExchangeMethodIndex**, IPSec**PolicyLocalIPAddressType**, IPSec**PolicyRemoteTunnelIPAddress**, IPsec**PolicyRemoteSubnetMask**; [\IPSEC_SPD_TABLE] For example: [IPSEC_SPD_TABLE] Format SPD_INDEX = IPSecMode, IPSecPolicyRemoteIPAddress, IpsecPolicySrcPort, IPSecPolicyDStPort,IPSecPolicyProtocol, IPSecPolicyLifeInSec, IPSecPolicyProposalEncryption_0, IPSecPolicyProposalAuthentication_0, IPSecPolicyProposalEncryption_1, IPSecPolicyProposalAuthentication_1, IPSecPolicyKeyExchangeMethodIndex, IPSecPolicyLocalIPAddressType; IPSEC_SPD_TABLE 0 = 0, 10.11.2.21, 0, 0, 17, 900, 1,2, 2,2 ,1, 0; [\IPSEC_SPD_TABLE] In the example above, all packets designated to IP address 10.11.2.21 that originate from the OAMP interface (regardless of destination and source ports) and whose protocol is UDP are encrypted. The IPSec SPD also defines an SA lifetime of 900 seconds and two security proposals (DES/SHA1 and 3DES/SHA1). IPsec is performed using the Transport mode. **Notes:** ▪ Each row in the table refers to a different IP destination. ▪ To support more than one Encryption / Authentication proposal, for each proposal specify the relevant parameters in the Format line. ▪ The proposal list must be contiguous. ▪ To configure the IKE table using the Web interface, refer to "Configuring the IPSec Table" on page 114. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
IKE Parameters	
IPSec_IKEDB_Table	This *ini* file table parameter configures the IKE table. The format of this parameter is as follows: [IPSec_IKEDB_Table] Format IKE_DB_INDEX = IKEPolicy**SharedKey**, IKEPolicy**ProposalEncryption_X**, IKEPolicy**ProposalAuthentication_X**, IKEPolicy**ProposalDHGroup_X**, IKEPolicy**LifeInSec**, IKEPolicy**LifeInKB**, IkePolicy**AuthenticationMethod**; [\IPSEC_IKEDB_TABLE] For example:

Parameter	Description
	[IPSec_IKEDB_Table] Format IKE_DB_INDEX = IKEPolicySharedKey, IKEPolicyProposalEncryption_0, IKEPolicypRoposalAuthentication_0, IKEPolicyProposalDHGroup_0, IKEPolicyProposalEncryption_1, IKEPolicyProposalAuthentication_1, IKEPolicyProposalDHGroup_1, IKEPolicyLifeInSec, IkePolicyAuthenticationMethod; IPSEC_IKEDB_TABLE 0 = 123456789, 1, 2, 0, 2, 2, 1, 28800, 0; [\IPSEC_IKEDB_TABLE] In the example above, a single IKE peer is configured and a pre-shared key authentication is selected. Its pre-shared key is 123456789. Two security proposals are configured: DES/SHA1/786DH and 3DES/SHA1/1024DH **Notes:** ▪ Each row in the table refers to a different IKE peer. ▪ To support more than one Encryption / Authentication / DH Group proposal, for each proposal specify the relevant parameters in the Format line. ▪ The proposal list must be contiguous. ▪ To configure the IKE table using the Web interface, refer to "Configuring the IKE Table" on page 117. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
Secure Hypertext Transport Protocol (HTTPS) Parameters	
HTTPSOnly	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
HTTPSPort	Determines the local Secured HTTPS port of the device. The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443.
HTTPSCipherString	Defines the Cipher string for HTTPS (in OpenSSL cipher list format). For the valid range values, refer to URL http://www.openssl.org/docs/apps/ciphers.html. The default is EXP:RC4.
WebAuthMode	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
HTTPSRequireClientCertificate	Requires client certificates for HTTPS connection. The client certificate must be preloaded to the device, and its matching private key must be installed on the managing PC. Time and date must be correctly set on the device, for the client certificate to be verified. ▪ **[0]** = Client certificates are not required (default). ▪ **[1]** = Client certificates are required.

Parameter	Description
HTTPSRootFileName	Defines the name of the HTTPS trusted root certificate file to be loaded via TFTP. The file must be in base64-encoded PEM (Privacy Enhanced Mail) format. The valid range is a 47-character string. **Note:** This parameter is only relevant when the device is loaded via BootP/TFTP. For information on loading this file via the Web interface, refer to the *Product Reference Manual*.
HTTPSPkeyFileName	Defines the name of a private key file (in unencrypted PEM format) to be loaded from the TFTP server.
HTTPSCertFileName	Defines the name of the HTTPS server certificate file to be loaded via TFTP. The file must be in base64-encoded PEM format. The valid range is a 47-character string. **Note:** This parameter is only relevant when the device is loaded using BootP/TFTP. For information on loading this file via the Web interface, refer to the *Product Reference Manual*.
Internal Firewall Parameters	
AccessList	This *ini* file table parameter configures the device's access list (firewall), which defines network traffic filtering rules. The format of this parameter is as follows: [ACCESSLIST] FORMAT AccessList_**Index** = AccessList_**Source_IP**, AccessList_**Net_Mask**, AccessList_**Start_Port**, AccessList_**End_Port**, AccessList_**Protocol**, AccessList_**Packet_Size**, AccessList_**Byte_Rate**, AccessList_**Byte_Burst**, AccessList_**Allow_Type**; [\ACCESSLIST] For example: [ACCESSLIST] FORMAT AccessList_Index = AccessList_Source_IP, AccessList_Net_Mask, AccessList_Start_Port, AccessList_End_Port, AccessList_Protocol, AccessList_Packet_Size, AccessList_Byte_Rate, AccessList_Byte_Burst, AccessList_Allow_Type; AccessList 10 = mgmt.customer.com, 255.255.255.255, 0, 80, tcp, 0, 0, 0, allow; AccessList 22 = 10.4.0.0, 255.255.0.0, 4000, 9000, any, 0, 0, 0, block; [\ACCESSLIST] In the example above, Rule #10 allows traffic from the host ‘mgmt.customer.com’ destined to TCP ports 0 to 80. Rule #22 blocks traffic from the subnet 10.4.xxx.yyy destined to ports 4000 to 9000. **Notes:** ▪ This parameter can include up to 50 indices. ▪ If the end of the table is reached without a match, the packet is accepted. ▪ To configure the firewall using the Web interface and for a description of the parameters of this *ini* file table parameter, refer to "Configuring the Firewall Settings" on page 103. ▪ For a description of configuring with ini file table parameters,

Parameter	Description
	refer to "Structure of ini File Table Parameters" on page 257.
AccessList_MatchCount	For a description of this parameter, refer to "Configuring the Firewall Settings" on page 103.

4.4.5 RADIUS Parameters

The RADIUS-related *ini* file configuration parameters are described in the table below. For detailed information on the supported RADIUS attributes, refer to "Supported RADIUS Attributes" on page 362.

Table 4-5: RADIUS ini File Parameters

Parameter	Description
EnableRADIUS	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
AAAIndications	For a description of this parameter, refer to "Configuring RADIUS Accounting Parameters" on page 217.
BehaviorUponRadiusTimeout	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
MaxRADIUSSessions	Number of concurrent calls that can communicate with the RADIUS server (optional). The valid range is 0 to 240. The default value is 240.
SharedSecret	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
RADIUSRetransmission	Number of retransmission retries. The valid range is 1 to 10. The default value is 3.
RadiusTO	Determines the time interval (measured in seconds) the device waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default value is 10.
RADIUSAuthServerIP	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
RADIUSAuthPort	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
RADIUSAccServerIP	For a description of this parameter, refer to "Configuring RADIUS Accounting Parameters" on page 217.
RADIUSAccPort	For a description of this parameter, refer to "Configuring RADIUS Accounting Parameters" on page 217.
RadiusAccountingType	For a description of this parameter, refer to "Configuring RADIUS Accounting Parameters" on page 217.
DefaultAccessLevel	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
RadiusLocalCacheMode	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
RadiusLocalCacheTimeout	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.

Parameter	Description
RadiusVSAVendorID	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.
RadiusVSAAccessAttribute	For a description of this parameter, refer to "Configuring the General Security Settings" on page 109.

4.4.6 SNMP Parameters

The SNMP-related *ini* file configuration parameters are described in the table below.

Table 4-6: SNMP ini File Parameters

Parameter	Description
DisableSNMP	For a description of this parameter, refer to "Configuring the Management Settings" on page 220.
SNMPPort	The device's local UDP port used for SNMP Get/Set commands. The range is 100 to 3999. The default port is 161.
SNMPTrustedMGR_x	Up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes get and set requests. **Notes:** ▪ If no values are assigned to these parameters any manager can access the device. ▪ Trusted managers can work with *all* community strings.
KeepAliveTrapPort	The port to which the keep-alive traps are sent. The valid range is 0 - 65534. The default is port 162.
SendKeepAliveTrap	When enabled, this parameter invokes the keep-alive trap and sends it every 9/10 of the time defined in the parameter defining NAT Binding Default Timeout. ▪ **[0]** = Disable ▪ **[1]** = Enable
SNMPSysOid	Defines the base product system OID. Default is eSNMP_AC_PRODUCT_BASE_OID_D.
SNMPTrapEnterpriseOid	Defines a Trap Enterprise OID. Default is eSNMP_AC_ENTERPRISE_OID. The inner shift of the trap in the AcTrap subtree is added to the end of the OID in this parameter.
acUserInputAlarmDescription	Defines the description of the input alarm.
acUserInputAlarmSeverity	Defines the severity of the input alarm.
AlarmHistoryTableMaxSize	Determines the maximum number of rows in the Alarm History table. The parameter can be controlled by the Config Global Entry Limit MIB (located in the Notification Log MIB). The valid range is 50 to 1000. The default value is 500.

Parameter	Description
SNMP Trap Parameters	
SNMPManagerTableIP_x	For a description of this parameter, refer to "Configuring the SNMP Managers Table" on page 222.
SNMPManagerTrapPort_x	For a description of this parameter, refer to "Configuring the SNMP Managers Table" on page 222.
SNMPManagerTrapUser_x	This parameter can be set to the name of any configured SNMPV3 user to associate with this trap destination. This determines the trap format, authentication level, and encryption level. By default, the trap is associated with the SNMP trap community string.
SNMPManagerIsUsed_x	For a description of this parameter, refer to "Configuring the SNMP Managers Table" on page 222.
SNMPManagerTrapSendingEnable_x	For a description of this parameter, refer to "Configuring the SNMP Managers Table" on page 222.
SNMPTrapManagerHostName	For a description of this parameter, refer to "Configuring the Management Settings" on page 220.
SNMP Community String Parameters	
SNMPReadOnlyCommunityString_x	For a description of this parameter, refer to "Configuring the SNMP Community Strings" on page 224.
SNMPReadWriteCommunityString_x	For a description of this parameter, refer to "Configuring the SNMP Community Strings" on page 224.
SNMPTrapCommunityString	For a description of this parameter, refer to "Configuring the SNMP Community Strings" on page 224.
SNMP v3 Users Parameters	
SNMPUsers	This *ini* file table parameter configures SNMP v3 users. The format of this parameter is as follows: [SNMPUsers] FORMAT SNMPUsers_**Index** = SNMPUsers_**Username**, SNMPUsers_**AuthProtocol**, SNMPUsers_**PrivProtocol**, SNMPUsers_**AuthKey**, SNMPUsers_**PrivKey**, SNMPUsers_**Group**; [\SNMPUsers] For example: [SNMPUsers] FORMAT SNMPUsers_Index = SNMPUsers_Username, SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol, SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group; SNMPUsers 1 = v3admin1, 1, 0, myauthkey, -, 1; [\SNMPUsers] The example above configures user 'v3admin1' with security level authNoPriv(2), authentication protocol MD5, authentication text password 'myauthkey', and ReadWriteGroup2. **Notes:** ▪ This parameter can include up to 10 indices. ▪ To configure SNMP v3 users through the Web interface and for a description of the parameters of this *ini* file table, refer to "Configuring SNMP V3 Users" on page 225.

Parameter	Description
	- For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

4.4.7 SIP Configuration Parameters

The SIP-related *ini* file configuration parameters are described in the table below.

Table 4-7: SIP ini File Parameters

Parameter	Description
ReliableConnectionPersistentMode	Determines whether all TCP/TLS connections are set as persistent and therefore, not released. - **[0]** = Disable (default) - all TCP connections (except those that are set to a proxy IP) are released if not used by any SIP dialog\transaction. - **[1]** = Enable - TCP connections to all destinations are persistent and not released unless the device reaches 70% of its maximum TCP resources. While trying to send a SIP message connection, reuse policy determines whether alive connections to the specific destination are re-used. Persistent TCP connection ensures less network traffic due to fewer setting up and tearing down of TCP connections and reduced latency on subsequent requests due to avoidance of initial TCP handshake. For TLS, persistent connection may reduce the number of costly TLS handshakes to establish security associations, in addition to the initial TCP connection set up.
SIPTransportType	For a description of this parameter, refer to "SIP General Parameters" on page 121.
TCPLocalSIPPort	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SIPDestinationPort	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableTCPConnectionReuse	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SIPTCPTimeout	For a description of this parameter, refer to "SIP General Parameters" on page 121.
LocalSIPPort	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableFaxReRouting	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SIPGatewayName	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
IsProxyUsed	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ProxyName	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.

Parameter	Description
AlwaysSendToProxy	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
PreferRouteTable	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
SIPReroutingMode	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
EnableProxyKeepAlive	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ProxyKeepAliveTime	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
DNSQueryType	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ProxyDNSQueryType	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ProxyIP	This *ini* file table parameter configures the Proxy Set ID table for configuring up to six Proxy Sets, each with up to five Proxy server IP addresses. The format of this parameter is as follows: [ProxyIP] FORMAT ProxyIp_**Index** = ProxyIp_**IpAddress**, ProxyIp_**TransportType**, ProxyIp_**ProxySetId**; [\ProxyIP] For example: [ProxyIP] FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_ProxySetId; ProxyIp 0 = 10.33.37.77, -1, 0; ProxyIp 1 = 10.8.8.10, 0, 2; ProxyIp 2 = 10.5.6.7, -1, 1; [\ProxyIP] **Notes:** ▪ This parameter can include up to 30 indices (0-29). ▪ For assigning various attributes (such as Proxy Load Balancing) to each Proxy Set ID, refer to the *ini* file parameter ProxySet. ▪ For configuring the Proxy Set ID table using the Web interface and for a description of the parameters of this *ini* file table, refer to "Proxy Sets Table" on page 141. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
ProxySet	This *ini* file table parameter configures the Proxy Set table by assigning various attributes per Proxy Set ID. The format of this parameter is as follows: [ProxySet] FORMAT ProxySet_**Index** = ProxySet_**EnableProxyKeepAlive**, ProxySet_**ProxyKeepAliveTime**, ProxySet_**ProxyLoadBalancingMethod**, ProxySet_**IsProxyHotSwap**; [\ProxySet]

Parameter	Description
	For example: [ProxySet] FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap; ProxySet 0 = 0, 60, 0, 0; ProxySet 1 = 1, 60, 1, 0; [\ProxySet] **Notes:** ▪ This table parameter can include up to 6 indices (0-5). ▪ For configuring the Proxy Sets, refer to the *ini* file parameter ProxyIP. ▪ For configuring the Proxy Set ID table using the Web interface and for a description of the parameters of this *ini* file table, refer to "Proxy Sets Table" on page 141. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
UseSIPTgrp	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableGRUU	For a description of this parameter, refer to "SIP General Parameters" on page 121.
UserAgentDisplayInfo	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SIPSDPSessionOwner	For a description of this parameter, refer to "SIP General Parameters" on page 121.
RetryAfterTime	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnablePAssociatedURIHeader	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableContactRestriction	For a description of this parameter, refer to "SIP General Parameters" on page 121.
RemoveToTagInFailureResponse	Determines whether the device removes the ‘to’ header tag from final SIP failure responses to INVITE transactions. ▪ **[0]** = Do not remove tag (default). ▪ **[1]** = Remove tag.
ReRegisterOnConnectionFailure	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
SourceNumberPreference	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableRTCPAttribute	Enables or disables the use of the 'rtcp' attribute in the outgoing SDP. ▪ **[0]** = Disable ▪ **[1]** = Enable (default)
OPTIONSUserPart	Defines the User-Part value of the Request-URI for outgoing SIP OPTIONS requests. If no value is configured, the configuration parameter ‘Username’ value is used.

Parameter	Description
	A special value is ‘empty’, indicating that no User-Part in the Request-URI (Host-Part only) is used. The valid range is a 30-character string. The default value is an empty string (‘’).
TDMOverIPMinCallsForTrunkActivation	Defines the minimal number of SIP dialogs that must be established when using TDM Tunneling to consider the specific trunk as active. When using TDM Tunneling, if calls from this number of B-Channels pertaining to a specific Trunk fail (i.e., SIP dialogs are not properly set up), an AIS alarm is sent on this trunk toward the PSTN, and all current calls are dropped. The originator gateway continues the INVITE attempts. When this number of calls succeed (i.e., SIP dialogs are set up properly), the AIS alarm is cleared. The valid range is 0 to 31. The default value is 0 (i.e., don't send AIS alarms).
UseGatewayNameForOptions	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
IsProxyHotSwap	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
HotSwapRtx	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ProxyRedundancyMode	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ProxyLoadBalancingMethod	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ProxyIPListRefreshTime	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
IsFallbackUsed	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
UserName	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
Password	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
Cnonce	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
SIPChallengeCachingMode	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
MutualAuthenticationMode	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
IsRegisterNeeded	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
RegistrarIP	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
RegistrarTransportType	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.

Parameter	Description
RegistrarName	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
GWRegistrationName	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
AuthenticationMode	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
OOSOnRegistrationFail	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
RegistrationTime	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
RegistrationTimeDivider	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
RegistrationRetryTime	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
RegisterOnInviteFailure	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
RegistrationTimeThreshold	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
ZeroSDPHandling	Determines the device's response to an incoming SDP with an IP address of 0.0.0.0 in the Connection line. ▪ **[0]** Sets the IP address of the outgoing SDP Connection line to 0.0.0.0 (default). ▪ **[1]** Sets the IP address of the outgoing SDP Connection line to the device's own IP address and adds a 'a=sendonly' line to the SDP.
ForkingHandlingMode	For a description of this parameter, refer to "SIP General Parameters" on page 121.
Account	This *ini* file table parameter configures the Account table for registering and/or authenticating (digest) a Trunk Group (e.g., IP-PBX) to a Serving IP Group (e.g., Internet Telephony Service Provider - ITSP). The format of this parameter is as follows: [Account] FORMAT Account_Index = Account_**ServedTrunkGroup**, Account_**ServedIPGroup**, Account_**ServingIPGroup**, Account_**Username**, Account_**Password**, Account_**HostName**, Account_**Register**, Account_**ContactUser**; [\Account] For example: [Account] FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup, Account_ServingIPGroup, Account_Username, Account_Password, Account_HostName, Account_Register, Account_ContactUser; Account 0 = 1, -1, 1, user, 1234, acl, 1, ITSP1; [\Account] **Notes:** ▪ This table can include up to 10 indices. ▪ You can define multiple table indices having the same

Parameter	Description
	ServedTrunkGroup with different ServingIPGroups, username, password, HostName, and ContactUser. This provides the capability for registering the same Trunk Group to several ITSP's (i.e., Serving IP Groups). ▪ For configuring the Account table using the Web interface and for a description of the items in this *ini* file table, refer to "Configuring the Account Table" on page 204. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
IPGroup	This *ini* file table parameter configures the IP Group table. The format of this parameter is as follows: [IPGroup] FORMAT IPGroup_**Index** = IPGroup_**Type**, IPGroup_**Description**, IPGroup_**ProxySetId**, IPGroup_**SIPGroupName**, IPGroup_**ContactUser**, IPGroup_**EnableSurvivability**, IPGroup_**ServingIPGroup**, IPGroup_**SIPReRoutingMode**, IPGroup_**AlwaysUseRouteTable**; [\IPGroup] For example: [IPGroup] FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability, IPGroup_ServingIPGroup, IPGroup_SIPReRoutingMode, IPGroup_AlwaysUseRouteTable; IPGroup 1 = 0, "acme gateway", 1, firstIPgroup, , 0, -1, 0, 0; IPGroup 2 = 0, "abc server", 2, secondIPgroup, , 0, -1, 0, 0; IPGroup 3 = 0, "IP phones", 1, thirdIPGroup, , 0, -1, 0, 0; [\IPGroup] **Notes:** ▪ This table parameter can include up to 9 indices (1-9). ▪ For configuring the IP Group table using the Web interface and for a description of the items in this *ini* file table, refer to "Configuring the IP Groups" on page 201. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
NumberOfActiveDialogs	Defines the maximum number of active SIP dialogs that are not call related (i.e., REGISTER and SUBSCRIBE). This parameter is used to control the Registration / Subscription rate. The valid range is 1 to 20. The default value is 20.
PrackMode	For a description of this parameter, refer to "SIP General Parameters" on page 121.
AssertedIdMode	For a description of this parameter, refer to "SIP General Parameters" on page 121.
PAssertedUserName	Defines a 'representative number' (up to 50 characters) that is used as the User Part of the Request-URI in the P-Asserted-Identity header of an outgoing INVITE (for Tel-to-IP calls). The default value is NULL.

Parameter	Description
UseAORInReferToHeader	Defines the source for the SIP URI set in the Refer-To header of outgoing REFER messages. ▪ **[0]** = Use SIP URI from Contact header of the initial call (default). ▪ **[1]** = Use SIP URI from To/From header of the initial call.
UseTelURIForAssertedID	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableRPIheader	For a description of this parameter, refer to "SIP General Parameters" on page 121.
IsUserPhone	For a description of this parameter, refer to "SIP General Parameters" on page 121.
IsUserPhoneInFrom	For a description of this parameter, refer to "SIP General Parameters" on page 121.
IsUseToHeaderAsCalledNumber	Determines whether the called number is set in the user part of the To header. ▪ **[0]** = Sets the destination number to the user part of the Request-URI for IP-to-Tel calls, and sets the Contact header to the source number for Tel-to-IP calls (default). ▪ **[1]** = Sets the destination number to the user part of the To header for IP-to-Tel calls, and sets the Contact header to the username parameter for Tel-to-IP calls.
EnableHistoryInfo	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SIPSubject	For a description of this parameter, refer to "SIP General Parameters" on page 121.
MultiPtimeFormat	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableReasonHeader	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableSemiAttendedTransfer	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SIP183Behavior	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnablePtime	Determines whether the ptime header is included in the SDP. ▪ **[0]** = Remove the ptime header from SDP. ▪ **[1]** = Include the ptime header in SDP (default).
EnableUserInfoUsage	For a description of this parameter, refer to "Advanced Parameters" on page 151.
HandleReasonHeader	Determines whether the device uses the value of the incoming SIP Reason header for Release Reason mapping. ▪ **[0]** Disregard Reason header in incoming SIP messages. ▪ **[1]** Use the Reason header value for Release Reason mapping (default).
EnableSilenceSuppInSDP	Determines the device's behavior upon receipt of SIP Re-INVITE messages that include the silencesupp:off attribute.

Parameter	Description
	▪ **[0]** = Disregard the silecesupp attribute (default). ▪ **[1]** = Handle incoming Re-INVITE messages that include the silencesupp:off attribute in the SDP as a request to switch to the Voice-Band-Data (VBD) mode.
EnableRport	Enables / disables the usage of the 'rport' parameter in the Via header. ▪ **[0]** = Enabled. ▪ **[1]** = Disabled (default). The device adds an 'rport' parameter to the Via header of each outgoing SIP message. The first Proxy that receives this message sets the 'rport' value of the response to the actual port from which the request was received. This method is used, for example, to enable the device to identify its port mapping outside a NAT. If the Via doesn't include 'rport' tag, the destination port of the response is taken from the host part of the Via header. If the Via includes 'rport' tag without a port value, the destination port of the response is the source port of the incoming request. If the Via includes 'rport' tag with a port value (rport=1001), the destination port of the response is the port indicated in the 'rport' tag.
DSPVersionTemplateNumber	For a description of this parameter, refer to Configuring the DSP Templates on page 79.
VBRCoderHeaderFormat	Defines the format of the RTP header for VBR coders. ▪ **[0]** = Payload only (no header, no TOC, no m-factor) -- similar to RFC 3558 Header Free format (default). ▪ **[1]** = Supports RFC 2658 - 1 byte for interleaving header (always 0), TOC, no m-factor. ▪ **[2]** = Payload including TOC only, allow m-factor. ▪ **[3]** = RFC 3558 Interleave/Bundled format.
VBRCoderHangover	Determines the required number of silence frames at the beginning of each silence period, when using the VBR Coder silence suppression. The range is 0 to 255. The default value is 1.
AMRFECRedundancyDepth	Defines the AMR / WB-AMR Redundancy depth according to RFC 3267. The valid range is 0 to 3. The default is 0.
AMRFECNumberOfCodecModes	Determines the number of entries to be defined in the AMR Management Policy table. Each entry defines the policy of a different rate. The range is 0 - 9. The default is 0.
AMRFECDelayThreshhold	Defines the one-way delay value (in msec) that may cause the AMR Hand Out report. ▪ 0 = 'Hand Out' report is disabled (default) ▪ 255 msec
AMRFECDelayHysteresis	Defines the hysteresis of the Delay Threshold for AMR Hand-out events (in msec). The valid values are 0 to 255. The default is 100 msec.

Parameter	Description
AMRCoderHeaderFormat	Determines the format of the AMR header. - **[0]** (default) = Non standard multiple frames packing in a single RTP frame. Each frame has a CMR & TOC header. - **[1]** = Reserved. - **[2]** = AMR Header according to RFC 3267 Octet Aligned header format. - **[3]** = AMR is passed using the AMR IF2 format.
TransparentCoderOnDataCall	- **[0]** = Only use coders from the coder list (default). - **[1]** = Use transparent coder for data calls (according to RFC 4040). The 'Transparent' coder can be used on data calls. When the device receives a Setup message from the ISDN with 'TransferCapabilities = data', it can initiate a call using the coder 'Transparent' (even if the coder is not included in the coder list). The initiated INVITE includes the following SDP attribute: a=rtpmap:97 CLEARMODE/8000 The default Payload Type is set according to the CoderName table. If the Transparent coder is not set in the Coders table, the default value is set to 56. The Payload Type is negotiated with the remote side, i.e., the selected Payload Type is according to the remote side selection. The receiving device must include the 'Transparent' coder in its coder list.
IsFaxUsed	For a description of this parameter, refer to "SIP General Parameters" on page 121.
T38UseRTPPort	Defines the port (with relation to RTP port) for sending and receiving T.38 packets. - **[0]** = Use the RTP port +2 to send / receive T.38 packets (default). - **[1]** = Use the same port as the RTP port to send / receive T.38 packets. **Notes:** - For this parameter to take effect, you must reset the device. - When the device is configured to use V.152 to negotiate audio and T.38 coders, the UDP port published in SDP for RTP and for T38 must be different. Therefore, set the the parameter T38UseRTPPort to 0.
DefaultReleaseCause	For a description of this parameter, refer to "SIP General Parameters" on page 121.
IPAlertTimeout	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SIPPSessionExpires	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SessionExpiresMethod	For a description of this parameter, refer to "SIP General Parameters" on page 121.
MINSE	For a description of this parameter, refer to "SIP General Parameters" on page 121.

Parameter	Description
SIPMaxRtx	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SipT1Rtx	For a description of this parameter, refer to "SIP General Parameters" on page 121.
SipT2Rtx	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableEarlyMedia	For a description of this parameter, refer to "SIP General Parameters" on page 121.
IgnoreAlertAfterEarlyMedia	Determines the device's interworking of ALERT messages from PRI to SIP. ▪ **[0]** = Disabled (default). ▪ **[1]** = Enabled. When enabled, if the device already sent a 183 response with an SDP included and an ALERT message is received from the Tel side (with or without Progress Indicator), the device does not send an additional 18x response and the voice channel remains open. When disabled, the device sends additional 18x responses as a result of receiving an ALERT message whether or not a 18x response was already sent.
EnableTransfer	For a description of this parameter, refer to "Supplementary Services" on page 159.
XferPrefix	For a description of this parameter, refer to "Supplementary Services" on page 159.
EnableMicrosofExt	Modifies the called number for numbers received with Microsoft's proprietary "ext=xxx" parameter in the SIP INVITE URI user part. Microsoft Office Communications Server sometimes uses this proprietary parameter to indicate the extension number of the called party. For example, if a calling party makes a call to telephone number 622125519100 Ext. 104, the device receives the SIP INVITE (from Microsoft's application) with the URI user part as INVITE sip:622125519100;ext=104@10.1.1.10 (or INVITE tel:622125519100;ext=104). If the parameter EnableMicrosofExt is enabled, the device modifies the called number by adding an "e" as the prefix, removing the "ext=" parameter, and adding the extension number as the suffix (e.g., **e**622125519100**104**). Once modified, the device can then manipulate the number further, using the Number Manipulation tables (refer to "Number Manipulation and Routing Parameters" on page 313) to leave only the last 3 digits (for example) for sending to a PBX. ▪ **[0]** = Disabled (default). ▪ **[1]** = Enabled.
XferPrefixIP2Tel	Defines the prefix that is added to the destination number received in the SIP Refer-to header (in IP-to-Tel calls). This parameter is applicable for CAS Blind Transfer modes (TrunkTransferMode = 3). The valid range is a string of up to 9 characters. The default is an empty string.

Parameter	Description
EnableHold	For a description of this parameter, refer to "Supplementary Services" on page 159.
HoldFormat	For a description of this parameter, refer to "Supplementary Services" on page 159.
HeldTimeout	For a description of this parameter, refer to "Supplementary Services" on page 159.
EnableForward	For a description of this parameter, refer to "Supplementary Services" on page 159.
EnableCallWaiting	For a description of this parameter, refer to "Supplementary Services" on page 159.
Send180ForCallWaiting	Determines the SIP response code for indicating call waiting. ▪ **[0]** = Use 182 Queued response to indicate call waiting (default). ▪ **[1]** = Use 180 Ringing response to indicate call waiting.
HookFlashCode	For a description of this parameter, refer to "Supplementary Services" on page 159.
UseSIPURIForDiversionHeader	Sets the URI format in the SIP Diversion header. ▪ **[0]** = 'tel:' (default) ▪ **[1]** = 'sip:'
RTPOnlyModeForTrunk_ID	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
RTPOnlyMode	For a description of this parameter, refer to "Advanced Parameters" on page 151.
TimeoutBetween100And18x	Defines the timeout (in msec) between receiving a 100 Trying response and a subsequent 18x response. If a 18x response is not received before this timer expires, the call is disconnected. The valid range is 0 to 32,000. The default value is 0 (i.e., no timeout).
TransparentCoderPresentation	Determines the format of the Transparent coder representation in the SDP. ▪ **[0]** = clearmode (default) ▪ **[1]** = X-CCD
RxDTMFOption	For a description of this parameter, refer to "DTMF & Dialing Parameters" on page 147.
TxDTMFOption	This *ini* file table parameter determines a single or several (up to 5) preferred transmit DTMF negotiation methods. The format of this parameter is as follows: [TxDTMFOption] FORMAT TxDTMFOption_Index = TxDTMFOption_**Type**; [\TxDTMFOption] For example: [TxDTMFOption] TxDTMFOption 0 = 1; [\TxDTMFOption] **Notes:** ▪ DTMF negotiation methods are prioritized according to the

Parameter	Description
	order of their appearance. - When out-of-band DTMF transfer is used ([1], [2], or [3]), the parameter DTMFTransportType is automatically set to 0 (DTMF digits are erased from the RTP stream). - When RFC 2833 ([4]) is used, the device: 1) Negotiates RFC 2833 Payload Type (PT) using local and remote SDPs. 2) Sends DTMF packets using RFC 2833 PT according to the PT in the received SDP. 3) Expects to receive RFC 2833 packets with the same PT as configured by the parameter RFC2833PayloadType. 4) Uses the same PT for send and receive if the remote party doesn't include the RFC 2833 DTMF PT in its SDP. - When TxDTMFOption is set to [0], the RFC 2833 PT is set according to the parameter RFC2833PayloadType for both transmit and receive. - For defining this parameter using the Web interface, refer to "DTMF & Dialing Parameters" on page 147. - For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
DisableAutoDTMFMute	Enables / disables the automatic muting of DTMF digits when out-of-band DTMF transmission is used. - **[0]** = Automatic mute is used (default). - **[1]** = No automatic mute of in-band DTMF. When DisableAutoDTMFMute = 1, the DTMF transport type is set according to the parameter DTMFTransportType and the DTMF digits aren't muted if out-of-band DTMF mode is selected (TxDTMFOption =1, 2 or 3). This enables the sending of DTMF digits in-band (transparent of RFC 2833) in addition to out-of-band DTMF messages. **Note:** Usually this mode is not recommended.
EnableImmediateTrying	Determines if and when the device sends a 100 Trying response to an incoming INVITE request. - **[0]** = 100 Trying response is sent upon receipt of Proceeding message from the PSTN. - **[1]** = 100 Trying response is sent immediately upon receipt of INVITE request (default).
FirstCallRBTId	For a description of this parameter, refer to "Advanced Parameters" on page 151.
EnableReasonHeader	For a description of this parameter, refer to "SIP General Parameters" on page 121.
3xxBehavior	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnablePChargingVector	For a description of this parameter, refer to "SIP General Parameters" on page 121.
EnableVMURI	For a description of this parameter, refer to "SIP General Parameters" on page 121.

Parameter	Description
MaxActiveCalls	For a description of this parameter, refer to "Advanced Parameters" on page 151.
MaxCallDuration	For a description of this parameter, refer to "Advanced Parameters" on page 151.
EnableBusyOut	For a description of this parameter, refer to "Advanced Parameters" on page 151.
EnableDigitDelivery2IP	For a description of this parameter, refer to "Advanced Parameters" on page 151.
EnableDigitDelivery	For a description of this parameter, refer to "Advanced Parameters" on page 151.
SITDetectorEnable	Enables or disables Special Information Tone (SIT) detection according to the ITU-T recommendation E.180/Q.35. ▪ **[0]** = Disable (default). ▪ **[1]** = Enable.
SourceIPAddressInput	For a description of this parameter, refer to "Routing General Parameters" on page 171.
EnableSBC	For a description of this parameter, refer to “SBC Configuration” on page 163.
SBCRegistrationTime	For a description of this parameter, refer to “SBC Configuration” on page 163.
Stand-Alone Survivability (SAS) Parameters	
EnableSAS	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
SASLocalSIPUDPPort	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
SASDefaultGatewayIP	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
SASRegistrationTime	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
SASLocalSIPTCPPort	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
SASLocalSIPTLSPort	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
SASProxySet	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
RedundantSASProxySet	For a description of this parameter, refer to “Stand-Alone Survivability” on page 161.
SASSurvivabilityMode	Determines the Survivability mode used by the SAS application. ▪ **[0]** Standard = All incoming INVITE and REGISTER requests are forwarded to the defined Proxy list in SASProxySet in Normal mode and handled by the SAS application in Emergency mode (default). ▪ **[1]** Always Emergency = The SAS application does not use Keep-Alive messages towards the SASProxySet and instead, always operates in Emergency mode (as if no Proxy in the

Parameter	Description
	SASProxySet is available). ▪ **[2]** Ignore REGISTER = Use regular SAS Normal/Emergency logic (same as option 0) but when in Normal mode, incoming REGISTER requests are ignored.
SASBindingMode	Determines the SAS application database binding mode. ▪ **[0]** URI = If the incoming AoR in the INVITE requests is using a 'tel:' URI or 'user=phone' is defined, the binding is performed according to the user part of the URI only. Otherwise, the binding is according to the entire URI, i.e., User@Host (default). ▪ **[1]** User Part only = The binding is always performed according to the User Part only.
SASEnableENUM	Determines whether the SAS application uses ENUM queries to route incoming INVITE requests when in Emergency mode. Once an INVITE is received in Emergency mode, the SAS database of registered users is searched for a matching AoR. If not found, the Redundant SAS servers are searched. If there is still no match, an ENUM query is performed and the response is used to correctly route the INVITE. If no response is received from the ENUM server, the INVITE is routed to the default gateway. ▪ [0] = Disable (default) ▪ [1] = Enable
SASRegistrationManipulation	This ini file table parameter is used by the SAS application to manipulate the User-Part of an incoming REGISTER request AoR (the To header), before saving it to the registered users database. The format of this table parameter is as follows: [SASRegistrationManipulation] FORMAT SASRegistrationManipulation_Index = SASRegistrationManipulation_RemoveFromRight, SASRegistrationManipulation_LeaveFromRight; [\SASRegistrationManipulation] ▪ RemoveFromRight = number of digits removed from the right side of the User-Part before saving to the registered user database. ▪ LeaveFromRight = number of digits to keep from the right side. If both RemoveFromRight and LeaveFromRight are defined, the RemoveFromRight is applied first. The registered database contains the AoR before and after the manipulation. The range of both RemoveFromRight and LeaveFromRight is 0 to 30. **Note:** This table can include only one index entry.
SASEmergencyNumbers	Defines emergency numbers for the device's SAS application. When the device's SAS agent receives a SIP INVITE (from an IP phone) that includes one of the emergency numbers (in the SIP user part), it forwards the INVITE to the default gateway (configured by the parameter SASDefaultGatewayIP), i.e., the device itself, which sends the call directly to the PSTN. This is important for routing emergency numbers such as 911 (in North America) directly to the PSTN. This is applicable to SAS operating in Normal and Emergency modes.

Parameter	Description
	Up to four emergency numbers can be defined, where each number can be up to four digits.
Profile Parameters	
CoderName	This *ini* file table parameter defines the device's coder list. This includes up to five groups of coders (consisting of up to five coders per group) that can be associated with IP or Tel profiles ('Coder Group Settings' page in the Web interface -- refer to ''Coder Group Settings'' on page 190). The first group of coders (indices 0 through 4) is the default coder list and default coder group. The format of this parameter is as follows: [CoderName] FORMAT CoderName_Index = CoderName_**Type**, CoderName_**PacketInterval**, CoderName_**rate**, CoderName_**PayloadType**, CoderName_**Sce**; [\CoderName] Where, ▪ Type = Coder name ▪ PacketInterval = Packetization time ▪ Rate = Packetization rate ▪ PayloadType = Payload type ▪ Sce = Silence suppression mode For example: [CoderName] CoderName 0 = g711Alaw64k, 20,,,0; CoderName 1 = g726, $$, 3, 38, 0; CoderName 2 = g729, 40, 255, 255, 1; [\CoderName] **Notes:** ▪ This parameter can include up to 25 indices (i.e., five coders per five coder groups). ▪ The coder name is case-sensitive. ▪ If silence suppression is not defined for a specific coder, the value defined by the parameter EnableSilenceCompression is used. ▪ The value of several fields is hard-coded according to common standards (e.g., payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored. ▪ Only the ptime of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined. ▪ If the coder G.729 is selected and silence suppression is enabled (for this coder), the device includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception is when the remote device is a Cisco gateway (IsCiscoSCEMode). ▪ Both GSM-FR and MS-GSM coders use Payload Type 3. When using SDP, it isn’t possible to differentiate between the

Parameter	Description
	two. Therefore, it is recommended not to select both coders simultaneously. ▪ For a list of supported coders, refer to "Coders" on page 144. ▪ To configure the 'Coders' table in the Web interface, refer to "Coders" on page 144. ▪ For a description of using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
IPProfile	This *ini* file table parameter configures the IP profiles table. The format of this parameter is as follows: [IPProfile] FORMAT IPProfile_Index = IPProfile_**ProfileName**, IPProfile_**IpPreference**, IPProfile_**CodersGroupID**, IPProfile_**IsFaxUsed***, IPProfile_**JitterBufMinDelay***, IPProfile_**JitterBufOptFactor***, IPProfile_**IPDiffServ***, IPProfile_**SigIPDiffServ***, N/A, IPProfile_**RTPRedundancyDepth**, IPProfile_**RemoteBaseUDPPort**, IPProfile_**CNGmode**, IPProfile_**VxxTransportType**, IPProfile_**NSEMode**, N/A, IPProfile_**PlayRBTone2IP**, IPProfile_**EnableEarlyMedia***, IPProfile_**ProgressIndicator2IP***, IPProfile_**EnableEchoCanceller***, IPProfile_CopyDest2RedirectNumber, IPProfile_**MediaSecurityBehaviour**, IPProfile_**CallLimit**, IPProfile_ **DisconnectOnBrokenConnection**; [\IPProfile] For example: [IPProfile] IPProfile_1 = name1,2,1,0,10,13,15,44,1,1,6000,0,2,0,0,0,1,0,1,0,0,-1,1; IPProfile_2 = name2,$$,40,$$; [\IPProfile] **Notes:** ▪ This parameter can appear up to 9 times (i.e., indices 1-9). ▪ * Indicates common parameters used in both IP and Tel profiles. ▪ IpPreference = determines the priority of the Profile (1 to 20, where 20 is the highest preference). If both IP and Tel profiles apply to the same call, the coders and other common parameters (indicated with an asterisk) of the preferred Profile are applied to that call. If the Tel and IP profiles are identical, the Tel Profile parameters are applied. ▪ Two adjacent dollar signs ('$$') indicate that the parameter's default value is used. ▪ IPProfile can be used in the 'Tel to IP Routing' (or 'Outbound IP Routing Table' if EnableSBC is set to 1) and 'IP to Trunk Group Routing' tables (Prefix and PSTNPrefix parameters). ▪ The 'Profile Name' assigned to a Profile index, must enable users to identify it intuitively and easily. ▪ To configure the IP Profile table using the Web interface, refer to "IP Profile Settings" on page 193.

Parameter	Description
	- For a description of using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
TelProfile	This *ini* file table parameter configures the Tel Profile Settings table. The format of this parameter is as follows: [TelProfile] FORMAT TelProfile_**Index** = TelProfile_**ProfileName**, TelProfile_**TelPreference**, TelProfile_**CodersGroupID**, TelProfile_**IsFaxUsed***, TelProfile_**JitterBufMinDelay***, TelProfile_**JitterBufOptFactor***, TelProfile_**IPDiffServ***, TelProfile_**SigIPDiffServ***, TelProfile_**DtmfVolume**, TelProfile_**InputGain**, TelProfile_**VoiceVolume**, N/A, N/A, TelProfile_**EnableDigitDelivery**, TelProfile_**EnableEC**, N/A, N/A, TelProfile_**FlashHookPeriod**, TelProfile_**EnableEarlyMedia***, TelProfile_**ProgressIndicator2IP***, TelProfile_**TimeForReorderTone***, N/A, N/A, N/A; [\TelProfile] * = Indicates common parameters used in both IP and Tel profiles. TelPreference = determines the priority of the Profile (1 to 20, where 20 is the highest preference). If both IP and Tel profiles apply to the same call, the coders and other common parameters (indicated with an asterisk) of the preferred Profile are applied to that call. If the preference of the Tel and IP profiles is identical, the Tel Profile parameters are applied. For example: [TelProfile] TelProfile 1 = FaxProfile,1,1,1,40,13,22,33,$$,$$,$$,0,0,0,1,0,0,$$,0,$$,$$,$$,$$,$$; TelProfile 2 = ModemProfile,2,2,0,40,13,$$,$$,$$,$$,$$,$$,$$,$$,0,0,0,$$,0,$$,$$,$$,$$; [\TelProfile] **Notes:** - This parameter can appear up to 9 times (i.e., indices 1-9). - Two adjacent dollar signs ('$$') indicates that the parameter's default value is used. - The TelProfile index can be used in the Trunk Group table (TrunkGroup parameter). - The 'Profile Name' assigned to a Profile index must enable users to identify it intuitively and easily. - To configure the Tel Profile table using the Web interface, refer to "Tel Profile Settings" on page 192. - For a description of using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

4.4.8 Media Server Parameters

The media processing-related *ini* file configuration parameters are described in the table below.

Table 4-8: Media Server ini File Parameters

Parameter	Description
AMRCoderHeaderFormat	Determines the format of the AMR header. ▪ **[0]** = Non-standard multiple frames packing in a single RTP frame. Each frame has a CMR and TOC header. ▪ **[1]** = Reserved. ▪ **[2]** = AMR Header according to RFC 3267 Octet Aligned header format. ▪ **[3]** = AMR is passed using the AMR IF2 format.
EnableAGC	For a description of this parameter, refer to "Configuring the IPmedia Settings" on page 76.
AGCGainSlope	For a description of this parameter, refer to "Configuring the IPmedia Settings" on page 76.
AGCRedirection	For a description of this parameter, refer to "Configuring the IPmedia Settings" on page 76.
AGCTargetEnergy	For a description of this parameter, refer to "Configuring the IPmedia Settings" on page 76.
AGCMinGain	Defines the minimum gain (in dB) by the AGC when activated. The range is 0 to -31. The default is -20.
AGCMaxGain	Defines the maximum gain (in dB) by the AGC when activated. The range is 0 to 18. The default is 15.
AGCDisableFastAdaptation	Disables the AGC Fast Adaptation mode. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
AMDDetectionSensitivity	For a description of this parameter, refer to "Configuring the IPmedia Settings" on page 76.
AMDTimeout	Timeout (in msec) between receiving CONNECT messages from the ISDN and sending Answering Machine Detection (AMD) results. The valid range is 1 to 30,000. The default is 2,000 (i.e., 2 seconds).
AMDDetectionDirection	Determines the AMD (Answer Machine Detector) detection direction. ▪ **[0]** = Detection from the PSTN side ▪ **[1]** = Detection from the IP side

4.4.9 Voice Mail Parameters

The voice mail-related *ini* file configuration parameters are described in the table below. For detailed information on the Voice Mail application, refer to the *CPE Configuration Guide for Voice Mail*.

Table 4-9: Voice Mail ini File Parameters

Parameter	Description
VoiceMailInterface	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
SMDI	For a description of this parameter, refer to Configuring the Voice Mail (VM) Parameters on page 214.
SMDITimeOut	For a description of this parameter, refer to Configuring the Voice Mail (VM) Parameters on page 214.
LineTransferMode	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
WaitForDialTime	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
MWIOnCode	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
MWIOffCode	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
MWISuffixCode	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
MWISourceNumber	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
Digit Patterns The following digit pattern parameters apply only to VM applications that use the DTMF communication method. For the available pattern syntaxes, refer to the CPE Configuration Guide for Voice Mail.	
DigitPatternForwardOnBusy	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternForwardOnNoAnswer	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternForwardOnDND	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternForwardNoReason	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternForwardOnBusyExt	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternForwardOnNoAnswerExt	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternForwardOnDNDExt	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternForwardNoReasonExt	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.

Parameter	Description
DigitPatternInternalCall	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternExternalCall	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
TelDisconnectCode	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.
DigitPatternDigitToIgnore	For a description of this parameter, refer to "Configuring the Voice Mail (VM) Parameters" on page 214.

4.4.10 PSTN Parameters

The PSTN-related *ini* file configuration parameters are described in the table below.

Table 4-10: PSTN ini File Parameters

Parameter	Description
PCMLawSelect	For a description of this parameter, refer to “Configuring the TDM Bus Settings” on page 218.
ProtocolType	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ProtocolType_x	Same as the description for parameter ProtocolType, but for a specific trunk ID (x = 0 - 7).
TraceLevel	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
FramingMethod	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
FramingMethod_x	Same as the description for parameter FramingMethod, but for a specific trunk ID (x = 0 - 7).
TerminationSide	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
TerminationSide_x	Same as the description for parameter TerminationSide, but for a specific trunk ID (x = 0 - 7).
ClockMaster	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ClockMaster_x	Same as the description for parameter ClockMaster, but for a specific trunk ID (x = 0 - 7).
TDMBusClockSource	For a description of this parameter, refer to “Configuring the TDM Bus Settings” on page 218.
TDMBusPSTNAutoClockEnable	For a description of this parameter, refer to “Configuring the TDM Bus Settings” on page 218.
TDMBusLocalReference	For a description of this parameter, refer to “Configuring the TDM Bus Settings” on page 218.
AutoClockTrunkPriority	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.

Parameter	Description
TDMBusPSTNAutoClockRevertingEnable	For a description of this parameter, refer to "Configuring the TDM Bus Settings" on page 218.
TDMBusEnableFallback	Defines the automatic fallback of the clock. ▪ **[0]** = Manual (default) ▪ **[1]** = Auto Non-Revertive ▪ **[2]** = Auto Revertive
TDMBusFallbackClock	Selects the fallback clock source on which the device synchronizes in the event of a clock failure. ▪ **[4]** = PSTN Network (default) ▪ **[8]** = H.110A ▪ **[9]** = H.110B ▪ **[10]** = NetRef1 ▪ **[11]** = NetRef2
TDMBusNetrefSpeed	Determines the NetRef frequency (for both generation and synchronization). ▪ **[0]** = 8 kHz (default) ▪ **[1]** = 1.544 MHz ▪ **[2]** = 2.048 MHz
LineCode	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
LineCode_x	Same as the description for parameter LineCode, but for a specific trunk ID (where 0 depicts the first trunk).
EnableCallingPartyCategory	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
BChannelNegotiation	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
NFASGroupNumber_x	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
DChConfig_x	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
ISDNNFASInterfaceID_x	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
CASTableIndex_x	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
CASFileName_0 **CASFileName_1** **CASFileName_7**	CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol. It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device trunks using the parameter CASTableIndex_x.
CASTablesNum	1 to 8. Indicates how many CAS protocol configurations files are loaded.
IdleABCDPattern	For a description of this parameter, refer to "Configuring the TDM Bus Settings" on page 218.
IdlePCMPattern	For a description of this parameter, refer to "Configuring the TDM Bus Settings" on page 218.

Parameter	Description
LineBuildOut.Loss	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ISDNRxOverlap_x	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ISDNRxOverlap	**[0]** = Disabled (default). **[1]** = Enabled. Any number bigger than one = Number of digits to receive. **Notes:** ▪ If enabled, the device receives ISDN called number that is sent in the 'Overlap' mode. ▪ The INVITE to IP is sent only after the number (including 'Sending Complete' Info Element) was fully received (in SETUP and/or subsequent INFO Q.931 messages). For detailed information on ISDN overlap dialing, refer to ISDN Overlap Dialing on page 398.
R2Category	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
CallPriorityMode	For a description of this parameter, refer to "Supplementary Services" on page 159.
MLPPDefaultNamespace	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
SIPDefaultCallPriority	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
MLPPDiffserv	For a description of this parameter, refer to "Supplementary Services" on page 159.
PreemptionToneDuration	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
MLPPNormalizedServiceDomain	MLPP normalized service domain string. If the device receives an MLPP ISDN incoming call, it uses the parameter (if different from ‘FFFFFF’) as a Service domain in the SIP Resource-Priority header in outgoing INVITE messages. If the parameter is ‘FFFFFF’, the Resource-Priority header is set to the MLPP Service Domain obtained from the Precedence IE. The valid value is a 6 hexadecimal digits. The default is ‘000000’. **Note:** This parameter is applicable only to device's using the MLPP NI-2 ISDN variant with CallPriorityMode set to 1.
MLPPDefaultServiceDomain	MLPP default service domain string. If the device receives a non MLPP ISDN incoming call (without a Precedence IE), it uses the parameter as a Service domain in the SIP Resource-Priority header in outgoing (Tel-to-IP calls) INVITE messages. This parameter is used in conjunction with the parameter SipDefaultCallPriority. The valid value is a 6 hexadecimal digits. The default is "000000". **Note:** This parameter is applicable only to device's using the MLPP NI-2 ISDN variant with CallPriorityMode set to 1.

Parameter	Description
TrunkAdministrativeState	Defines the administrative state of a trunk. - **[0]** = Lock the trunk; stops trunk traffic to configure the trunk protocol type. - **[2]** = Unlock the trunk (default); enables trunk traffic.
ISDN Flexible Behavior Parameters ISDN protocol is implemented in different Switches / PBXs by different vendors. Several implementations vary a little from the specification. Therefore, to provide a flexible interface that supports these ISDN variants, the ISDN behavior parameters are used.	
ISDNInCallsBehavior	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ISDNIBehavior	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ISDNGeneralCCBehavior	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ISDNOutCallsBehavior	For a description of this parameter, refer to “Configuring the Trunk Settings” on page 82.
ISDNIBehavior_x	Same as the description for parameter ISDNIBehavior, but for a specific trunk ID.
ISDNInCallsBehavior_x	Same as the description for parameter ISDNInCallsBehavior, for a specific trunk ID.
ISDNOutCallsBehavior_x	Same as the description for parameter ISDNOutCallsBehavior, but for a specific trunk ID.
PlayRBTone2Tel	For a description of this parameter, refer to "SIP General Parameters" on page 121.
PlayRBTone2IP	For a description of this parameter, refer to "SIP General Parameters" on page 121.
ProgressIndicator2IP	For a description of this parameter, refer to "Advanced Parameters" on page 151.
TimeForReorderTone	Busy or Reorder Tone duration that the device, when configured to protocol type CAS, plays before releasing the line. The valid range is 0 to 15. The default value is 10 seconds. Applicable also to ISDN if PlayBusyTone2ISDN = 2. Selection of Busy or Reorder tone is done according to release cause received from IP.
ISDNDisconnectOnBusyTone	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
DisconnectOnBusyTone	For a description of this parameter, refer to Configuring the Digital Gateway Parameters on page 207.
EnableVoiceDetection	- **[1]** = The device sends 200 OK (to INVITE) messages when speech/fax/modem is detected from the Tel side. - **[0]** = The device sends 200 OK messages immediately after the device finishes dialing to the Tel side (default). Usually this feature is used only when early media (EnableEarlyMedia) is used to establish voice path before the call is answered. **Notes:** - To activate this feature, set EnableDSPIPMDetectors to 1. - This feature is applicable only when the protocol type is CAS.

Parameter	Description
DigitMapping	For a description of this parameter, refer to "DTMF & Dialing Parameters" on page 147.
TimeBetweenDigits	For a description of this parameter, refer to "DTMF & Dialing Parameters" on page 147.
MaxDigits	For a description of this parameter, refer to "DTMF & Dialing Parameters" on page 147.
TimeForDialTone	For a description of this parameter, refer to "DTMF & Dialing Parameters" on page 147.
RegretTime	For a description of this parameter, refer to "Advanced Parameters" on page 151.

4.4.11 ISDN and CAS Interworking-Related Parameters

The ISDN- and CAS-related *ini* file configuration parameters are described in the table below.

Table 4-11: ISDN and CAS Interworking-Related ini File Parameters

Parameter	Description
EnableTDMoverIP	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
EnableISDNTunnelingTel2IP	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
EnableISDNTunnelingIP2Tel	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
ISDNDuplicateQ931BuffMode	Controls the activation / deactivation of delivering raw Q.931 messages. ▪ **[0]** = ISDN messages aren't duplicated (default). ▪ **[128]** = All ISDN messages are duplicated. **Note:** This parameter is not updated on-the-fly and requires a device reset.
EnableQSIGTunneling	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
PlayRBTone2Trunk_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
DigitalOOSBehaviorFor Trunk_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
DigitalOOSBehavior	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
RemoveCallingName	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
DefaultCauseMapISDN2IP	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.

Parameter	Description
CauseMapSIP2ISDN	This *ini* file table parameter maps SIP Responses to Q.850 Release Causes. The format of this parameter is as follows: [CauseMapSIP2ISDN] FORMAT CauseMapSIP2ISDN_**Index** = CauseMapSIP2ISDN_**SipResponse**, CauseMapSIP2ISDN_**IsdnReleaseCause**; [\CauseMapSIP2ISDN] Where, ▪ SipResponse = SIP Response ▪ IsdnReleaseCause = Q.850 Release Cause For example: [CauseMapSIP2ISDN] CauseMapSIP2ISDN 0 = 480,50; CauseMapSIP2ISDN 0 = 404,3; [\CauseMapSIP2ISDN] When a SIP response is received (from the IP side), the device searches this mapping table for a match. If the SIP response is found, the Release Cause assigned to it is sent to the PSTN. If no match is found, the default static mapping is used. **Notes:** ▪ This parameter can appear up to 12 times. ▪ For an explanation on *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
CauseMapISDN2SIP	This *ini* file table parameter maps Q.850 Release Causes to SIP Responses. The format of this parameter is as follows: [CauseMapISDN2SIP] FORMAT CauseMapISDN2SIP_**Index** = CauseMapISDN2SIP_**IsdnReleaseCause**, CauseMapISDN2SIP_**SipResponse**; [\CauseMapISDN2SIP] Where, ▪ IsdnReleaseCause = Q.850 Release Cause ▪ SipResponse = SIP Response For example: [CauseMapISDN2SIP] CauseMapISDN2SIP 0 = 50,480; CauseMapISDN2SIP 0 = 6,406; [\CauseMapISDN2SIP] When a Release Cause is received (from the PSTN side), the device searches this mapping table for a match. If the Q.850 Release Cause is found, the SIP response assigned to it is sent to the IP side. If no match is found, the default static mapping is used. **Notes:** ▪ This parameter can appear up to 12 times. ▪ For an explanation on *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

Parameter	Description
SITQ850Cause	Determines the Q.850 cause value specified in the Reason header that is included in a 4xx response when Special Information Tone (SIT) is detected on an IP-to-Tel call. The valid range is 0 to 127. The default value is 34.
UserToUserHeaderFormat	Determines the format of the User-to-User header. ▪ **[0]** = X-UserToUser (default). ▪ **[1]** = User-to-User with Protocol Discriminator (pd) attribute User-to-User=30303734353137343136353533b313233343b3834;pd=4. This is in accordance with the definitions in 'draft-johnston-sipping-cc-uui-04'. ▪ **[2]** = User-to-User with pd embedded as the first byte. User-to-User=0430303734353137343136353533b313233343b3834; encoding=hex
RemoveCLIWhenRestricted	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
ScreeningInd2ISDN	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
ProgressIndicator2ISDN_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
PIForDisconnectMsg_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
ConnectOnProgressInd	Enables the play of announcements from IP to PSTN without the need to answer the Tel-to-IP call. It can be used with PSTN networks that don't support the opening of a TDM channel before an ISDN Connect message is received. ▪ **[0]** = Connect message isn't sent after SIP 183 Session Progress message is received (default). ▪ **[1]** = Connect message is sent after SIP 183 Session Progress message is received.
LocalISDNRBSource_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
PSTNAlertTimeout	For a description of this parameter, refer to "Advanced Parameters" on page 151.
TrunkPSTNAlertTimeout_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
ISDNTransferCapability_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
BChannelNegotiationForTrunk_ID	For a description of this parameter, refer to "Configuring the Trunk Settings" on page 82.
SendISDNTransferOnConnect	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
ISDNSubAddressFormat	Determines the format of the 'subaddress' value for ISDN Calling and Called numbers. ▪ **[0]** = ASCII (default).

Parameter	Description
	▪ **[1]** = BCD (Binary Coded Decimal) ▪ **[2]** = User Specified For IP-to-Tel calls, if the incoming SIP INVITE message includes subaddress values in the 'isub' parameter for the Called Number (in the Request-URI) and/or the Calling Number (in the From header), these values are mapped to the outgoing ISDN SETUP message. If the incoming ISDN SETUP message includes 'subaddress' values for the Called Number and/or the Calling Number, these values are mapped to the outgoing SIP INVITE message's ‘isub’ parameter in accordance with RFC 4715.
EnableHold2ISDN	For a description of this parameter, refer to "Supplementary Services" on page 159.
EnableUUITel2IP	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
EnableUUIIP2Tel	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
ScreeningInd2IP	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
SupportRedirectInFacility	Determines whether the Redirect Number is retrieved from the Facility IE. ▪ **[0]** = Not supported (default). ▪ **[1]** = Supports partial retrieval of Redirect Number (number only) from the Facility IE in ISDN SETUP messages. Applicable to Redirect Number according to ECMA-173 Call Diversion Supplementary Services. **Note:** To enable this feature, ISDNDuplicateQ931BuffMode must be set to 1.
EnableCIC	Determines whether Carrier Identification Code (CIC) is relayed to ISDN. ▪ **[0]** = Do not relay the Carrier Identification Code (CIC) to ISDN (default). ▪ **[1]** = CIC is relayed to the ISDN in Transit Network Selection (TNS) IE. If enabled, the CIC code (received in an INVITE Request-URI) is included in a TNS IE in the ISDN SETUP message. For example: INVITE sip:555666;cic=2345@100.2.3.4 sip/2.0. **Note:** Currently, this feature is supported only in the SIP-to-ISDN direction.
EnableAOC	▪ **[0]** = Not used (default). ▪ **[1]** = ISDN Advice of Charge (AOC) messages are interworked to SIP. The device supports receipt of ISDN (Euro ISDN) AOC messages. AOC messages can be received during a call (FACILITY messages) or at the end of a call (DISCONNECT or RELEASE messages). The device converts the AOC messages into SIP INFO (during a call) and BYE (end of a call) messages, using a proprietary AOC SIP header. The device supports both

Parameter	Description
	Currency and Pulse AOC messages.
PlayBusyTone2ISDN	For a description of this parameter, refer to "SIP General Parameters" on page 121.
TrunkTransferMode_X	Determines the supported trunk transfer method when a SIP REFER message is received. - **[0]** = Not supported (default). - **[1]** = Supports CAS NFA DMS-100 transfer. When a SIP REFER message is received, the device performs a Blind Transfer by executing a CAS Wink, waits for an acknowledged Wink from the remote side, dials the Refer-to number to the switch, and then releases the call. **Note:** A specific NFA CAS table is required. - **[2]** = Supports ISDN transfer: RLT (DMS-100), TBCT (NI2), ECT (EURO ISDN), and Path Replacement (QSIG). When a SIP REFER message is received, the device performs a transfer by sending FACILITY messages to the PBX with the necessary information on the call's legs that are to be connected. The different ISDN variants use slightly different methods (using FACILITY messages) to perform the transfer. - **[3]** = Supports CAS Normal transfer. When a SIP REFER message is received, the device performs a Blind Transfer by executing a CAS Wink, dialing the Refer-to number to the switch, and then releasing the call. - **[4]** = Supports QSIG Single Step transfer: IP-to-Tel: When a SIP REFER message is received, the device performs a transfer by sending a FACILITY message to the PBX, initiating Single Step transfer. Once a success return result is received, the transfer is completed. Tel-to-IP: When a FACILITY message initiating Single Step transfer is received from the PBX, a REFER message is sent to the IP side. **Notes:** - To use QSIG Path Replacement, the parameter UserToUserHeaderFormat must be set to 1. - To configure Trunk Transfer Mode using the Web interface, refer to "Configuring the Trunk Settings" on page 82.
CASTransportType	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
CASAddressingDelimiters	Determines if delimiters are added to the dialed address or dialed ANI parameters. - **[0]** = Disable (default) - **[1]** = Enable When this parameter is enabled, delimiters such as '*', '#', and 'ST' are added to the dialed address or dialed ANI parameters. When it is disabled, the address and ANI strings remain without delimiters.

Parameter	Description
CASDelimitersPaddingUsage	Defines the digits string delimiter padding usage per trunk. ▪ **[0]** (default) = default address string padding: '*XXX#' (where XXX is the digit string that begins with '*' and ends with '#', when using padding). ▪ **[1]** = special use of asterisks delimiters: '*XXX*YYY*' (where XXX is the address, YYY is the source phone number, and '*' is the only delimiter padding).
CasStateMachineGenerateDigitOnTime	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
CasStateMachineGenerateInterDigitTime	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
CasStateMachineDTMFMaxOnDetectionTime	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
CasStateMachineDTMFMinOnDetectionTime	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
CasStateMachineMaxNumOfIncomingAddressDigits	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
CasStateMachineMaxNumOfIncomingANIDigits	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
CasStateMachineCollectANI	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
CasStateMachineDigitSignalingSystem	For a description of this parameter, refer to "Configuring the CAS State Machines" on page 97.
EnableDSPIPMDetectors	Enables or disables the device's DSP detectors. ▪ **[0]** = Disable (default). ▪ **[1]** = Enable. **Notes:** ▪ The device's Feature Key should contain the 'IPMDetector' DSP option. ▪ When enabled (1), the number of available channels is reduced by a factor of 5/6. For example, a device with 8 E1 spans, capacity is reduced to 6 spans (180 channels), while a device with 8 T1 spans, capacity remains the same (192 channels).
XChannelHeader	For a description of this parameter, refer to "Advanced Parameters" on page 151.
AddIEinSetup	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
SendIEonTG	For a description of this parameter, refer to "Configuring the Digital Gateway Parameters" on page 207.
ISDNDMSTimerT310	Overrides the T310 timer for the DMS-100 ISDN variant. T310 defines the timeout between the reception of a PROCEEDING message and the reception of an ALERTING / CONNECT message. The valid range is 10 to 30. The default value is 10 (seconds). **Note:** Applicable only to Nortel DMS and Nortel MERIDIAN PRI variants (ProtocolType = 14 and 35).

Parameter	Description
ISDNJapanNTTTimerT3JA	T3_JA timer (in seconds). This parameter overrides the internal PSTN T301 timeout on the Users Side (TE side). If an outgoing call from the device to ISDN is not answered during this timeout, the call is released. The valid range is 10 to 240. The default value is 50. Applicable only to Japan NTT PRI variant (ProtocolType = 16). **Note:** This timer is also affected by the parameter PSTNAlertTimeout.
EnablePatternDetector	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
PDPattern	Defines the patterns that can be detected by the Pattern Detector. The valid range is 0 to 0xFF.
PDThreshold	Defines the number of consecutive patterns to trigger the pattern detection event. The valid range is 0 to 31. The default is 5.
Enable911LocationIdIP2Tel	Enables interworking of Emergency Location Identification from SIP to PRI. ▪ **[0]** = Disabled (default) ▪ **[1]** = Enabled When enabled, the From header received in the SIP INVITE is translated into the following ISDN Information Elements (IE): ▪ Emergency Call Control IE. ▪ Generic Information IE to carry the Location Identification Number information. ▪ Generic Information IE to carry the Calling Geodetic Location information. **Note:** This capability is supported only for the NI-2 ISDN variant.
EarlyAnswerTimeout	Defines the time (in seconds) that the device waits for a CONNECT message from the called party (Tel side) after sending a SETUP message. If the timer expires, the call is answered by sending a 200 OK message (IP side). The valid range is 0 to 600. The default value is 0 (i.e., disabled).

4.4.12 Number Manipulation and Routing Parameters

The number manipulation and routing-related *ini* file configuration parameters are described in the table below.

Table 4-12: Number Manipulation and Routing ini File Parameters

Parameter	Description
TrunkGroup	This *ini* file table parameter defines the device's Trunks and assigns them to Trunk Groups. The format of this parameter is shown below: [TrunkGroup] FORMAT TrunkGroup_**Index** = TrunkGroup_**TrunkGroupNum**, TrunkGroup_**FirstTrunkId**, TrunkGroup_**LastTrunkId**, TrunkGroup_**FirstBChannel**, TrunkGroup_**LastBChannel**, TrunkGroup_**FirstPhoneNumber**, TrunkGroup_**ProfileId**, TrunkGroup_**Module**; [\TrunkGroup] For example: [TrunkGroup] TrunkGroup 1 = 0, 0, 0, 1, 31 ,401, 0; (E1 span) TrunkGroup 1 = 0, 0, 0, 1, 31, $$, 1; TrunkGroup 2 = 1, 2, 2, 1, 24, 3000; (T1 span) TrunkGroup 1 = 2, 0, 7, 1, 20, 1000; (8 E1 spans; 20 B-channels) TrunkGroup 1 = 0, 0, 3, *, 1000;(4 E1 spans; all B-channels) [\TrunkGroup] **Notes:** ▪ The parameter TrunkGroup_Module is not applicable. ▪ To represent all B-channels, use an asterisk (*). ▪ For configuring this table in the Web interface, refer to Configuring the Trunk Group Table on page 195. ▪ For a description of *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
DefaultNumber	For a description of this parameter, refer to "DTMF & Dialing Parameters" on page 147.
ChannelSelectMode	For a description of this parameter, refer to "SIP General Parameters" on page 121.
TrunkGroupSettings	This *ini* file table parameter defines rules for port allocation per Trunk Group. If no rule exists, the global rule defined by the parameter ChannelSelectMode takes effect. The format of this parameter is as follows: [TrunkGroupSettings] FORMAT TrunkGroupSettings_**Index** = TrunkGroupSettings_**TrunkGroupId**, TrunkGroupSettings_**ChannelSelectMode**, TrunkGroupSettings_**RegistrationMode**, TrunkGroupSettings_**GatewayName**,TrunkGroupSettings_**ContactUser**, TrunkGroupSettings_**ServingIPGroup**; [\TrunkGroupSettings] For example:

Parameter	Description
	[TrunkGroupSettings] TrunkGroupSettings 0 = 1, 0, 5, audiocodes, user, 1; TrunkGroupSettings 1 = 2, 1, 0, localname, user1, 2; [\TrunkGroupSettings] **Notes:** ▪ This parameter can include up to 240 indices. ▪ For configuring Trunk Group Settings using the Web interface, refer to "Configuring Trunk Group Settings" on page 197. ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
AddTrunkGroupAsPrefix	For a description of this parameter, refer to "Routing General Parameters" on page 171.
AddPortAsPrefix	For a description of this parameter, refer to "Routing General Parameters" on page 171.
ReplaceEmptyDstWithPortNumber	For a description of this parameter, refer to Routing General Parameters on page 171.
CopyDestOnEmptySource	▪ [0] = Leave Source Number empty (default). ▪ [1] = If the Source Number of a Tel-to-IP call is empty, the Destination Number is copied to the Source Number.
AddNPIandTON2CallingNumber	For a description of this parameter, refer to Routing General Parameters on page 171.
AddNPIandTON2CalledNumber	For a description of this parameter, refer to Routing General Parameters on page 171.
UseSourceNumberAsDisplayName	For a description of this parameter, refer to "Routing General Parameters" on page 171.
UseDisplayNameAsSourceNumber	For a description of this parameter, refer to "SIP General Parameters" on page 121.
AlwaysUseRouteTable	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
Prefix	This *ini* file table parameter configures the 'Tel to IP Routing' table for routing Tel-to-IP calls and the 'Outbound IP Routing' table for IP-to-IP calls. The format of this parameter is as follows: [PREFIX] FORMAT PREFIX_**Index** = PREFIX_**DestinationPrefix**, PREFIX_**DestAddress**, PREFIX_**SourcePrefix**, PREFIX_**ProfileId**, PREFIX_**MeteringCode**, PREFIX_**DestPort**, PREFIX_**SrcIPGroupID**, PREFIX_**DestHostPrefix**, PREFIX_**DestIPGroupID**, PREFIX_**SrcHostPrefix**, PREFIX_**TransportType**, PREFIX_**SrcTrunkGroupID**; [\PREFIX] For example: [PREFIX] FORMAT PREFIX_Index = PREFIX_DestinationPrefix, PREFIX_DestAddress, PREFIX_SourcePrefix, PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort, PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_DestIPGroupID, PREFIX_SrcHostPrefix,

Parameter	Description
	PREFIX_TransportType, PREFIX_SrcTrunkGroupID; PREFIX 0 = *, quest, *, 0, 255, $$, -1, , 1, , -1, -1; PREFIX 1 = 20, 10.33.37.77, *, 0, 255, $$, -1, , 2, , 0, -1; PREFIX 2 = 30, 10.33.37.79, *, 1, 255, $$, -1, , -1, , 2, -1; [\PREFIX] **Notes:** ▪ This parameter can include up to 50 indices. ▪ For a description of these parameters, refer to the corresponding Web parameters in "Tel to IP Routing Table" on page 175 or Outbound IP Routing Table on page 178. ▪ The parameter PREFIX_MeteringCode is not applicable. ▪ The destination and source phone prefixes (PREFIX_DestinationPrefix and PREFIX_SourcePrefix respectively) can be a single number or a range of numbers. ▪ Parameters can be skipped using two dollar ($$) symbols, for example: Prefix = $$,10.2.10.2,202,1. ▪ The destination IP address (PREFIX_DestAddress) can be either in dotted-decimal notation or FQDN. If an FQDN is used, DNS resolution is performed according to DNSQueryType. ▪ If the string 'ENUM' is specified for the destination IP address, an ENUM query containing the destination phone number is sent to the DNS server. The ENUM reply includes a SIP URI used as the Request-URI in the outgoing INVITE and for routing (if Proxy is not used). ▪ The IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g., 10.8.8.xx represents all addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g., 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. ▪ For available notations, refer to "Dialing Plan Notation" on page 168. ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
PSTNPrefix	This *ini* file table parameter configures the routing of IP-to-Tel calls to Trunk Groups or Inbound IP Routing for IP-to-IP calls. The format of this parameter is as follows: [PSTNPrefix] FORMAT PstnPrefix_Index = PstnPrefix_**DestPrefix**, PstnPrefix_**TrunkGroupId**, PstnPrefix_**SourcePrefix,** PstnPrefix_**SourceAddress**, PstnPrefix_**ProfileId**, PstnPrefix_**SrcIPGroupID**, PstnPrefix_**DestHostPrefix**, PstnPrefix_**SrcHostPrefix**; [\PSTNPrefix] For example: [PSTNPrefix] FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId, PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix;

Parameter	Description
	PstnPrefix 0 = 100, 1, 200, *, 0, 2, , ; PstnPrefix 1 = *, 2, *, , 1, 3, acl, joe; [\PSTNPrefix] **Notes:** ▪ This parameter can include up to 24 indices. ▪ For a description of these parameters, refer to the corresponding Web parameters in "IP to Trunk Group Routing Table" on page 181 or Inbound IP Routing Table on page 184 (for IP-to-IP calls). ▪ To support the In-Call Alternative Routing feature, you can use two entries that support the same call, but assigned with a different Trunk Group. The second entry functions as an alternative selection if the first rule fails as a result of one of the release reasons listed in the AltRouteCauseIP2Tel table. ▪ Selection of Trunk Groups (for IP-to-Tel calls) is according to destination number, source number,and source IP address. ▪ The source IP address (SourceAddress) can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 and 10.8.8.99. ▪ The source IP address (SourceAddress) can include the asterisk ('*') wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. ▪ If the source IP address (SourceAddress) includes an FQDN, DNS resolution is performed according to DNSQueryType. ▪ For available notations that represent multiple numbers, refer to "Dialing Plan Notation" on page 168. ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
RemovePrefix	For a description of this parameter, refer to "Routing General Parameters" on page 171.
RouteModeIP2Tel	For a description of this parameter, refer to "IP to Trunk Group Routing" on page 181.
RouteModeTel2IP	For a description of this parameter, refer to "Tel to IP Routing Table" on page 175.
SwapRedirectNumber	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
Prefix2RedirectNumber	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
SourceManipulationMode	Determines the SIP headers containing the source number after manipulation: ▪ **[0]** = Both SIP From and P-Asserted-Id headers contain the source number after manipulation (default). ▪ **[1]** = Only SIP From header contains the source number after manipulation, while the P-Asserted-Id header contains the source number before manipulation.

Parameter	Description
SwapTel2IPCalled&CallingNumbers	If enabled, the device swaps the calling and called numbers received from the Tel side. The INVITE message contains the swapped numbers. Applicable for Tel-to-IP calls. ▪ **[0]** = Disabled (default) ▪ **[1]** = Swap calling and called numbers
AddTON2RPI	For a description of this parameter, refer to "SIP General Parameters" on page 121.
NumberMapTel2IP	This *ini* file table parameter manipulates the destination number of Tel-to-IP calls. The format of this parameter is as follows: [NumberMapTel2Ip] FORMAT NumberMapTel2Ip_Index = NumberMapTel2Ip_**DestinationPrefix**, NumberMapTel2Ip_**SourcePrefix**, NumberMapTel2Ip_**SourceAddress**, NumberMapTel2Ip_**NumberType**, NumberMapTel2Ip_**NumberPlan**, NumberMapTel2Ip_**RemoveFromLeft**, NumberMapTel2Ip_**RemoveFromRight**, NumberMapTel2Ip_**LeaveFromRight**, NumberMapTel2Ip_**Prefix2Add**, NumberMapTel2Ip_**Suffix2Add**, NumberMapTel2Ip_**IsPresentationRestricted**, NumberMapTel2Ip_**SrcTrunkGroupID**, NumberMapTel2Ip_ **SrcIPGroupID**; [\NumberMapTel2Ip] For example: [NumberMapTel2Ip] NumberMapTel2Ip 0 = 01,$$,*,0,0,2,$$,$$,971,$$,$$,$$,$$; NumberMapTel2Ip 1 = 10,10,*,255,255,3,0,5,100,$$,255,$$,$$; [\NumberMapTel2Ip] **Notes:** ▪ This table parameter can include up to 100 indices. ▪ The parameters SourceAddress and IsPresentationRestricted are not applicable. Set these to $$. ▪ The parameter RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and NumberPlan are applied if the called and calling numbers match the DestinationPrefix and SourcePrefix conditions. ▪ The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. ▪ Parameters can be skipped by using two dollar signs ('$$'). ▪ Number Plan and Type can optionally be used in Remote Party ID (RPID) header by using the EnableRPIHeader and AddTON2RPI parameters. ▪ To configure manipulation of destination numbers for Tel-to-IP calls using the Web interface, refer to "Configuring the Number Manipulation Tables" on page 164). ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

Parameter	Description
NumberMapIP2Tel	This *ini* file table parameter manipulates the destination number of IP-to-Tel calls. The format of this parameter is as follows: [NumberMapIp2Tel] FORMAT NumberMapIp2Tel_**Index** = NumberMapIp2Tel_**DestinationPrefix**, NumberMapIp2Tel_**SourcePrefix**, NumberMapIp2Tel_**SourceAddress**, NumberMapIp2Tel_**NumberType**, NumberMapIp2Tel_**NumberPlan**, NumberMapIp2Tel_**RemoveFromLeft**, NumberMapIp2Tel_**RemoveFromRight**, NumberMapIp2Tel_**LeaveFromRight**, NumberMapIp2Tel_**Prefix2Add**, NumberMapIp2Tel_**Suffix2Add**, NumberMapIp2Tel_**IsPresentationRestricted**; [\NumberMapIp2Tel] For example: [NumberMapIp2Tel] NumberMapIp2Tel 0 = 01,034,10.13.77.8,$$,0,$$,2,$$,667,$$; NumberMapIp2Tel 1 = 10,10,1.1.1.1,255,255,3,0,5,100,$$,255; [\NumberMapIp2Tel] **Notes:** ▪ This table parameter can include up to 100 indices. ▪ The parameter NumberMapIp2Tel_IsPresentationRestricted is not applicable. Set its value to $$. ▪ RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and NumberPlan are applied if the called and calling numbers match the DestinationPrefix, SourcePrefix, and SourceAddress conditions. ▪ The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. ▪ Parameters can be skipped using two dollar signs ('$$'). ▪ The Source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all addresses between 10.8.8.10 and 10.8.8.99. ▪ The Source IP address can include the asterisk ('*') wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255. ▪ To configure manipulation of destination numbers for IP-to-Tel calls using the Web interface, refer to "Configuring the Number Manipulation Tables" on page 164). ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

Parameter	Description
SourceNumberMapTel2IP	This *ini* file table parameter manipulates the source phone number for Tel-to-IP calls. The format of this parameter is as follows: [SourceNumberMapTel2Ip] FORMAT SourceNumberMapTel2Ip_**Index** = SourceNumberMapTel2Ip_**DestinationPrefix**, SourceNumberMapTel2Ip_**SourcePrefix**, SourceNumberMapTel2Ip_**SourceAddress**, SourceNumberMapTel2Ip_**NumberType**, SourceNumberMapTel2Ip_**NumberPlan**, SourceNumberMapTel2Ip_**RemoveFromLeft**, SourceNumberMapTel2Ip_**RemoveFromRight**, SourceNumberMapTel2Ip_**LeaveFromRight**, SourceNumberMapTel2Ip_**Prefix2Add**, SourceNumberMapTel2Ip_**Suffix2Add**, SourceNumberMapTel2Ip_**IsPresentationRestricted**, NumberMapTel2Ip_**SrcTrunkGroupID**, NumberMapTel2Ip_**SrcIPGroupID**; [\SourceNumberMapTel2Ip] For example: [SourceNumberMapTel2Ip] SourceNumberMapTel2Ip 0 = 22,03,$$,0,0,$$,2,$$,667,$$,0,$$,$$; SourceNumberMapTel2Ip 0 = 10,10,*,255,255,3,0,5,100,$$,255,$$,$$; [\SourceNumberMapTel2Ip] **Notes:** ▪ This table parameter can include up to 120 indices. ▪ RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, NumberPlan, and IsPresentationRestricted are applied if the called and calling numbers match the DestinationPrefix and SourcePrefix conditions. ▪ The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. ▪ Parameters can be skipped by using two dollar signs ('$$'). ▪ An asterisk ('*') represents all IP addresses. ▪ IsPresentationRestricted is set to 'Restricted' only if 'Asserted Identity Mode' is set to 'P-Asserted'. ▪ Number Plan and Type can optionally be used in Remote Party ID (RPID) header by using the EnableRPIHeader and AddTON2RPI parameters. ▪ To configure manipulation of source numbers for Tel-to-IP calls using the Web interface, refer to "Configuring the Number Manipulation Tables" on page 164). ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
SourceNumberMapIP2Tel	This *ini* file table parameter manipulates the source number for IP-to-Tel calls. The format of this parameter is as follows: [SourceNumberMapIp2Tel]

Parameter	Description
	FORMAT SourceNumberMapIp2Tel_**Index** = SourceNumberMapIp2Tel_**DestinationPrefix**, SourceNumberMapIp2Tel_**SourcePrefix**, SourceNumberMapIp2Tel_**SourceAddress**, SourceNumberMapIp2Tel_**NumberType**, SourceNumberMapIp2Tel_**NumberPlan**, SourceNumberMapIp2Tel_**RemoveFromLeft**, SourceNumberMapIp2Tel_**RemoveFromRight**, SourceNumberMapIp2Tel_**LeaveFromRight**, SourceNumberMapIp2Tel_**Prefix2Add**, SourceNumberMapIp2Tel_**Suffix2Add**, SourceNumberMapIp2Tel_**IsPresentationRestricted**; [\SourceNumberMapIp2Tel] For example: [SourceNumberMapIp2Tel] SourceNumberMapIp2Tel 0 = 22,03,$$,$$,$$,$$,2,667,$$,$$; SourceNumberMapIp2Tel 1 = 034,01,1.1.1.1,$$,0,2,$$,$$,972,$$,10; [\SourceNumberMapIp2Tel] **Notes:** ▪ RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and NumberPlan are applied if the called and calling numbers match the DestinationPrefix, SourcePrefix, and SourceAddress conditions. ▪ The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. ▪ Parameters can be skipped by using two dollar signs ('$$'). ▪ The Source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all addresses between 10.8.8.10 and 10.8.8.99. ▪ The Source IP address can include the asterisk ('*') wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255. ▪ To configure manipulation of source numbers for IP-to-Tel calls using the Web interface, refer to "Configuring the Number Manipulation Tables" on page 164). ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
For ETSI ISDN variant, the following Number Plan and Type combinations (Plan/Type) are supported in the Destination and Source Manipulation tables: ▪ 0,0 = Unknown, Unknown ▪ 9,0 = Private, Unknown ▪ 9,1 = Private, Level 2 Regional ▪ 9,2 = Private, Level 1 Regional ▪ 9,3 = Private, PISN Specific ▪ 9,4 = Private, Level 0 Regional (local) ▪ 1,0 = Public(ISDN/E.164), Unknown	

Parameter	Description
▪ 1,1 = Public(ISDN/E.164), International ▪ 1,2 = Public(ISDN/E.164), National ▪ 1,3 = Public(ISDN/E.164), Network Specific ▪ 1,4 = Public(ISDN/E.164), Subscriber ▪ 1,6 = Public(ISDN/E.164), Abbreviated For NI-2 and DMS-100 ISDN variants the valid combinations of TON and NPI for calling and called numbers are (Plan/Type): ▪ 0/0 - Unknown/Unknown ▪ 1/1 - International number in ISDN/Telephony numbering plan ▪ 1/2 - National number in ISDN/Telephony numbering plan ▪ 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan ▪ 9/4 - Subscriber (local) number in Private numbering plan	
SecureCallsFromIP	For a description of this parameter, refer to "Advanced Parameters" on page 151.
AltRouteCauseTel2IP	This *ini* file table parameter configures SIP call failure reason values received from the IP side. If a call is released as a result of one of these reasons, the device attempts to locate an alternative route to the call in the 'Tel to IP Routing' table (if Proxy is not used) or used as a redundant Proxy (when Proxy is used). The format of this parameter is as follows: [AltRouteCauseTel2IP] FORMAT AltRouteCauseTel2IP_**Index** = AltRouteCauseTel2IP_**ReleaseCause**; [\AltRouteCauseTel2IP] For example: [AltRouteCauseTel2IP] AltRouteCauseTel2IP 0 = 486; (Busy Here) AltRouteCauseTel2IP 1 = 480; (Temporarily Unavailable) AltRouteCauseTel2IP 2 = 408; (No Response) [\AltRouteCauseTel2IP] **Notes:** ▪ The 408 reason can be used to specify no response from the remote party to the INVITE request. ▪ This parameter can include up to 5 indices. ▪ For defining the Reasons for Alternative Routing table using the Web interface, refer to "Reasons for Alternative Routing" on page 188. ▪ For an explanation on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
AltRouteCauseIP2Tel	This *ini* file table parameter configures call failure reason values received from the PSTN side (in Q.931 presentation). If a call is released as a result of one of these reasons, the device attempts to locate an alternative Trunk Group for the call in the 'IP to Trunk Group Routing' table. The format of this parameter is as follows: [AltRouteCauseIP2Tel] FORMAT AltRouteCauseIP2Tel_**Index** =

Parameter	Description
	AltRouteCauseIP2Tel_**ReleaseCause**; [\AltRouteCauseIP2Tel] For example: [AltRouteCauseIP2Tel] AltRouteCauseIP2Tel 0 = 3 (No Route to Destination) AltRouteCauseIP2Tel 1 = 1 (Unallocated Number) AltRouteCauseIP2Tel 2 = 17 (Busy Here) [\AltRouteCauseIP2Tel] **Notes:** ▪ This parameter can include up to 5 indices. ▪ If the device fails to establish a call to the PSTN because it has no available channels in a specific trunk group (e.g., all trunk group's channels are occupied, or the trunk group's spans are disconnected or out of sync), it uses the Internal Release Cause '3' (No Route to Destination). This cause can be used in the AltRouteCauseIP2Tel table to define routing to an alternative trunk group. ▪ For defining the Reasons for Alternative Routing table using the Web interface, refer to "Reasons for Alternative Routing" on page 188. ▪ For an explanation on usng *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.
EnableETSIDiversion	Defines the method in which the Redirect Number is passed toward the Tel side. ▪ **[0]** = Q.931 Redirecting Number Information Element (IE) (default) ▪ **[1]** = ETSI DivertingLegInformation2 in a Facility IE
CopyDest2RedirectNumber	For a description of this parameter, refer to “Configuring the Digital Gateway Parameters” on page 207.
FilterCalls2IP	For a description of this parameter, refer to "Advanced Parameters" on page 151.
Alternative Routing Parameters	
RedundantRoutingMode	For a description of this parameter, refer to "Proxy & Registration Parameters" on page 132.
AltRoutingTel2IPEnable	For a description of this parameter, refer to "Routing General Parameters" on page 171.
AltRoutingTel2IPMode	For a description of this parameter, refer to "Routing General Parameters" on page 171.
AltRoutingTel2IPConnMethod	For a description of this parameter, refer to "Routing General Parameters" on page 171.
AltRoutingTel2IPKeepAliveTime	For a description of this parameter, refer to "Routing General Parameters" on page 171.
IPConnQoSMaxAllowedPL	For a description of this parameter, refer to "Routing General Parameters" on page 171.
IPConnQoSMaxAllowedDelay	For a description of this parameter, refer to "Routing General Parameters" on page 171.

Parameter	Description
Phone-Context Parameters	
AddPhoneContextAsPrefix	For a description of this parameter, refer to "Mapping NPI/TON to Phone-Context" on page 170.
PhoneContext	This *ini* file table parameter defines the Phone Context table. The format for this parameter is as follows: [PhoneContext] FORMAT PhoneContext_**Index** = PhoneContext_**Npi**, PhoneContext_**Ton**, PhoneContext_**Context**; [\PhoneContext] Where, ▪ Npi = Number Plan. ▪ Ton = Type of Number. ▪ Context = Phone-Context value. When a call is received from the ISDN, the NPI and TON are compared to the table, and the Phone-Context value is used in the outgoing SIP INVITE message. The same mapping occurs when an INVITE with a Phone-Context attribute is received. The Phone-Context parameter appears in the standard SIP headers where a phone number is used (Request-URI, To, From, Diversion). For example: [PhoneContext] PhoneContext 0 = 0,0,unknown.com PhoneContext 1 = 1,1,host.com PhoneContext 2 = 9,1,na.e164.host.com [\PhoneContext] **Notes:** ▪ This parameter can include up to 20 indices. ▪ Several entries with the same NPI-TON or Phone-Context are allowed. In this scenario, a Tel-to-IP call uses the first match. ▪ Phone-Context '+' is a unique as it doesn't appear in the Request-URI as a Phone-Context parameter. Instead, it's added as a prefix to the phone number. The '+' isn't removed from the phone number in the IP-to-Tel direction. ▪ To configure the Phone Context table using the Web interface, refer to "Mapping NPI/TON to Phone-Context" on page 170. ▪ For a description on using *ini* file table parameters, refer to "Structure of ini File Table Parameters" on page 257.

4.4.13 Channel Parameters

The channel-related *ini* file configuration parameters are described in the table below. The channel parameters define the DTMF, fax and modem transfer modes.

Table 4-13: Channel ini File Parameters

Parameter	Description
DJBufMinDelay	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
DJBufOptFactor	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
FaxTransportMode	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxRelayEnhancedRedundancyDepth	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxRelayRedundancyDepth	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxRelayMaxRate	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxRelayECMEnable	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxModemBypassCoderType	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
CNGDetectorMode	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxCNGMode	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxModemBypassM	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
FaxModemNTEMode	Determines whether the device sends RFC 2833 ANS/ANSam events upon detection of fax and/or modem answer tones (i.e., CED tone). ▪ **[0]** = Disabled (default). ▪ **[1]** = Enabled. **Note:** This parameter is applicable only when the fax or modem transport type is set to bypass or Transparent-with-Events.
FaxBypassPayloadType	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
CallerIDTransportType	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
ModemBypassPayloadType	Modem Bypass dynamic payload type. The range is 0-127. The default value is 103.
FaxModemRelayVolume	Determines the fax gain control. The range -18 to -3 corresponds to -18 dBm to -3 dBm in 1-dB steps. The default is -6 dBm fax gain control.

Parameter	Description
FaxBypassOutputGain	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
ModemBypassOutputGain	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
T38MaxDatagram	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
T38FaxMaxBufferSize	Defines the maximum size (in bytes) of a T.38 buffer supported by the device. This value is included in the outgoing SDP when T.38 is used for fax relay over IP. The valid range is 100 to 1,024. The default value is 1,024.
DetFaxOnAnswerTone	For a description of this parameter, refer to "SIP General Parameters" on page 121.
NTEMaxDuration	Maximum time for sending Named Telephony Events (NTEs) to the IP side, regardless of the time range when the TDM signal is detected. The range is -1 to 200,000,000 msec (i.e., 55 hours). The default is -1 (i.e., NTE stops only upon detection of an End event).
EchoCancellerAggressiveNLP	Enables or disables the Aggressive NLP at the first 0.5 second of the call. When enabled, the echo is removed only in the first half a second of the incoming IP signal. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
FaxModemBypassBasicRTPPacketInterval	Determines the basic frame size that is used during fax / modem bypass sessions. ▪ **[0]** = Determined internally (default) ▪ **[1]** = 5 msec (not recommended) ▪ **[2]** = 10 msec ▪ **[3]** = 20 msec **Note:** When set for 5 msec (1), the maximum number of simultaneous channels supported is 120.
FaxModemBypassDJBufMinDelay	Determines the Jitter Buffer delay (in milliseconds) during fax and modem bypass session. The range is 0 to 150 msec. The default is 40.
EnableFaxModemInbandNetworkDetection	Enables or disables in-band network detection related to fax/modem. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable When this parameter is enabled on Bypass mode (VxxTransportType = 2), 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. This can be useful when, for example, the payload of voice and bypass is the same, allowing the originator to switch to bypass mode as well.

Parameter	Description
NSEMode	Cisco compatible fax and modem bypass mode. ▪ **[0]** = NSE disabled (default) ▪ **[1]** = NSE enabled **Notes:** ▪ This feature can be used only if VxxModemTransportType = 2 (Bypass). ▪ If NSE mode is enabled, the SDP contains the following line: 'a=rtpmap:100 X-NSE/8000'. ▪ To use this feature: -- The Cisco gateway must include the following definition: 'modem passthrough nse payload-type 100 codec g711alaw'. -- Set the Modem transport type to Bypass mode (VxxModemTransportType = 2) for all modems. -- Configure the gateway parameter NSEPayloadType = 100. In NSE bypass mode, the device starts using G.711 A-Law (default) or G.711μ-Law according to the parameter FaxModemBypassCoderType. The payload type used with these G.711 coders is a standard one (8 for G.711 A-Law and 0 for G.711 μ-Law). The parameters defining payload type for the 'old' AudioCodes' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass. The bypass packet interval is selected according to the parameter FaxModemBypassBasicRtpPacketInterval.
NSEPayloadType	NSE payload type for Cisco Bypass compatible mode. The valid range is 96-127. The default value is 105. **Note:** Cisco gateways usually use NSE payload type of 100.
V21ModemTransportType	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
V22ModemTransportType	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
V23ModemTransportType	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
V32ModemTransportType	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
V34ModemTransportType	For a description of this parameter, refer to "Configuring the Fax / Modem / CID Settings" on page 67.
V34FaxTransportType	Determines the V.34 fax transport method. ▪ **[0]** = Transparent ▪ **[1]** = Relay (default) ▪ **[2]** = Bypass ▪ **[3]** = Transparent with Events

Parameter	Description
UserDefinedToneDetectorEnable	Enables or disables detection of User Defined Tones signaling. - **[0]** = Disable (default) - **[1]** = Enable
BellModemTransportType	Determines the Bell modem transport method. - **[0]** = Transparent (default). - **[2]** = Bypass. - **[3]** = Transparent with events.
InputGain	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
VoiceVolume	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
RTPRedundancyDepth	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
RFC2198PayloadType	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
EnableSilenceCompression	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
IsCiscoSCEMode	Determines whether a Cisco gateway exists at the remote side. - **[0]** = No Cisco gateway exists at the remote side (default). - **[1]** = A Cisco gateway exists at the remote side. When there is a Cisco gateway at the remote side, the device must set the value of the 'annexb' parameter of the fmtp attribute in the SDP to 'no'. This logic is used if EnableSilenceCompression = 2 (enable without adaptation). In this case, Silence Suppression is used on the channel, but not declared in the SDP. **Note:** The IsCiscoSCEMode parameter is only relevant when the selected coder is G.729.
EnableEchoCanceller	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
MaxEchoCancellerLength	For a description of this parameter, refer to “Configuring the General Media Settings” on page 78.
ECNLPMode	Defines the echo cancellation Non-Linear Processing (NLP) mode. - **[0]** = NLP adapts according to echo changes (default). - **[1]** = Disables NLP.
EchoCancellerAggressiveNLP	Enables or disables the Aggressive Non-Linear Processor (NLP) in the first 0.5 second of the call. - **[0]** = Disabled (default) - **[1]** = Enabled
EnableNoiseReduction	Enables / disables the DSP Noise Reduction mechanism. - **[0]** = Disable (default). - **[1]** = Enable. **Note:** When this parameter is enabled the channel capacity might be reduced.

Parameter	Description
EnableStandardSIDPayloadType	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
ComfortNoiseNegotiation	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
RTPSIDCoeffNum	Determines the number of spectral coefficients added to an SID packet being sent according to RFC 3389. Valid only if EnableStandardSIDPayloadType is set to 1. The valid values are **[0]** (default), **[4]**, **[6]**, **[8]** and **[10]**.
DTMFVolume	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
DTMFGenerationTwist	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
DTMFInterDigitInterval	Time in msec between generated DTMF digits to PSTN side (if TxDTMFOption = 1, 2 or 3). The default value is 100 msec. The valid range is 0 to 32767.
DTMFDigitLength	Time (in msec) for generating DTMF tones to the PSTN side (if TxDTMFOption = 1, 2 or 3). It also configures the duration that is sent in INFO (Cisco) messages. The valid range is 0 to 32767. The default value is 100.
RxDTMFHangOverTime	Defines the Voice Silence time (in msec units) after playing DTMF or MF digits to the Tel / PSTN side that arrive as Relay from the IP side. Valid range is 0 to 2,000 msec. The default is 1,000 msec.
TxDTMFHangOverTime	Defines the Voice Silence time (in msec) after detecting the end of DTMF or MF digits at the Tel / PSTN side when the DTMF Transport Type is either Relay or Mute. Valid range is 0 to 2,000 msec. The default is 1,000 msec.
DTMFTransportType	For a description of this parameter, refer to "Configuring the Voice Settings" on page 66.
RFC2833PayloadType	For a description of this parameter, refer to "DTMF & Dialing Parameters" on page 147.
R1DetectionStandard	Determines the R1 MF protocol used for detection. ▪ **[0]** = ITU (default) ▪ **[1]** = R1.5
UserDefinedToneDetectorEnable	Enables or disables detection of User Defined Tones signaling. ▪ **[0]** = Disable ▪ **[1]** = Enable
UDTDetectorFrequencyDeviation	Defines the deviation (in Hz) allowed for the detection of each signal frequency. The valid range is 1 to 50. The default value is 50.
CPTDetectorFrequencyDeviation	Defines the deviation (in Hz) allowed for the detection of each CPT signal frequency. The valid range is 1 to 30. The default value is 10.

Parameter	Description
MGCPDTMFDetectionPoint	▪ **[0]** = DTMF event is reported on the end of a detected DTMF digit. ▪ **[1]** = DTMF event is reported on the start of a detected DTMF digit (default).
KeyBlindTransfer	Keypad sequence that activates blind transfer for Tel-to-IP calls. There are two possible scenarios: ▪ **Option 1:** After this sequence is dialed, the current call is put on hold (using Re-INVITE), a dial tone is played to the B-channel, and then phone number collection starts. ▪ **Option 2:** A Hook-Flash is pressed, the current call is put on hold, a dial tone is played to the B-channel, and then digit collection starts. After this sequence is identified, the device continues the collection of the destination phone number. For both options, after the phone number is collected, it's sent to the transferee in a SIP REFER request (without a Replaces header). The call is then terminated and a confirmation tone is played to the B-channel. If the phone number collection fails due to a mismatch, a reorder tone is played to the B-channel. **Note:** It is possible to configure whether the KeyBlindTransfer code is added as a prefix to the dialed destination number, by using the parameter KeyBlindTransferAddPrefix.
KeyBlindTransferAddPrefix	Determines whether the device adds the Blind Transfer code (KeyBlindTransfer) to the dialed destination number. ▪ **[0]** Disable (default). ▪ **[1]** Enable.
VoicePayloadFormat	Determines the bit ordering of the G.726/G.727 voice payload format. ▪ **[0]** = Little Endian (default) ▪ **[1]** = Big Endian **Note:** To ensure high voice quality when using G.726/G.727, both communicating ends should use the same endianness format. Therefore, when the device communicates with a third-party entity that uses the G.726/G.727 voice coder and voice quality is poor, change the settings of this parameter (between Big Endian and Little Endian).
VQMonEnable	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
VQMonBurstHR	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
VQMonDelayTHR	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
VQMonEOCRValTHR	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
VQMonGMin	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.
RTCPInterval	For a description of this parameter, refer to “Configuring the RTP / RTCP Settings” on page 71.

Parameter	Description
DisableRTCPRandomize	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
RTCPXRESCTransportType	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the RTCP-XR Collection Server. ▪ **[-1]** Not Configured (default) ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When set to 'Not Configured', the value of the parameter SIPTransportType is used.
RTCPXREscIP	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.
RTCPXRReportMode	For a description of this parameter, refer to "Configuring the RTP / RTCP Settings" on page 71.

4.4.14 Auxiliary / Configuration Files Parameters

The configuration files (i.e., auxiliary files) can be loaded to the device using the Web interface or a TFTP session (refer to "Auxiliary Files" on page 231). Before you load them to the device, you need to specify these files in the *ini* file and whether they must be stored in the non-volatile memory. The table below lists the *ini* file parameters associated with these auxiliary files:

Table 4-14: Auxiliary / Configuration ini File Parameters

Parameter	Description
CallProgressTonesFilename	The name of the file containing the Call Progress Tones definitions. Refer to the *Product Reference Manual* for additional information on how to create and load this file.
CASFileName	This is the name of the file containing specific CAS protocol definition (such as 'E_M_WinkTable.dat'). These files are provided to support various types of CAS signaling.
CASFileName_x	CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol. It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device trunks using the parameter CASTableIndex_x.
CASTablesNum	Number 1 to 8. Specifies how many CAS configuration files are loaded.
VoicePromptsFileName	The name (and path) of the file containing the Voice Prompts definitions. Refer to the Product Reference Manual for additional information on how to create and load this file.
PrerecordedTonesFileName	The name (and path) of the file containing the Prerecorded Tones.
CasTrunkDialPlanName	The Dial Plan name (up to 11-character strings) that is used on the specific trunk.

Parameter	Description
DialPlanFileName	The name (and path) of the file containing dial-plan configuration for CAS and SIP protocols. This file should be constructed using the TrunkPack Conversion Utility (refer to the Product Reference Manual) supplied as part of the software package on the CD accompanying the device.
UserInfoFileName	The name (and path) of the file containing the User Information data.
SetDefaultOnIniFileProcess	Determines if all the device's parameters are set to their defaults before processing the updated *ini* file. ▪ **[0]** Disable - parameters not included in the downloaded *ini* file are not returned to default settings (i.e., retain their current settings). ▪ **[1]** Enable (default)
SaveConfiguration	Determines if the device's configuration (parameters and files) is saved to flash (non-volatile memory). ▪ **[0]** = Configuration isn't saved to flash memory. ▪ **[1]** = Configuration is saved to flash memory (default).

5 Default Settings

You can restore the device's factory default settings or define your own default settings for the device.

5.1 Defining Default Settings

The device is shipped with factory default configuration values stored on its non-volatile memory (flash). However, you can define your own default values instead of using the factory defaults. This is performed using an *ini* file that includes the header '[ClientDefaults]'. Below this header, simply define new default values for the required *ini* file parameters. The parameters are defined in the same format as in the standard *ini* file, and loaded to the device using TFTP (i.e., not via the Web interface).

An example of a ClientsDefault *ini* file for defining default values for Syslog server parameters is shown below:

```
[ClientDefaults]
EnableSyslog = 1
SyslogServerIP = 10.13.2.20
```

➢ To define default values for device parameters, take these 2 steps:

1. Configure the ClientDefaults *ini* file with new default parameter values, as required.
2. Load the ClientDefaults *ini* file to the device, using TFTP (refer to the *Product Reference Manual*).

➢ To remove user-defined defaults and restore factory default values, take this step:

- Load an empty (i.e., without any parameters) ClientDefaults *ini* file to the device, using TFTP.

5.2 Restoring Factory Defaults

You can restore all or most of the device's configuration settings to default settings:

- Restoring default settings except for the device's IP address and Web interface's login user name and password: Load to the device an empty *ini* file (without any parameters or with a semicolon (;) preceding all lines). When a parameter is absent from a loaded *ini* file, the default value is assigned to that parameter (according to the *cmp* file loaded to the device) and saved to the non-volatile memory (thereby, overriding the value previously defined for that parameter).
- Restoring all default settings, including the device's IP address and Web interface's login user name and password: Use the device's hardware Reset button (refer to the device's *Installation Manual*).

Reader’s Notes

6 Auxiliary Configuration Files

This section describes the auxiliary files (with the *dat* file extension), which are loaded, in addition to the *ini* file, to the device. You can load the auxiliary files to the device using one of the following methods:

- Web interface (refer to "Loading Auxiliary Files" on page 231)
- *ini* file: specify the name of the relevant auxiliary file in the device's *ini* file and then load the *ini* file to the device (refer to "Loading Auxiliary Files" on page 231).

6.1 Configuring the Call Progress Tones File

The Call Progress Tones (CPT) auxiliary file used by the device is a binary file (with file extension *dat*). This file contains the definitions of the Call Progress Tones (levels and frequencies) that are detected / generated by the device.

You can either use one of the supplied device auxiliary (*dat*) files or create your own file. To create your own auxiliary file, it's recommended to modify the supplied *usa_tone.ini* file (in any standard text editor) to suit your specific requirements, and to convert the modified *ini* file into binary format using the TrunkPack Downloadable Conversion Utility. For the description of the procedure on how to convert CPT *ini* file into a binary *dat* file, refer to the *Product Reference Manual*.

To load the Call Progress Tones *(dat*) file to the device, use the Web interface or *ini* file (refer to "Loading Auxiliary Files" on page 231).

Note: Only the *dat* file can be loaded to the device.

You can create up to 32 different Call Progress Tones, each with frequency and format attributes. The frequency attribute can be single or dual-frequency (in the range of 300 to 1980 Hz), or an Amplitude Modulated (AM). In total, up to 64 different frequencies are supported. Only eight AM tones, in the range of 1 to 128 kHz, can be configured (the detection range is limited to 1 to 50 kHz). Note that when a tone is composed of a single frequency, the second frequency field must be set to zero.

The format attribute can be one of the following:

- **Continuous:** (e.g., dial tone) a steady non-interrupted sound. Only the 'First Signal On time' should be specified. All other on and off periods must be set to zero. In this case, the parameter specifies the detection period. For example, if it equals 300, the tone is detected after 3 seconds (300 x 10 msec). The minimum detection time is 100 msec.
- **Cadence:** A repeating sequence of on and off sounds. Up to four different sets of on / off periods can be specified.
- **Burst:** A single sound followed by silence. Only the 'First Signal On time' and 'First Signal Off time' should be specified. All other on and off periods must be set to zero. The burst tone is detected after the off time is completed.

You can specify several tones of the same type. These additional tones are used only for tone detection. Generation of a specific tone conforms to the first definition of the specific tone. For example, you can define an additional dial tone by appending the second dial tone's definition lines to the first tone definition in the *ini* file. The device reports dial tone detection if either of the two tones is detected.

The Call Progress Tones section of the *ini* file comprises the following segments:

- **[NUMBER OF CALL PROGRESS TONES]:** Contains the following key: 'Number of Call Progress Tones' defining the number of Call Progress Tones that are defined in the file.
- **[CALL PROGRESS TONE #X]:** containing the Xth tone definition (starting from 1 and not exceeding the number of Call Progress Tones defined in the first section) using the following keys:
    - **Tone Type:** Call Progress Tone types:
        - **[1]** Dial Tone
        - **[2]** Ringback Tone
        - **[3]** Busy Tone
        - **[7]** Reorder Tone
        - **[8]** Confirmation Tone (Applicable only to Analog devices)
        - **[9]** Call Waiting Tone (Applicable only to Analog devices)
        - **[15]** Stutter Dial Tone (Applicable only to Analog devices)
        - **[16]** Off Hook Warning Tone (Applicable only to Analog devices)
        - **[17]** Call Waiting Ringback Tone
        - **[23]** Hold Tone
    - **Tone Modulation Type:** Either Amplitude Modulated (1) or regular (0).
    - **Tone Form:** The tone's format can be one of the following:
        - Continuous (1)
        - Cadence (2)
        - Burst (3)
    - **Low Freq [Hz]:** frequency (in Hz) of the lower tone component in case of dual frequency tone, or the frequency of the tone in case of single tone. This is not relevant to Amplitude Modulated (AM) tones.
    - **High Freq [Hz:** frequency (in Hz) of the higher tone component in case of dual frequency tone, or zero (0) in case of single tone (not relevant to AM tones).
    - **Low Freq Level [-dBm]:** generation level 0 dBm to -31 dBm in dBm (not relevant to AM tones).
    - **High Freq Level:** generation level. 0 to -31 dBm. The value should be set to 32 in the case of a single tone (not relevant to AM tones).
    - **First Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the first cadence on-off cycle. For be continuous tones, this parameter defines the detection period. For burst tones, 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 tones). For burst tones, this parameter defines the off time required after the burst tone ends and the tone detection is reported. For continuous tones, this parameter is ignored.
    - **Second Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
    - **Second Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
    - **Third Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the third cadence ON-OFF cycle. Can be omitted if there isn't a third cadence.

- **Third Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the third cadence ON-OFF cycle. Can be omitted if there isn't a third cadence.
- **Fourth Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the fourth cadence ON-OFF cycle. Can be omitted if there isn't a fourth cadence.
- **Fourth Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the fourth cadence ON-OFF cycle. Can be omitted if there isn't a fourth cadence.
- **Carrier Freq [Hz]:** frequency of the carrier signal for AM tones.
- **Modulation Freq [Hz]:** frequency of the modulated signal for AM tones (valid range from 1 to 128 Hz).
- **Signal Level [-dBm]:** level of the tone for AM tones.
- **AM Factor [steps of 0.02]:** amplitude modulation factor (valid range from 1 to 50. Recommended values from 10 to 25).

Notes:

- When the same frequency is used for a continuous tone and a cadence tone, the 'Signal On Time' parameter of the continuous tone must 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.
- The tones frequency should differ by at least 40 Hz from one tone to other defined tones.

For example, to configure the dial tone to 440 Hz only, enter the following text:

```
#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 (-10 dBm)
High Freq Level [-dBm]=32 (use 32 only if a single tone is
required)
First Signal On Time [10msec]=300; the dial tone is detected after
3 sec
First Signal Off Time [10msec]=0
Second Signal On Time [10msec]=0
Second Signal Off Time [10msec]=0
```

6.2 Prerecorded Tones (PRT) File

The Call Progress Tones (CPT) mechanism has several limitations such as a limited number of predefined tones and a limited number of frequency integrations in one tone. To overcome these limitations and provide tone generation capability that is more flexible, the Prerecorded Tones (PRT) file can be used. If a specific prerecorded tone exists in the PRT file, it takes precedence over the same tone that exists in the CPT file and is played instead of it.

Note: The Prerecorded tones are used only for generation of tones. Detection of tones is performed according to the CPT file.

The PRT is a **.dat* file containing a set of prerecorded tones that can be played by the device. Up to 40 tones (totaling approximately 10 minutes) can be stored in a single PRT file on the device's flash memory. The prerecorded tones are prepared offline using standard recording utilities (such as CoolEdit™) and combined into a single file using AudioCodes' TrunkPack Downloadable Conversion utility (refer to the *Product Reference Manual*).

The raw data files must be recorded with the following characteristics:

- **Coders:** G.711 A-law or G.711 µ-law
- **Rate:** 8 kHz
- **Resolution:** 8-bit
- **Channels:** mono

The generated PRT file can then be loaded to the device using AudioCodes' BootP/TFTP utility or the Web interface (refer to "Loading Auxiliary Files" on page 231).

The prerecorded tones are played repeatedly. This allows you to record only part of the tone and then play the tone for the full duration. For example, if a tone has a cadence of 2 seconds on and 4 seconds off, the recorded file should contain only these 6 seconds. The PRT module repeatedly plays this cadence for the configured duration. Similarly, a continuous tone can be played by repeating only part of it.

6.3 Voice Prompts File

The voice announcement file contains a set of Voice Prompts that can be played by the device during operation. The voice announcements are prepared offline using standard recording utilities and combined into a single file using the TrunkPack Downloadable Conversion Utility. The generated announcement file can then be loaded to the device using the BootP/TFTP utility (refer to the *Product Reference Manual*).

If the size of the combined Voice Prompts file is less than 1 MB, it can permanently be stored on flash memory. Larger files, up to 10 MB, are stored in RAM, and should be loaded again (using BootP/TFTP utility) after the device is reset.

The Voice Prompts integrated file is a collection of raw voice recordings and / or *wav* files. These recordings can be prepared using standard utilities such as CoolEdit, Goldwave™ and others. The raw voice recordings must be sampled at 8000 kHz / mono / 8 bit. The *wav* files must be recorded with G.711µ-Law/A-Law/Linear.

When the list of recorded files is converted to a single *voiceprompts.dat* file, every Voice Prompt is tagged with an ID number, starting with '1'. This ID is used later by the device to start playing the correct announcement. Up to 1,000 Voice Prompts can be used.

AudioCodes provides a professionally recorded English (U.S.) Voice Prompts file.

➢ To generate and load the Voice Prompts file, take these 3 steps:

1. Prepare one or more voice files using standard utilities.
2. Use the TrunkPack Downloadable Conversion Utility to generate the *voiceprompts.dat* file from the pre-recorded voice messages (refer to the *Product Reference Manual*).
3. Load the *voiceprompts.dat* file to the device using TFTP (refer to the *Product Reference Manual*) or Web interface (refer to "Loading Auxiliary Files" on page 231).

6.4 CAS Protocol Auxiliary Files

The CAS Protocol auxiliary files contain the CAS Protocol definitions that are used for CAS-terminated trunks. You can either use the supplied files or construct your own files. Up to eight files can be loaded and different files can be assigned to different trunks. The CAS files can be loaded to the device using the Web interface or *ini* file (refer to "Loading Auxiliary Files" on page 231).

Note: All CAS files loaded together must belong to the same Trunk Type (i.e., either E1 or T1).

6.5 Dial Plan File

The source file for the Dial Plan configuration contains a list of known prefixes (e.g. area codes and international telephone number patterns) for the PSTN to which the device is connected. The device uses this information to detect end-of-dialing in certain CAS configurations where the end-indicator (ST) is not used. The device supports up to 8,000 distinct prefixes in the dial-plan file.

The CasTrunkDialPlanName *ini* file parameter determines which Dial Plan (in a Dial Plan file) to use for a specific trunk (refer to "Configuring the Trunk Settings" on page 82). The Dial Plan can be loaded using the Web interface (refer to "Loading Auxiliary Files" on page 231).

The following is an example of an *ini* file that includes these definitions. This *ini* file is converted (using the TrunkPack Conversion Utility - refer to the *Product Reference Manual*) to a binary file and loaded to the device.

```
; Example of dial-plan configuration.
; This file contains two dial plans: you may specify which
; one to use in CAS configuration.
[ PLAN1 ]
; Define the area codes 02, 03, 04.
; In these area codes, phone numbers have 7 digits.
02,7
03,7
04,7
; Define the cellular/VoIP area codes 052, 054, 050, and 077.
; In these area codes, phone numbers have 8 digits.
052,8
054,8
050,8
077,8
; Define the international prefixes 00, 012, 014.
; The number following these prefixes may
; be 7 to 14 digits in length.
00,7-14
012,7-14
014,7-14
; Define the emergency number 911.
; No additional digits are expected.
911,0
[ PLAN2 ]
; Define the area codes 02, 03, 04.
; In these area codes, phone numbers have 7 digits.
0[2-4],7
; Operator services starting with a star: *41, *42, *43.
```

```
        ; No additional digits are expected.
        *4[1-3],0
```

The list must be prepared in a textual *ini* file with the following syntax:

- Every line in the file defines a known dialing prefix and the number of digits expected to follow that prefix. The prefix must be separated from the number of additional digits by a comma (',').
- Empty lines are ignored.
- Lines beginning with a semicolon (';') are ignored.
- Multiple dial plans may be specified in one file; A name in square brackets on a separate line indicates the beginning of a new dial plan. Up to eight dial plans can be defined.
- Asterisks ('*') and number-signs ('#') can be specified as part of the prefix.
- Numeric ranges are allowed in the prefix.
- A numeric range is allowed in the number of additional digits.

Note: The prefixes must not overlap. Attempting to process an overlapping configuration in the TrunkPack Conversion Utility results in an error message specifying the problematic line.

6.6 User Information File

The User Information file is a text file that maps PBX extensions, connected to the device, to global IP numbers. In this context, a global IP phone number (alphanumerical) serves as a routing identifier for calls in the 'IP World'. The PBX extension uses this mapping to emulate the behavior of an IP phone.

Note: The mapping mechanism is disabled by default and must be activated using the parameter EnableUserInfoUsage (refer to "Advanced Parameters" on page 151).

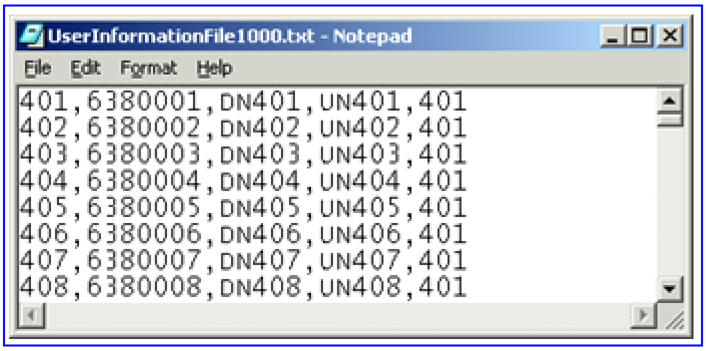
Each line in the file represents a mapping rule of a single PBX extension. Up to 1,000 rules can be configured. Each line includes five items separated with commas. The items are described in the table below:

Table 6-1: User Information Items

Item	Description	Maximum Size (Characters)
PBX extension #	The relevant PBX extension number.	10
Global phone #	The relevant global phone number.	20
Display name	A string that represents the PBX extensions for the Caller ID.	30
Username	A string that represents the user name for SIP registration.	40
Password	A string that represents the password for SIP registration.	20

An example of a User Information file is shown in the figure below:

Figure 6-1: Example of a User Information File



```
401,6380001,DN401,UN401,401
402,6380002,DN402,UN402,401
403,6380003,DN403,UN403,401
404,6380004,DN404,UN404,401
405,6380005,DN405,UN405,401
406,6380006,DN406,UN406,401
407,6380007,DN407,UN407,401
408,6380008,DN408,UN408,401
```

Note: The last line in the User Information file must end with a carriage return (i.e., by pressing the <Enter> key).

The User Information file can be loaded to the device using the *ini* file (UserInfoFileName parameter described in "Auxiliary / Configuration Files Parameters" on page 331), the Web interface (refer to "Loading Auxiliary Files" on page 231), or by using the automatic update mechanism (UserInfoFileURL, refer to the *Product Reference Manual*).

The maximum permissible size of the file is 108,000 bytes.

Each PBX extension registers separately (a REGISTER message is sent for each entry only if AuthenticationMode is set to Per Endpoint) using the IP number in the From / To headers. The REGISTER messages are sent gradually. Initially, the device sends requests according to the maximum number of allowed SIP dialogs (configured by the parameter NumberOfActiveDialogs). After each received response, the subsequent request is sent. Therefore, no more than NumberOfActiveDialogs dialogs are active simultaneously. The user name and password are used for SIP Authentication when required.

The calling number of outgoing Tel-to-IP calls is first translated to an IP number and then (if defined), the manipulation rules are performed. The Display Name is used in the From header in addition to the IP number. The called number of incoming IP-to-Tel calls is translated to a PBX extension only after manipulation rules (if defined) are performed.

Reader’s Notes

7 IP Telephony Capabilities

This section describes the device's IP telephony capabilities.

7.1 IP-to-IP Routing (SIP Trunking)

The AudioCodes device supports IP-to-IP VoIP call routing (or SIP trunking). The device enables Enterprises to seamlessly connect their IP-PBX to a SIP trunk provided by an Internet Telephony Service Provider (ITSP). The Enterprise can communicate with the PSTN through the ITSP, which interfaces directly with PSTN. Alternatively, the device can also provide the interface with the PSTN.

At the same time, the device can also provide an interface with the traditional PSTN network, enabling PSTN fallback in case of IP network failure. In addition, the device supports multiple SIP trunks, whereby if a connection to one ITSP goes down, the call can immediately be transferred to another ITSP. By allowing multiple SIP trunks where each trunk is designated for a specific ITSP, the device can route calls to an ITSP, based on call destination (e.g., country code).

Therefore, in addition to providing VoIP communication within an Enterprise's LAN, the device allows the Enterprise to communicate outside of the corporate LAN, using SIP trunking.

The device interfaces between the Enterprise's IP-PBX and ITSP, allowing SIP trunking implementation by the Enterprise, for example, in the following scenarios:

- VoIP between headquarters and remote offices
- VoIP between Enterprise and PSTN via their ITSP

For a detailed explanation on configuring IP-to-IP call routing, refer to the document *IP-to-IP SIP Call Routing Application Note.*

7.2 Answer Machine Detector (AMD)

Answering Machine Detection can be useful in automatic dialing applications. In some of these applications, it is important to detect if a human voice or answering machine is answering the call. Answering Machine Detection can be activated and de-activated only after a channel is already open. The direction of the detection (PSTN or IP) can be configured (using the parameter AMDDetectionDirection - refer to "Media Server Parameters" on page 300), as well as the detector detection sensitivity using the parameter AMDDetectionSensitivity - refer to "Configuring the IPmedia Settings" on page 76).

Upon every Answering Machine Detection activation, the device can send a SIP INFO message to an Application server, notifying it of one of the following:

- Human voice has been detected
- Answering machine has been detected
- Silence (i.e., no voice detected) has been detected

The table below shows the success rates of the AMD feature for correctly detecting live and fax calls:

Table 7-1: Approximate AMD Detection Sensitivity (Based on North American English)

AMD Detection Sensitivity	**Performance**	
	Success Rate for Live Calls	**Success Rate for Answering Machine**
0 (Best for Answering Machine)	-	-
1	82.56%	97.10%
2	85.87%	96.43%
3 (Default)	88.57%	94.76%
4	88.94%	94.31%
5	90.42%	91.64%
6	90.66%	91.30%
7 (Best for Live Calls)	94.72%	76.14%

A pre-requisite for enabling the AMD feature is to set the *ini* file parameter EnableDSPIPMDetectors to 1. In addition, to enable voice detection, required once the AMD detects the answering machine, the *ini* file parameter EnableVoiceDetection must be set to 1.

Note: The device's AMD feature is based on voice detection for North American English. If you want to implement AMD in a different language or region, you must provide AudioCodes with a database of recorded voices in the language on which the device's AMD mechanism can base its voice detector algorithms for detecting these voices. The data needed for an accurate calibration should be recorded under the following guidelines:

- Statistical accuracy: The number of recordings should be large (i.e., about 100) and varied. The calls must be made to different people, at different times. The calls must be made in the specific location in which the device's AMD mechanism is to operate.
- Real-life recording: The recordings should simulate real-life answering of a person picking up the phone without the caller speaking (until the AMD decision).
- Normal environment interferences: The environment should almost simulate real-life scenarios, i.e., not sterile but not too noisy either. Interferences, for example, could include background noises of other people talking, spikes, and car noises.

The SIP call flows below show an example of implementing the device's AMD feature. This scenario example allows a third-party Application server to play a recorded voice message to an answering machine.

1. Upon detection by the device of the answering machine, the device sends a SIP INFO message to the Application server:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac1566945480
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c1505895240
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29758@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-IPmedia 260 UN/v.5.20A.040.004
Content-Type: application/x-detect
Content-Length: 30
Type= AMD
SubType= AUTOMATA
```

2. The device then detects the start of voice (i.e., the greeting message of the answering machine), and then sends the following to the Application server:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac482466515
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c419779142
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29753@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-IPmedia 260_UN/v.5.20A.040.004
Content-Type: application/x-detect
Content-Length: 34
Type= PTT
SubType= SPEECH-START
```

3. Upon detection of the end of voice (i.e., end of the greeting message of the answering machine), the device sends the Application server the following:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac482466515
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c419779142
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29753@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-IPmedia 260 UN/v.5.20A.040.004
Content-Type: application/x-detect
Content-Length: 34
Type= PTT
SubType= SPEECH-END
```

4. The Application server now sends its message to the answering message.

If the device detects voice and not an answering machine, the SIP INFO message includes:

```
Type= AMD
SubType= VOICE
```

If the device detects silence, the SIP INFO message includes the SubType **SILENT**.

7.3 Stand-Alone Survivability (SAS) Feature

The device's Stand-Alone Survivability (SAS) feature ensures telephony communication continuity (survivability) for enterprises using hosted IP services (such as IP Centrex) or IP-PBX in cases of failure of these entities. In case of failure of the IP Centrex, IP-PBX servers (or even WAN connection and access Internet modem), the enterprise typically loses its internal telephony service at any branch, between its offices, as well as with the external environment. In addition, typically these failures lead to the inability to make emergency calls (e.g., 911 in North America). Despite these possible point of failures, the device's SAS feature ensures that the Enterprise's telephony services (e.g., SIP IP phones or soft phones) are maintained by routing calls to the PSTN (i.e., providing PSTN fallback).

The SAS feature operates in one of two modes:

- **Normal:** Initially, the device's SAS agent serves as a registrar (and outbound Proxy server) to which every VoIP CPE (e.g., IP phones) within the Enterprise's LAN registers. The SAS agent at the same time sends all these registration requests to the Proxy server (e.g., IP-Centrex or IP-PBX). This ensures registration redundancy by the SAS agent for all telephony devices. Therefore, SAS agent functions as a stateful proxy, passing all SIP requests received from the Enterprise to the Proxy and vice versa. In parallel, the SAS agent continuously maintains a keep-alive "handshake" with the Proxy server using SIP OPTIONS or re-INVITE messages.

- **Emergency:** The SAS agent switches to Emergency mode if it detects (from the keep-alive responses) that the connection with the Proxy is lost. This can occur due to Proxy server failure or WAN problems. In this mode, when the connection with the Proxy server is down, the SAS agent controls all internal calls within the Enterprise. In the case of outgoing calls, the SAS agent forwards them to a local VoIP gateway (this can be the device itself or a separate analog or digital gateway). For PSTN fallback, the local VoIP gateway should be equipped with analog (FXO) lines or digital (E1/T1) trunk(s) for PSTN connectivity. In this way, the Enterprise preserves its capability for internal and outgoing calls.

The SAS agent continuously attempts to communicate with the Proxy using the regular keep-alive method. After the connection is re-established, the SAS agent switches to pre-Normal mode. In this mode, the SAS agent maintains all terminations of existing calls while any new SIP call signaling (issued by new INVITE sessions) is transacted to/from the Proxy server. This is accomplished using the SAS agent's database of current active calls. After releasing all calls established during Emergency mode, the SAS agent resumes operating in Normal mode.

For SAS implementation, the primary Proxy server for the VoIP CPE's (e.g., IP phones) is the SAS agent (i.e., the device itself) while the IP Centrex or IP-PBX is defined as the secondary Proxy server. For SAS configuration, the device is composed of two different applications (SAS and Gateway), where each application has its own SIP interface (UDP/TCP/TLS ports).

- Configuring the device to use and operate with the SAS capabilities (refer to "Configuring SAS" on page 347)
- Configuring SAS emergency call routing (refer to "Configuring Emergency Calls" on page 348)

7.3.1 Configuring SAS

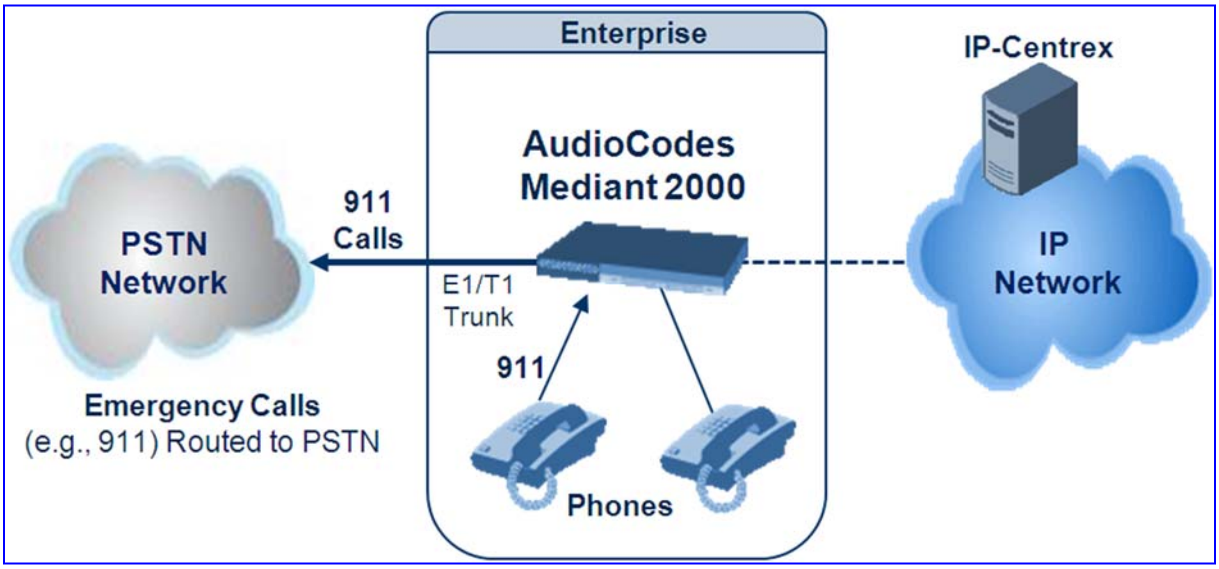
For configuring the device to operate with SAS, perform the following configurations:

- IsProxyUsed = 1
- ProxyIP 0 = <SAS agent's IP address, i.e., the device>
- ProxyIP 1 = <external Proxy server IP address>
- IsRegisterNeeded = 1 (for the device)
- RegistrarIP = ‘ ‘
- SIPDestinationPort = 5080
- IsUserPhone = 0 (don’t use “user=phone” in SIP URL)
- IsUserPhoneInFrom = 0 (don’t use “user=phone” in From Header)
- IsFallbackUsed = 0
- EnableProxyKeepAlive = 1 (enables keep-alive with Proxy using OPTIONS)
- EnableSAS = 1
- SASLocalSIPUDPPort = (default 5080)
- SASRegistrationTime = <expiration time that SAS returns in the 200 OK to REGISTER in Emergency mode> (default 20)
- SASDefaultGatewayIP = < SAS gateway IP address>
- SASProxySet = 1

7.3.2 Configuring Emergency Calls

The device's SAS agent can be configured to detect a user-defined, emergency number (e.g. 911 in North America), which it then redirects the call directly to the PSTN (through its E1/T1 trunk). The emergency number is configured using the *ini* file parameter SASEmergencyNumbers (for a detailed description, refer to "SIP Configuration Parameters" on page 284).

Figure 7-1: Device's SAS Agent Redirecting Emergency Calls to PSTN



To configure support for emergency calls, configure the parameters below. The device and the SAS feature are configured independently. If the device and the SAS agent use different proxies, then the device's proxy server is defined using the 'Use Default Proxy' parameter, while the SAS proxy agent is defined using the 'Proxy Set' table and SASProxySet parameter.

- EnableSAS = 1
- SASLocalSIPUDPPort = (default 5080)
- IsProxyUsed = 1
- ProxyIP 0 = <external proxy IP address (device)>
- ProxyIP 1 = <external proxy IP address (SAS)>
- IsRegisterNeeded = 1 (for the device)
- IsFallbackUsed = 0
- SASRegistrationTime = <expiration time that SAS returns in the 200 OK to REGISTER in Emergency mode> (default 20)
- SASDefaultGatewayIP = < SAS gateway IP address>
- SASProxySet = 1

7.4 Configuring the DTMF Transport Types

You can control the way DTMF digits are transported over the IP network to the remote endpoint, by using one of the following modes:

- **Using INFO message according to Nortel IETF draft:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:

  - RxDTMFOption = 0 (*ini* file); 'Declare RFC 2833 in SDP' field = 'No' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  - TxDTMFOption = 1 (*ini* file); '1st to 5th Tx DTMF Option' field = 'INFO (Nortel)' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  Note that in this mode, DTMF digits are erased from the audio stream [DTMFTransportType is automatically set to 0 ('DTMF Transport Type' field = 'DTMF Mute' -- Web interface)].

- **Using INFO message according to Cisco's mode:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:

  - RxDTMFOption = 0 (*ini* file); 'Declare RFC 2833 in SDP' field = 'No' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  - TxDTMFOption = 3 (*ini* file); '1st to 5th Tx DTMF Option' field = 'INFO (Cisco)' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0 ('DTMF Transport Type' field = 'DTMF Mute' -- Web interface)].

- **Using NOTIFY messages according to <draft-mahy-sipping-signaled-digits-01.txt>**: DTMF digits are carried to the remote side using NOTIFY messages. To enable this mode, define the following:

  - RxDTMFOption = 0 (*ini* file); 'Declare RFC 2833 in SDP' field = 'No' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  - TxDTMFOption = 2 (*ini* file); '1st to 5th Tx DTMF Option' field = 'NOTIFY' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0 ('DTMF Transport Type' field = 'DTMF Mute' -- Web interface)].

- **Using RFC 2833 relay with Payload type negotiation:** DTMF digits are carried to the remote side as part of the RTP stream in accordance with RFC 2833 standard. To enable this mode, define the following:

  - RxDTMFOption = 3 (*ini* file); 'Declare RFC 2833 in SDP' field = 'Yes' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  - TxDTMFOption = 4 (*ini* file); '1st to 5th Tx DTMF Option' field = 'RFC 2833' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  Note that to set the RFC 2833 payload type with a different value (other than its default, 96) configure the RFC2833PayloadType (RFC 2833 Payload Type) parameter. The device negotiates the RFC 2833 payload type using local and remote SDP and sends packets using the payload type from the received SDP. The device expects to receive RFC 2833 packets with the same payload type as configured by the RFC2833PayloadType parameter. If the remote side doesn't include 'telephony-event' in its SDP, the device sends DTMF digits in transparent mode (as part of the voice stream).

- **Sending DTMF digits (in RTP packets) as part of the audio stream (DTMF Relay is disabled):** This method is typically used with G.711 coders; with other low-bit rate (LBR) coders, the quality of the DTMF digits is reduced. To enable this mode, define the following:
  - RxDTMFOption = 0 (*ini* file); 'Declare RFC 2833 in SDP' field = 'No' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)
  - TxDTMFOption = 0 (*ini* file); '1st to 5th Tx DTMF Option' field = 'Disable' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)
  - DTMFTransportType = 2 (DTMF Transport Type = Transparent DTMF)
- **Using INFO message according to Korea mode:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:
  - RxDTMFOption = 0 (*ini* file); 'Declare RFC 2833 in SDP' field = 'No' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)
  - TxDTMFOption = 3 (*ini* file); '1st to 5th Tx DTMF Option' field = 'INFO (Korea)' (Web interface -- refer to "DTMF & Dialing Parameters" on page 147)

  Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0 (DTMF Mute)).

Notes:

- The device is always ready to receive DTMF packets over IP in all possible transport modes: INFO messages, NOTIFY, and RFC 2833 (in proper payload type) or as part of the audio stream.
- To exclude RFC 2833 Telephony event parameter from the device's SDP, set RxDTMFOption to 0 in the *ini* file.

The following parameters affect the way the device handles the DTMF digits:

- TxDTMFOption, RxDTMFOption, and RFC2833PayloadType (described in "DTMF & Dialing Parameters" on page 147)
- MGCPDTMFDetectionPoint, DTMFVolume, DTMFTransportType, DTMFDigitLength, and DTMFInterDigitInterval (refer to "Channel Parameters" on page 324)

7.5 Fax and Modem Capabilities

7.5.1 Fax/Modem Operating Modes

The device supports two modes of operations:

- Fax / modem negotiation that isn’t performed during the establishment of the call.
- VBD mode for V.152 implementation (refer to "Supporting V.152 Implementation" on page 357): fax / modem capabilities are negotiated between the device and the remote endpoint at the establishment of the call. During a call, when a fax / modem signal is detected, transition from voice to VBD (or T.38) is automatically performed and no additional SIP signaling is required. If negotiation fails (i.e., no match is achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter IsFaxUsed).

7.5.2 Fax/Modem Transport Modes

The device supports the following transport modes for fax per modem type (V.22/V.23/Bell/V.32/V.34):

- T.38 fax relay (refer to "Fax Relay Mode" on page 351)
- Fax and modem bypass: a proprietary method that uses a high bit rate coder (refer to "Fax/Modem Bypass Mode" on page 352)
- NSE Cisco's Pass-through bypass mode for fax and modem (refer to "Fax / Modem NSE Mode" on page 353)
- Transparent: passing the fax / modem signal in the current voice coder (refer to "Fax / Modem Transparent Mode" on page 354)
- Transparent with events: passing the fax / modem signal in the current voice coder with adaptations (refer to "Fax / Modem Transparent with Events Mode" on page 355)
- G.711 Transport: switching to G.711 when fax/modem is detected (refer to "G.711 Fax / Modem Transport Mode" on page 355)
- Fax fallback to G.711 if T.38 is not supported (refer to "Fax Fallback" on page 356)

'Adaptations' refer to automatic reconfiguration of certain DSP features for handling fax/modem streams differently than voice.

7.5.2.1 T.38 Fax Relay Mode

In Fax Relay mode, fax signals are transferred using the T.38 protocol. T.38 is an ITU standard for sending fax across IP networks in real-time mode. The device currently supports only the T.38 UDP syntax.

T.38 can be configured in the following ways:

- Switching to T.38 mode using SIP Re-INVITE messages (refer to "Switching to T.38 Mode using SIP Re-INVITE" on page 351)
- Automatically switching to T.38 mode without using SIP Re-INVITE messages (refer to "Automatically Switching to T.38 Mode without SIP Re-INVITE" on page 352)

When fax transmission ends, the reverse switching from fax relay to voice is automatically performed at both the local and remote endpoints.

You can change the fax rate declared in the SDP, using the parameter FaxRelayMaxRate (this parameter doesn't affect the actual transmission rate). In addition, you can enable or disable Error Correction Mode (ECM) fax mode using the FaxRelayECMEnable parameter.

When using T.38 mode, you can define a redundancy feature to improve fax transmission over congested IP networks. This feature is activated using the FaxRelayRedundancyDepth and FaxRelayEnhancedRedundancyDepth parameters. Although this is a proprietary redundancy scheme, it should not create problems when working with other T.38 decoders.

7.5.2.1.1 Switching to T.38 Mode using SIP Re-INVITE

In the Switching to T.38 Mode using SIP Re-INVITE mode, upon detection of a fax signal, the terminating device negotiates T.38 capabilities using a Re-INVITE message. If the far-end device doesn't support T.38, the fax fails. In this mode, the parameter FaxTransportMode is ignored.

To configure T.38 mode using SIP Re-INVITE messages, set IsFaxUsed to 1. Additional configuration parameters include the following:

- FaxRelayEnhancedRedundancyDepth
- FaxRelayRedundancyDepth
- FaxRelayECMEnable
- FaxRelayMaxRate

7.5.2.1.2 Automatically Switching to T.38 Mode without SIP Re-INVITE

In the Automatically Switching to T.38 Mode without SIP Re-INVITE mode, when a fax signal is detected, the channel automatically switches from the current voice coder to answer tone mode, and then to T.38-compliant fax relay mode.

To configure automatic T.38 mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 1
- Additional configuration parameters:
  - FaxRelayEnhancedRedundancyDepth
  - FaxRelayRedundancyDepth
  - FaxRelayECMEnable
  - FaxRelayMaxRate

7.5.2.2 Fax/Modem Bypass Mode

In this proprietary mode, when fax or modem signals are detected, the channel automatically switches from the current voice coder to a high bit-rate coder (according to the parameter FaxModemBypassCoderType). In addition, the channel is automatically reconfigured with the following fax / modem adaptations:

- Disables silence suppression
- Enables echo cancellation for fax
- Disables echo cancellation for modem
- Performs certain jitter buffering optimizations

The network packets generated and received during the bypass period are regular voice RTP packets (per the selected bypass coder), but with a different RTP payload type (according to the parameters FaxBypassPayloadType and ModemBypassPayloadType). During the bypass period, the coder uses the packing factor, which is defined by the parameter FaxModemBypassM. The packing factor determines the number of coder payloads (each the size of FaxModemBypassBasicRTPPacketInterval) that are used to generate a single fax/modem bypass packet. When fax/modem transmission ends, the reverse switching, from bypass coder to regular voice coder is performed.

To configure fax / modem bypass mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 2
- V21ModemTransportType = 2
- V22ModemTransportType = 2

- V23ModemTransportType = 2
- V32ModemTransportType = 2
- V34ModemTransportType = 2
- BellModemTransportType = 2
- Additional configuration parameters:
  - FaxModemBypassCoderType
  - FaxBypassPayloadType
  - ModemBypassPayloadType
  - FaxModemBypassBasicRTPPacketInterval
  - FaxModemBypassDJBufMinDelay

Note: When the device is configured for modem bypass and T.38 fax, V.21 low-speed modems are not supported and fail as a result.

Tip: When the remote (non-AudioCodes') gateway uses G711 coder for voice and doesn't change the coder payload type for fax or modem transmission, it is recommended to use the Bypass mode with the following configuration:

- EnableFaxModemInbandNetworkDetection = 1
- FaxModemBypassCoderType = same coder used for voice
- FaxModemBypassM = same interval as voice
- ModemBypassPayloadType = 8 if voice coder is A-Law; 0 if voice coder is Mu-Law

7.5.2.3 Fax / Modem NSE Mode

In this mode, fax and modem signals are transferred using Cisco-compatible Pass-through bypass mode. Upon detection of fax or modem answering tone signal, the terminating device sends three to six special NSE RTP packets (using NSEpayloadType, usually 100). These packets signal the remote device to switch to G.711 coder (according to the parameter FaxModemBypassCoderType). After a few NSE packets are exchanged between the devices, both devices start using G.711 packets with standard payload type (8 for G.711 A-Law and 0 for G.711 Mu-Law). In this mode, no Re-INVITE messages are sent. The voice channel is optimized for fax/modem transmission (same as for usual bypass mode).

The parameters defining payload type for the proprietary AudioCodes' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass.

When configured for NSE mode, the device includes in its SDP the following line:

```
a=rtpmap:100 X-NSE/8000
```

(where 100 is the NSE payload type)

The Cisco gateway must include the following definition: "modem passthrough nse payload-type 100 codec g711alaw".

To configure NSE mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 2
- NSEMode = 1
- NSEPayloadType = 100
- V21ModemTransportType = 2
- V22ModemTransportType = 2
- V23ModemTransportType = 2
- V32ModemTransportType = 2
- V34ModemTransportType = 2
- BellModemTransportType = 2

7.5.2.4 Fax / Modem Transparent Mode

In this mode, fax and modem signals are transferred using the current voice coder without notifications to the user and without automatic adaptations. It's possible to use the Profiles mechanism (refer to "Configuring the Profile Definitions" on page 190) to apply certain adaptations to the channel used for fax / modem (e.g., to use the coder G.711, to set the jitter buffer optimization factor to 13, and to enable echo cancellation for fax and disable it for modem).

To configure fax / modem transparent mode, use the following parameters:

- IsFaxUsed = 0
- FaxTransportMode = 0
- V21ModemTransportType = 0
- V22ModemTransportType = 0
- V23ModemTransportType = 0
- V32ModemTransportType = 0
- V34ModemTransportType = 0
- BellModemTransportType = 0
- Additional configuration parameters:
    - CoderName
    - DJBufOptFactor
    - EnableSilenceCompression
    - EnableEchoCanceller

Note: This mode can be used for fax, but is not recommended for modem transmission. Instead, use the modes Bypass (refer to "Fax/Modem Bypass Mode" on page 352) or Transparent with Events (refer to "Fax / Modem Transparent with Events Mode" on page 355) for modem.

7.5.2.5 Fax / Modem Transparent with Events Mode

In this mode, fax and modem signals are transferred using the current voice coder with the following automatic adaptations:

- Echo Canceller = on (or off, for modems)
- Echo Canceller Non-Linear Processor Mode = off
- Jitter buffering optimizations

To configure fax / modem transparent with events mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 3
- V21ModemTransportType = 3
- V22ModemTransportType = 3
- V23ModemTransportType = 3
- V32ModemTransportType = 3
- V34ModemTransportType = 3
- BellModemTransportType = 3

7.5.2.6 G.711 Fax / Modem Transport Mode

In this mode, when the terminating device detects fax or modem signals (CED or AnsAM), it sends a Re-INVITE message to the originating device requesting it to re-open the channel in G.711 VBD with the following adaptations:

- Echo Canceller = off
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

After a few seconds upon detection of fax V.21 preamble or super G3 fax signals, the device sends a second Re-INVITE enabling the echo canceller (the echo canceller is disabled only on modem transmission).

A ‘gpmd’ attribute is added to the SDP according to the following format:

- **For G.711A-law:** a=gpmd:0 vbd=yes;ecan=on (or off, for modems)
- **For G.711 µ-law:** a=gpmd:8 vbd=yes;ecan=on (or off for modems)

The parameters FaxTransportMode and VxxModemTransportType are ignored and automatically set to the mode called ‘transparent with events’.

To configure fax / modem transparent mode, set IsFaxUsed to 2.

7.5.2.7 Fax Fallback

In this mode, when the terminating device detects a fax signal, it sends a Re-INVITE message to the originating device with T.38. If the remote device doesn't support T.38 (replies with SIP response 415 'Media Not Supported'), the device sends a new Re-INVITE with G.711 VBD with the following adaptations:

- Echo Canceller = on
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

When the device initiates a fax session using G.711, a 'gpmd' attribute is added to the SDP according to the following format:

- **For G.711A-law:** a=gpmd:0 vbd=yes;ecan=on
- **For G.711 μ-law:** a=gpmd:8 vbd=yes;ecan=on

In this mode, the parameter FaxTransportMode is ignored and automatically set to 'transparent'.

To configure fax fallback mode, set IsFaxUsed to 3.

7.5.3 Supporting V.34 Faxes

Unlike T.30 fax machines, V.34 fax machines have no relay standard to transmit data over IP to the remote side. Therefore, the device provides the following operation modes for transporting V.34 fax data over the IP:

- Using bypass mechanism for V.34 fax transmission (refer to "Using Bypass Mechanism for V.34 Fax Transmission" on page 356)
- Using relay mode, i.e., fallback to T.38 (refer to "Using Relay mode for both T.30 and V.34 faxes" on page 357)

Using the *ini* file parameter V34FaxTransportType, you can determine whether to pass V.34 Fax-over-T.38 fallback to T.30, or use Bypass over the High Bit Rate coder (e.g. PCM A-Law).

Note: The CNG detector is disabled (CNGDetectorMode = 0) in all the subsequent examples.

7.5.3.1 Using Bypass Mechanism for V.34 Fax Transmission

In this proprietary scenario, the device uses bypass (or NSE) mode to transmit V.34 faxes, enabling the full utilization of its speed.

Configure the following parameters to use bypass mode for both T.30 and V.34 faxes:

- FaxTransportMode = 2 (Bypass)
- V34ModemTransportType = 2 (Modem bypass)
- V32ModemTransportType = 2

- V23ModemTransportType = 2
- V22ModemTransportType = 2

Configure the following parameters to use bypass mode for V.34 faxes and T.38 for T.30 faxes:

- FaxTransportMode = 1 (Relay)
- V34ModemTransportType = 2 (Modem bypass)
- V32ModemTransportType = 2
- V23ModemTransportType = 2
- V22ModemTransportType = 2

7.5.3.2 Using Relay mode for both T.30 and V.34 faxes

In this scenario, V.34 fax machines are forced to use their backward compatibility with T.30 faxes and operate in the slower T.30 mode.

Use the following parameters to use T.38 mode for both V.34 faxes and T.30 faxes:

- FaxTransportMode = 1 (Relay)
- V34ModemTransportType = 0 (Transparent)
- V32ModemTransportType = 0
- V23ModemTransportType = 0
- V22ModemTransportType = 0

7.5.4 Supporting V.152 Implementation

The device supports the ITU-T recommendation V.152 (Procedures for Supporting Voice-Band Data over IP Networks). Voice-band data (VBD) is the transport of modem, facsimile, and text telephony signals over a voice channel of a packet network with a codec appropriate for such signals.

For V.152 capability, the device supports T.38 as well as VBD codecs (i.e., G.711 A-law and G.711 µ-law). The selection of capabilities is performed using the coders table (refer to "Coders" on page 144).

When in VBD mode for V.152 implementation, support is negotiated between the device and the remote endpoint at the establishment of the call. During this time, initial exchange of call capabilities is exchanged in the outgoing SDP. These capabilities include whether VBD is supported and associated RTP payload types ('gpmd' SDP attribute), supported codecs, and packetization periods for all codec payload types ('ptime' SDP attribute). After this initial negotiation, no Re-INVITE messages are necessary as both endpoints are synchronized in terms of the other side's capabilities. If negotiation fails (i.e., no match was achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter IsFaxUsed).

Below is an example of media descriptions of an SDP indicating support for V.152.

```
v=0
o=-  0 0 IN IPV4 <IPAdressA>
s=-
t=0 0
p=+1
c=IN IP4  <IPAddressA
m=audio <udpPort A> RTP/AVP 18 0
a=ptime:10
a=rtpmap:96 PCMU/8000
a=gpmd: 96 vbd=yes
```

In the example above, V.152 implementation is supported (using the dynamic payload type 96 and G.711 u-law as the VBD codec) as well as the voice codecs G.711 µ-law and G.729.

Instead of using VBD transport mode, the V.152 implementation can use alternative relay fax transport methods (e.g., fax relay over IP using T.38). The preferred V.152 transport method is indicated by the SDP 'pmft' attribute. Omission of this attribute in the SDP content means that VBD mode is the preferred transport mechanism for voice-band data.

To configure T.38 mode, use the CoderName parameter.

7.6 Event Notification using X-Detect Header

The device supports the sending of notifications to a remote party notifying the occurrence (or detection) of certain events on the media stream. Event detection and notifications is performed using the X-Detect SIP message header, and only when establishing a SIP dialog.

For supporting some events, certain device configurations need to be performed. The table below lists the support event types (and subtypes) and the corresponding device configurations, if required:

Table 7-2: Supported X-Detect Event Types

Events Type	Subtype	Required Configuration

AMD	voice
	automatic
	silence
	unknown
		EnableDSPIPMDetectors = 1
		AMDTimeout = 2000 (msec)

CPT	SIT	SITDetectorEnable = 1
		UserDefinedToneDetectorEnable = 1

FAX	CED	(IsFaxUsed ≠ 0) or (IsFaxUsed = 0, and FaxTransportMode ≠ 0)
	modem	VxxModemTransportType = 3
PTT	voice-start voice-end	EnableDSPIPMDetectors = 1

The X-Detect event notification process is as follows:

1. For IP-to-Tel or Tel-to-IP calls, the device receives a SIP request message (using the X-Detect header) that the remote party wishes to detect events on the media stream. For incoming (IP-to-Tel) calls, the request must be indicated in the initial INVITE and responded to either in the 183 response (for early dialogs) or in the 200 OK response (for confirmed dialogs). For outgoing calls (Tel-to-IP), the request may be received in the 183 (for early dialogs) and responded to in the PRACK, or received in the 200 OK (for confirmed dialogs) and responded to in the ACK.

2. Once the device receives such a request, it sends a SIP response message (using the X-Detect header) to the remote party, listing all supported events that can be detected. The absence of the X-Detect header indicates that no detections are available.

3. Each time the device detects a supported event, the event is notified to the remote party, by sending an INFO message with the following message body:

   - Content-Type: application/X-DETECT
   - Type = [AMD | CPT | FAX | PTT…]
   - Subtype = xxx (according to the defined subtypes of each type)

Below is an example of SIP messages implementing the X-Detect header:

```
INVITE sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X- Detect: Request=CPT,FAX
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>;tag=1c19282
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:101@10.33.2.53>
X- Detect: Response=CPT,FAX
INFO sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X- Detect: Response=CPT,FAX
Content-Type: Application/X-Detect
Content-Length: xxx
Type = CPT
Subtype = SIT
```

7.7 RTP Multiplexing (ThroughPacket)

The device supports a proprietary method to aggregate RTP streams from several channels to reduce the bandwidth overhead caused by the attached Ethernet, IP, UDP, and RTP headers, and to reduce the packet / data transmission rate. This option reduces the load on network routers and can typically save 50% (e.g., for G.723) on IP bandwidth. RTP Multiplexing (ThroughPacket™) is accomplished by aggregating payloads from several channels that are sent to the same destination IP address into a single IP packet.

RTP multiplexing can be applied to the entire device (refer to "Configuring the RTP / RTCP Settings" on page 71) or to specific IP destinations using the IP Profile feature (refer to "IP Profile Settings" on page 193).

To enable RTP Multiplexing, set the parameter RemoteBaseUDPPort to a nonzero value. Note that the value of RemoteBaseUDPPort on the local device must equal the value of BaseUDPPort of the remote device. The device uses these parameters to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels.

In RTP Multiplexing mode, the device uses a single UDP port for all incoming multiplexed packets and a different port for outgoing packets. These ports are configured using the parameters L1L1ComplexTxUDPPort and L1L1ComplexRxUDPPort.

When RTP Multiplexing is used, call statistics aren't available (since there is no RTCP flow).

Notes:

- RTP Multiplexing must be enabled on both devices.
- When VLANs are imlemented, the RTP Multiplexing mechanism is not supported.

7.8 Dynamic Jitter Buffer Operation

Voice frames are transmitted at a fixed rate. If the frames arrive at the other end at the same rate, voice quality is perceived as good. In many cases, however, some frames can arrive slightly faster or slower than the other frames. This is called jitter (delay variation), and degrades the perceived voice quality. To minimize this problem, the device uses a jitter buffer. The jitter buffer collects voice packets, stores them and sends them to the voice processor in evenly spaced intervals.

The device uses a dynamic jitter buffer that can be configured using the following two parameters:

- **Minimum delay:** DJBufMinDelay (0 msec to 150 msec)
  Defines the starting jitter capacity of the buffer. For example, at 0 msec, there is no buffering at the start. At the default level of 10 msec, the device always buffers incoming packets by at least 10 msec worth of voice frames.

- **Optimization Factor:** DJBufOptFactor (0 to 12, 13)
  Defines how the jitter buffer tracks to changing network conditions. When set at its maximum value of 12, the dynamic buffer aggressively tracks changes in delay (based on packet loss statistics) to increase the size of the buffer and doesn't decay back down. This results in the best packet error performance, but at the cost of extra delay. At the minimum value of 0, the buffer tracks delays only to compensate for clock drift and quickly decays back to the minimum level. This optimizes the delay performance but at the expense of a higher error rate.

The default settings of 10 msec Minimum delay and 10 Optimization Factor should provide a good compromise between delay and error rate. The jitter buffer ‘holds’ incoming packets for 10 msec before making them available for decoding into voice. The coder polls frames from the buffer at regular intervals in order to produce continuous speech. As long as delays in the network do not change (jitter) by more than 10 msec from one packet to the next, there is always a sample in the buffer for the coder to use. If there is more than 10 msec of delay at any time during the call, the packet arrives too late. The coder tries to access a frame and is not able to find one. The coder must produce a voice sample even if a frame is not available. It therefore compensates for the missing packet by adding a Bad-Frame-Interpolation (BFI) packet. This loss is then flagged as the buffer being too small. The dynamic algorithm then causes the size of the buffer to increase for the next voice session. The size of the buffer may decrease again if the device notices that the buffer is not filling up as much as expected. At no time does the buffer decrease to less than the minimum size configured by the Minimum delay parameter.

For certain scenarios, the **Optimization Factor is set to 13**: One of the purposes of the Jitter Buffer mechanism is to compensate for clock drift. If the two sides of the VoIP call are not synchronized to the same clock source, one RTP source generates packets at a lower rate, causing under-runs at the remote Jitter Buffer. In normal operation (optimization factor 0 to 12), the Jitter Buffer mechanism detects and compensates for the clock drift by occasionally dropping a voice packet or by adding a BFI packet.

Fax and modem devices are sensitive to small packet losses or to added BFI packets. Therefore, to achieve better performance during modem and fax calls, the Optimization Factor should be set to 13. In this special mode the clock drift correction is performed less frequently - only when the Jitter Buffer is completely empty or completely full. When such condition occurs, the correction is performed by dropping several voice packets simultaneously or by adding several BFI packets simultaneously, so that the Jitter Buffer returns to its normal condition.

7.9 Configuring Alternative Routing (Based on Connectivity and QoS)

The Alternative Routing feature enables reliable routing of Tel-to-IP calls when a Proxy isn’t used. The device periodically checks the availability of connectivity and suitable Quality of Service (QoS) before routing. If the expected quality cannot be achieved, an alternative IP route for the prefix (phone number) is selected.

Note: If the alternative routing destination is the device itself, the call can be configured to be routed back to one of the device's trunk groups and thus, back into the PSTN (PSTN Fallback).

7.9.1 Alternative Routing Mechanism

When a Tel-to-IP call is routed through the device, the call’s destination number is compared to the list of prefixes defined in the 'Tel to IP Routing' table (described in "Tel to IP Routing Table" on page 175). The 'Tel to IP Routing' table is scanned for the destination number’s prefix starting at the top of the table. For this reason, enter the main IP route above any alternative route. When an appropriate entry (destination number matches one of the prefixes) is found, the prefix’s corresponding destination IP address is verified. If the destination IP address is disallowed (or if the original call fails and the device has made two additional attempts to establish the call without success), an alternative route is searched in the table. , after which an alternative route is used.

Destination IP address is disallowed if no ping to the destination is available (ping is continuously initiated every seven seconds), when an inappropriate level of QoS was detected, or when a DNS host name is not resolved. The QoS level is calculated according to delay or packet loss of previously ended calls. If no call statistics are received for two minutes, the QoS information is reset.

7.9.2 Determining the Availability of Destination IP Addresses

To determine the availability of each destination IP address (or host name) in the routing table, one (or all) of the following (configurable) methods are applied:

- **Connectivity:** The destination IP address is queried periodically (currently only by ping).
- **QoS:** The QoS of an IP connection is determined according to RTCP statistics of previous calls. Network delay (in msec) and network packet loss (in percentage) are separately quantified and compared to a certain (configurable) threshold. If the calculated amounts (of delay or packet loss) exceed these thresholds, the IP connection is disallowed.
- **DNS resolution:** When host name is used (instead of IP address) for the destination route, it is resolved to an IP address by a DNS server. Connectivity and QoS are then applied to the resolved IP address.

7.9.3 PSTN Fallback as a Special Case of Alternative Routing

The PSTN Fallback feature enables the device to redirect PSTN originated calls back to the legacy PSTN network if a destination IP route is unsuitable (disallowed) for voice traffic at a specific time. To enable PSTN fallback, assign the device's IP address as an alternative route to the desired prefixes. Note that calls (now referred to as IP-to-Tel calls) can be re-routed to a specific trunk group using the Routing parameters (refer to "IP to Trunk Group Routing" on page 181).

7.9.4 Relevant Parameters

The following parameters (described in "Routing General Parameters" on page 171) are used to configure the Alternative Routing mechanism:

- AltRoutingTel2IPEnable
- AltRoutingTel2IPMode
- IPConnQoSMaxAllowedPL
- IPConnQoSMaxAllowedDelay

7.10 Supported RADIUS Attributes

Use the following table for explanations on the RADIUS attributes contained in the communication packets transmitted between the device and a RADIUS Server.

Table 7-3: Supported RADIUS Attributes

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA[1]
Request Attributes						
1	User-Name		Account number or calling party number or blank	String up to 15 digits long	5421385747	Start Acc Stop Acc
4	NAS-IP-Address		IP address of the requesting device	Numeric	192.168.14.43	Start Acc Stop Acc
6	Service-Type		Type of service requested	Numeric	1: login	Start Acc Stop Acc
26	H323-Incoming-Conf-Id	1	SIP call identifier	Up to 32 octets		Start Acc Stop Acc
26	H323-Remote-Address	23	IP address of the remote gateway	Numeric		Stop Acc
26	H323-Conf-ID	24	H.323/SIP call identifier	Up to 32 octets		Start Acc Stop Acc
26	H323-Setup-Time	25	Setup time in NTP format 1	String		Start Acc Stop Acc
26	H323-Call-Origin	26	The call's originator: Answering (IP) or Originator (PSTN)	String	Answer, Originate etc	Start Acc Stop Acc
26	H323-Call-Type	27	Protocol type or family used on this leg of the call	String	VoIP	Start Acc Stop Acc
26	H323-Connect-Time	28	Connect time in NTP format	String		Stop Acc
26	H323-	29	Disconnect time in NTP	String		Stop

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA[1]
	Disconnect-Time		format			Acc
26	H323-Disconnect-Cause	30	Q.931 disconnect cause code	Numeric		Stop Acc
26	H323-Gw-ID	33	Name of the gateway	String	SIPIDString	Start Acc Stop Acc
26	SIP-Call-ID	34	SIP Call ID	String	abcde@ac.com	Start Acc Stop Acc
26	Call-Terminator	35	The call's terminator: PSTN-terminated call (Yes); IP-terminated call (No).	String	Yes, No	Stop Acc
30	Called-Station-ID			String	8004567145	Start Acc
			Destination phone number	String	2427456425	Stop Acc
31	Calling-Station-ID		Calling Party Number (ANI)	String	5135672127	Start Acc Stop Acc
40	Acct-Status-Type		Account Request Type (start or stop) **Note:** ‘start’ isn’t supported on the Calling Card application.	Numeric	1: start, 2: stop	Start Acc Stop Acc
41	Acct-Delay-Time		No. of seconds tried in sending a particular record	Numeric	5	Start Acc Stop Acc
42	Acct-Input-Octets		Number of octets received for that call duration	Numeric		Stop Acc
43	Acct-Output-Octets		Number of octets sent for that call duration	Numeric		Stop Acc
44	Acct-Session-ID		A unique accounting identifier - match start & stop	String	34832	Start Acc Stop Acc
46	Acct-Session-Time		For how many seconds the user received the service	Numeric		Stop Acc
47	Acct-Input-Packets		Number of packets received during the call	Numeric		Stop Acc

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA[1]
48	Acct-Output-Packets		Number of packets sent during the call	Numeric		Stop Acc
61	NAS-Port-Type		Physical port type of device on which the call is active	String	0: Asynchronous	Start Acc Stop Acc
Response Attributes						
26	H323-Return-Code	103	The reason for failing authentication (0 = ok, other number failed)	Numeric	0 Request accepted	Stop Acc
44	Acct-Session-ID		A unique accounting identifier – match start & stop	String		Stop Acc

Below is an example of RADIUS Accounting, where the non-standard parameters are preceded with brackets.

```
Accounting-Request (361)
user-name = 111
acct-session-id = 1
nas-ip-address = 212.179.22.213
nas-port-type = 0
acct-status-type = 2
acct-input-octets = 4841
acct-output-octets = 8800
acct-session-time = 1
acct-input-packets = 122
acct-output-packets = 220
called-station-id = 201
calling-station-id = 202
// Accounting non-standard parameters:
(4923 33) h323-gw-id =
(4923 23) h323-remote-address = 212.179.22.214
(4923 1) h323-ivr-out = h323-incoming-conf-id:02102944 600a1899
3fd61009 0e2f3cc5
(4923 30) h323-disconnect-cause = 22 (0x16)
(4923 27) h323-call-type = VOIP
(4923 26) h323-call-origin = Originate
(4923 24) h323-conf-id = 02102944 600a1899 3fd61009 0e2f3cc5
```

7.11 Call Detail Record

The Call Detail Record (CDR) contains vital statistic information on calls made by the device. CDRs are generated at the end and (optionally) at the beginning of each call (determined by the parameter CDRReportLevel), and then sent to a Syslog server. The destination IP address for CDR logs is determined by the parameter CDRSyslogServerIP. For CDR in RADIUS format, refer to "Supported RADIUS Attributes" on page 362.

The following table lists the CDR fields that are supported.

Table 7-4: Supported CDR Fields

Field Name	Description
ReportType	Report for either Call Started, Call Connected, or Call Released
Cid	Port Number
CallId	SIP Call Identifier
Trunk	Physical Trunk Number
BChan	Selected B-Channel
ConId	SIP Conference ID
TG	Trunk Group Number
EPTyp	Endpoint Type
Orig	Call Originator (IP, Tel)
SourceIp	Source IP Address
DestIp	Destination IP Address
TON	Source Phone Number Type
NPI	Source Phone Number Plan
SrcPhoneNum	Source Phone Number
SrcNumBeforeMap	Source Number Before Manipulation
TON	Destination Phone Number Type
NPI	Destination Phone Number Plan
DstPhoneNum	Destination Phone Number
DstNumBeforeMap	Destination Number Before Manipulation
Durat	Call Duration
Coder	Selected Coder
Intrv	Packet Interval
RtpIp	RTP IP Address
Port	Remote RTP Port
TrmSd	Initiator of Call Release (IP, Tel, Unknown)
TrmReason	Termination Reason
Fax	Fax Transaction during the Call
InPackets	Number of Incoming Packets
OutPackets	Number of Outgoing Packets
PackLoss	Local Packet Loss
RemotePackLoss	Number of Outgoing Lost Packets
UniqueId	unique RTP ID
SetupTime	Call Setup Time
ConnectTime	Call Connect Time
ReleaseTime	Call Release Time

Field Name	Description
RTPdelay	RTP Delay
RTPjitter	RTP Jitter
RTPssrc	Local RTP SSRC
RemoteRTPssrc	Remote RTP SSRC
RedirectReason	Redirect Reason
TON	Redirection Phone Number Type
MeteringPulses	Number of Generated Metering Pulses
NPI	Redirection Phone Number Plan
RedirectPhonNum	Redirection Phone Number

7.12 Trunk-to-Trunk Routing Example

This example describes two devices, each interfacing with the PSTN through four E1 spans. Device **A** is configured to route all incoming Tel-to-IP calls to Device **B**. Device **B** generates calls to the PSTN on the same E1 trunk on which the call was originally received (in Device **A**).

- Device **A** IP address: 192.168.3.50
- Device **B** IP address: 192.168.3.51

The *ini* file parameters configuration for devices **A** and **B** include the following:

1. At both devices, define four trunk groups, each with 30 B-channels:
    - TrunkGroup_1 = 0/1-31,1000
    - TrunkGroup_2 = 1/1-31,2000
    - TrunkGroup_3 = 2/1-31,3000
    - TrunkGroup_4 = 3/1-31,4000
2. At Device **A**, add the originating Trunk Group ID as a prefix to the destination number for Tel-to-IP calls:

    AddTrunkGroupAsPrefix = 1
3. At Device **A**, route all incoming PSTN calls starting with prefixes 1, 2, 3, and 4, to the IP address of Device **B**:
    - Prefix = 1, 192.168.3.51
    - Prefix = 2, 192.168.3.51
    - Prefix = 3, 192.168.3.51
    - Prefix = 4, 192.168.3.51

    Note: You can also define Prefix = *,192.168.3.51, instead of the four lines above.
4. At Device **B**, route IP-to-PSTN calls to Trunk Group ID according to the first digit of the called number:
    - PSTNPrefix = 1,1
    - PSTNPrefix = 2,2

- PSTNPrefix = 3,4
- PSTNPrefix = 4,4

5. At Device **B**, remove the first digit from each IP-to-PSTN number before it is used in an outgoing call: NumberMapIP2Tel = *,1

7.13 Proxy or Registrar Registration Example

Below is an example of Proxy and Registrar Registration:

```
REGISTER sip:servername SIP/2.0
VIA: SIP/2.0/UDP 212.179.22.229;branch=z9hG4bRaC7AU234
From: <sip:GWRegistrationName@sipgatewayname>;tag=1c29347
To: <sip:GWRegistrationName@sipgatewayname>
Call-ID: 10453@212.179.22.229
Seq: 1 REGISTER
Expires: 3600
Contact: sip:GWRegistrationName@212.179.22.229
Content-Length: 0
```

The ‘servername’ string is defined according to the following rules:

- The "servername" is equal to "RegistrarName" if configured. The "RegistrarName" can be any string.
- Otherwise, the "servername" is equal to "RegistrarIP" (either FQDN or numerical IP address), if configured.
- Otherwise, the "servername" is equal to "ProxyName" if configured. The "ProxyName" can be any string.
- Otherwise, the "servername" is equal to "ProxyIP" (either FQDN or numerical IP address).

The parameter GWRegistrationName can be any string. This parameter is used only if registration is per device. If the parameter is not defined, the parameter UserName is used instead. If the registration is per endpoint, the endpoint phone number is used.

The 'sipgatewayname' parameter (defined in the *ini* file or Web interface) can be any string. Some Proxy servers require that the 'sipgatewayname' (in REGISTER messages) is set equal to the Registrar / Proxy IP address or to the Registrar / Proxy domain name. The 'sipgatewayname' parameter can be overwritten by the TrunkGroupSettings_GatewayName value if the TrunkGroupSettings_RegistrationMode is set to 'Per Endpoint'.

REGISTER messages are sent to the Registrar's IP address (if configured) or to the Proxy's IP address. A single message is sent once per device, or messages are sent per B-channel according to the parameter AuthenticationMode. There is also an option to configure registration mode per Trunk Group using the TrunkGroupSettings table. The registration request is resent according to the parameter RegistrationTimeDivider. For example, if RegistrationTimeDivider = 70 (%) and Registration Expires time = 3600, the device resends its registration request after 3600 x 70% = 2520 sec. The default value of RegistrationTimeDivider is 50%.

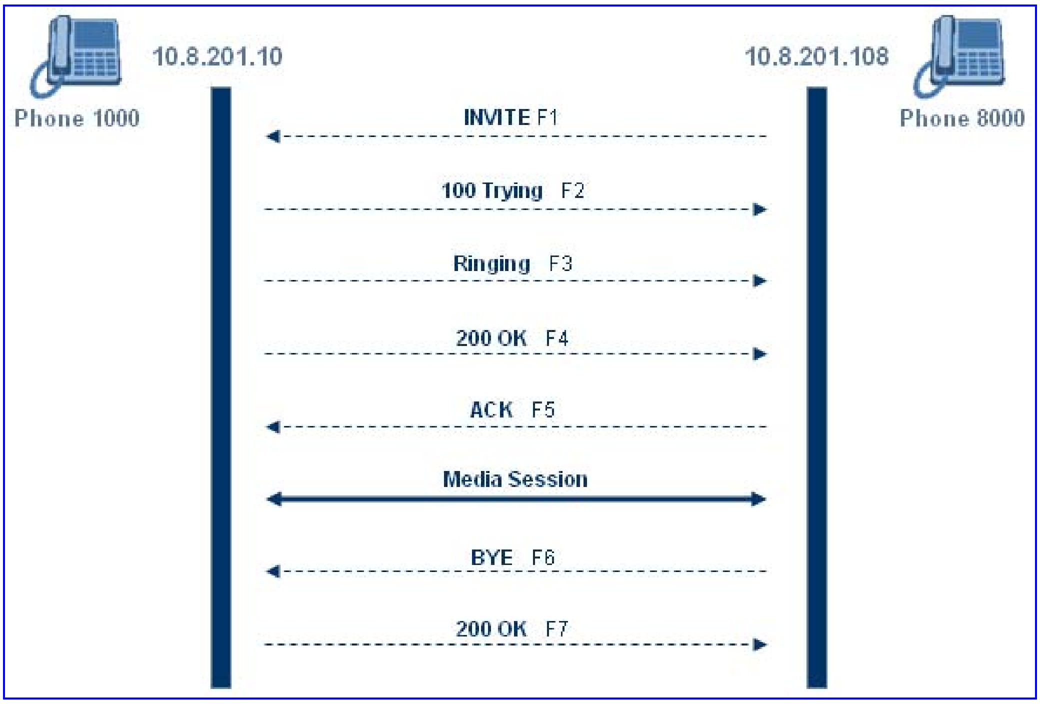
If registration per B-channel is selected, on device startup the device sends REGISTER requests according to the maximum number of allowed SIP dialogs (configured by the parameter NumberOfActiveDialogs). After each received response, the subsequent REGISTER request is sent.

7.14 Configuration Examples

7.14.1 SIP Call Flow

The SIP call flow (shown in the following figure), describes SIP messages exchanged between two devices during a simple call. In this call flow example, device (10.8.201.158) with phone number ‘6000’ dials device (10.8.201.161) with phone number ‘2000’.

Figure 7-2: SIP Call Flow



- **F1 (10.8.201.108 >> 10.8.201.10 INVITE):**

```
INVITE sip:1000@10.8.201.10;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
CSeq: 18153 INVITE
Contact: <sip:8000@10.8.201.108;user=phone>
User-Agent: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 208
v=0
o=AudiocodesGW 18132 74003 IN IP4 10.8.201.108
s=Phone-Call
c=IN IP4 10.8.201.108
t=0 0
m=audio 4000 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

- **F2 (10.8.201.10 >> 10.8.201.108 TRYING):**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
Server: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
CSeq: 18153 INVITE
Content-Length: 0
```

- **F3 (10.8.201.10 >> 10.8.201.108 180 RINGING):**

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
Server: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
CSeq: 18153 INVITE
Supported: 100rel,em
Content-Length: 0
```

Note: Phone ‘1000’ answers the call and then sends a 200 OK message to device 10.8.201.108.

- **F4 (10.8.201.10 >> 10.8.201.108 200 OK):**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
CSeq: 18153 INVITE
Contact: <sip:1000@10.8.201.10;user=phone>
Server: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 206
v=0
o=AudiocodesGW 30221 87035 IN IP4 10.8.201.10
s=Phone-Call
c=IN IP4 10.8.201.10
t=0 0
m=audio 7210 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=ptime:20
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

- **F5 (10.8.201.108 >> 10.8.201.10 ACK):**

```
ACK sip:1000@10.8.201.10;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacZYpJWxZ
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
CSeq: 18153 ACK
Supported: 100rel,em
Content-Length: 0
```

Note: Phone ‘8000’ goes on-hook and device 10.8.201.108 sends a BYE to device 10.8.201.10. Voice path is established.

- **F6 (10.8.201.108 >> 10.8.201.10 BYE):**

```
BYE sip:1000@10.8.201.10;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

- **F7 (10.8.201.10 >> 10.8.201.108 200 OK):**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:8000@10.8.201.108>;tag=1c5354
To: <sip:1000@10.8.201.10>;tag=1c7345
Call-ID: 534366556655skKw-8000--1000@10.8.201.108
Server: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

7.14.2 SIP Authentication Example

The device supports basic and digest (MD5) authentication types, according to SIP RFC 3261 standard. A proxy server might require authentication before forwarding an INVITE message. A Registrar/Proxy server may also require authentication for client registration. A proxy replies to an unauthenticated INVITE with a 407 Proxy Authorization Required response, containing a Proxy-Authenticate header with the form of the challenge. After sending an ACK for the 407, the user agent can then resend the INVITE with a Proxy-Authorization header containing the credentials.

User agent, redirect or registrar servers typically use 401 Unauthorized response to challenge authentication containing a WWW-Authenticate header, and expect the re-INVITE to contain an Authorization header.

The following example describes the Digest Authentication procedure, including computation of user agent credentials:

1. The REGISTER request is sent to Registrar/Proxy server for registration, as follows:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c17940
To: <sip: 122@10.1.1.200>
Call-ID: 634293194@10.1.1.200
User-Agent: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
```

2. Upon receipt of this request, the Registrar/Proxy returns 401 Unauthorized response.

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 10.2.1.200
From: <sip:122@10.2.2.222 >;tag=1c17940
To: <sip:122@10.2.2.222 >
Call-ID: 634293194@10.1.1.200
Cseq: 1 REGISTER
Date: Mon, 30 Jul 2001 15:33:54 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
WWW-Authenticate: Digest realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
stale=FALSE,
algorithm=MD5
```

3. According to the sub-header present in the WWW-Authenticate header, the correct REGISTER request is formed.

4. Since the algorithm is MD5, then:

   - The username is equal to the endpoint phone number 122.
   - The realm return by the proxy is audiocodes.com.
   - The password from the *ini* file is AudioCodes.
   - The equation to be evaluated is (according to RFC this part is called A1) **'122:audiocodes.com:AudioCodes'.**
   - The MD5 algorithm is run on this equation and stored for future usage.
   - The result is 'a8f17d4b41ab8dab6c95d3c14e34a9e1'.

5. Next, the par called A2 needs to be evaluated:

   - The method type is 'REGISTER'.
   - Using SIP protocol 'sip'.
   - Proxy IP from *ini* file is '10.2.2.222'.
   - The equation to be evaluated is **'REGISTER:sip:10.2.2.222'.**
   - The MD5 algorithm is run on this equation and stored for future usage.
   - The result is 'a9a031cfddcb10d91c8e7b4926086f7e'.

6. Final stage:

   - The A1 result: The nonce from the proxy response is ‘11432d6bce58ddf02e3b5e1c77c010d2’.
   - The A2 result: The equation to be evaluated is **‘A1:11432d6bce58ddf02e3b5e1c77c010d2:A2’.**
   - The MD5 algorithm is run on this equation. The outcome of the calculation is the response needed by the device to register with the Proxy.
   - The response is ‘b9c45d0234a5abf5ddf5c704029b38cf’.

   At this time, a new REGISTER request is issued with the following response:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Server: Audiocodes-Sip-Gateway/Mediant 2000/v.5.40.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
Authorization: Digest, username: 122,
realm="audiocodes.com”,
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
uri=”10.2.2.222”,
response=“b9c45d0234a5abf5ddf5c704029b38cf”
```

7. Upon receiving this request and if accepted by the Proxy, the proxy returns a 200 OK response closing the REGISTER transaction:

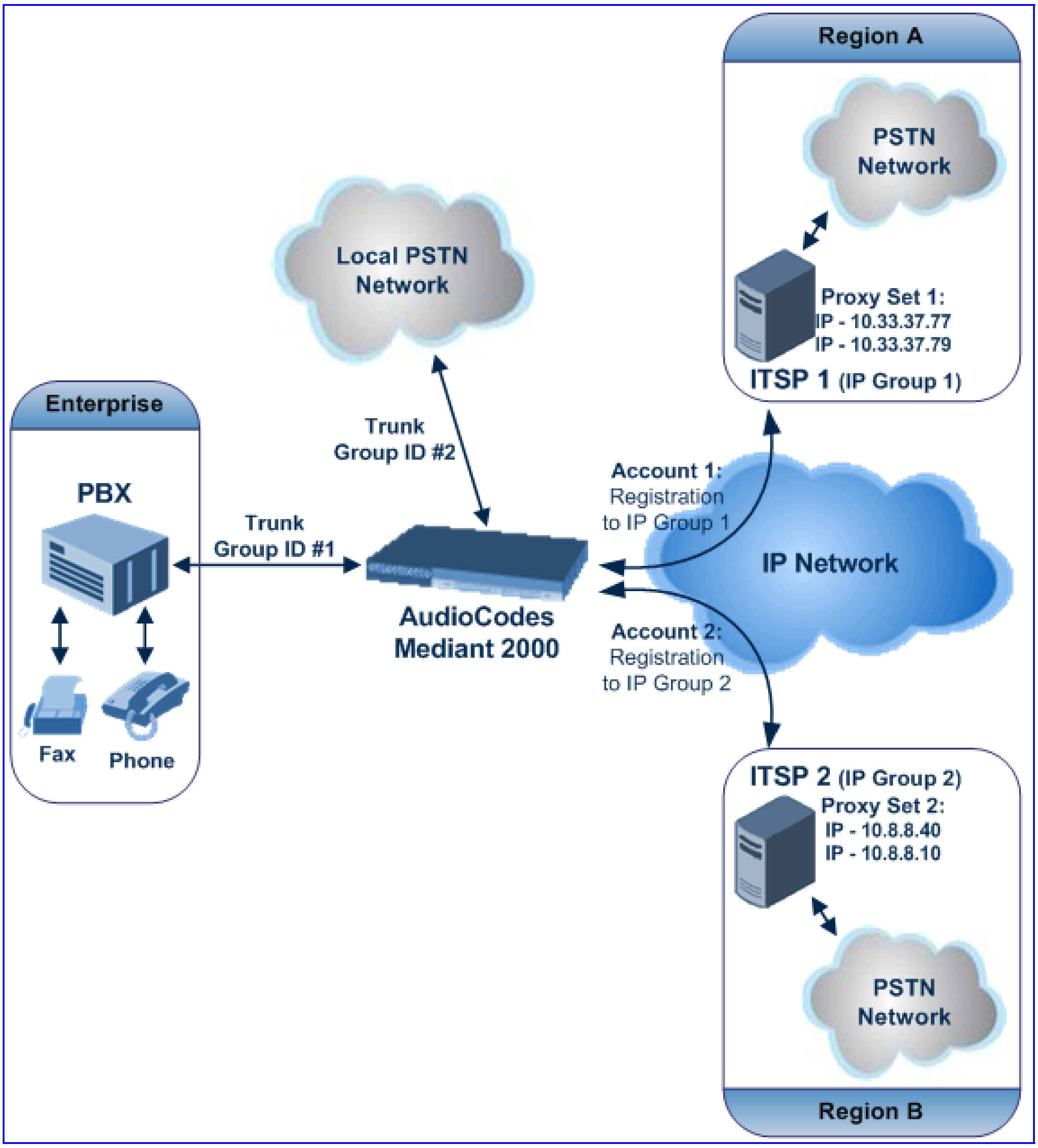
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Cseq: 1 REGISTER
Date: Thu, 26 Jul 2001 09:34:42 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
Contact: <sip:122@10.1.1.200>; expires="Thu, 26 Jul 2001 10:34:42
GMT"; action=proxy; q=1.00
Contact: <122@10.1.1.200:>; expires="Tue, 19 Jan 2038 03:14:07
GMT"; action=proxy; q=0.00
Expires: Thu, 26 Jul 2001 10:34:42 GMT
```

7.14.3 SIP Trunking between Enterprise and ITSPs

By implementing the device's enhanced and flexible routing configuration capabilities using Proxy Sets, IP Groups, and Accounts, you can "design" complex routing schemes. This section provides an example of an elaborate routing scheme for SIP trunking between an Enterprise's PBX and two Internet Telephony Service Providers (ITSP), using AudioCodes' device.

Scenario: In this example, the Enterprise wishes to connect its TDM PBX to two different ITSPs, by implementing a device in its network environment. It's main objective is for the device to route Tel-to-IP calls to these ITSPs according to a dial plan. The device is to register (on behalf of the PBX) to each ITSP, which implements two servers for redundancy and load balancing. The Register messages are to use different URI's in the From, To, and Contact headers per ITSP. In addition, all calls dialed from the Enterprise PBX with prefix '02' is sent to the local PSTN. The figure below illustrates the example setup:

Figure 7-3: Example Setup for Routing Between ITSP and Enterprise PBX



➢ To configure call routing between Enterprise and two ITSPs using the device, take these 8 steps:

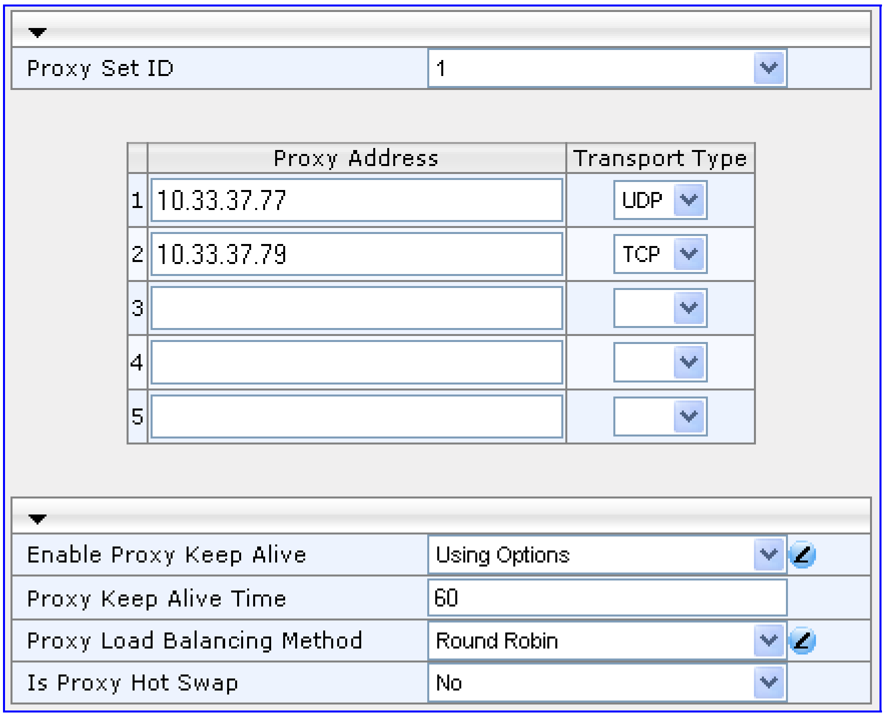
1. Enable the device to register to a Proxy / Registrar server, using the parameter IsRegisterNeeded in the 'Proxy & Registration' page (refer to ''Proxy & Registration Parameters'' on page 132).

2. In the 'Proxy Sets Table' page (refer to "Proxy Sets Table" on page 141), configure two Proxy Sets and for each, enable Proxy Keep-Alive (using SIP OPTIONS) and 'round robin' load-balancing method:

   - Proxy Set #**1** includes two IP addresses of the first ITSP (**ITSP 1**) - 10.33.37.77 and 10.33.37.79 - and using UDP.
   - Proxy Set #**2** includes two IP addresses of the second ITSP (**ITSP 2**) - 10.8.8.40 and 10.8.8.10 - and using TCP.

   The figure below displays the configuration of Proxy Set ID #1. Perform similar configuration for Proxy Set ID #2, but using different IP addresses.

Figure 7-4: Configuring Proxy Set ID #1 in the Proxy Sets Table Page



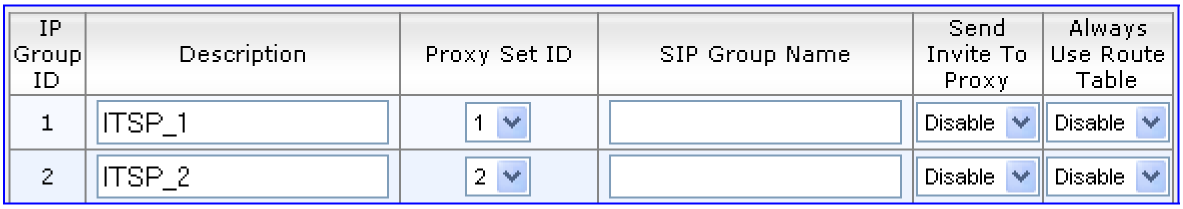
Proxy Set ID	1

	Proxy Address	Transport Type
1	10.33.37.77	UDP
2	10.33.37.79	TCP
3		
4		
5		

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	No

3. In the 'IP Group Table' page (refer to "Configuring the IP Groups" on page 201), configure the two IP Groups #1 and #2. Assign Proxy Sets #1 and #2 to IP Groups #1 and #2 respectively.

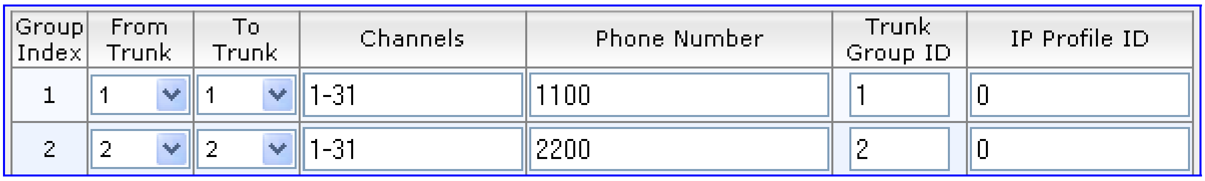
Figure 7-5: Configuring IP Groups #1 and #2 in the IP Group Table Page



IP Group ID	Description	Proxy Set ID	SIP Group Name	Send Invite To Proxy	Always Use Route Table
1	ITSP_1	1		Disable	Disable
2	ITSP_2	2		Disable	Disable

4. In the 'Trunk Group Table' page (refer to “Configuring the Trunk Group Table” on page 195), enable the Trunks connected between the Enterprise's PBX and the device (Trunk Group ID #1), and between the local PSTN and the device (Trunk Group ID #2).

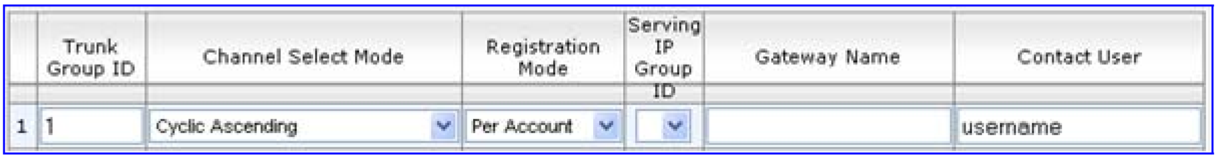
Figure 7-6: Assign the Trunk to Trunk Group ID #1 in the Trunk Group Table Page



Group Index	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	IP Profile ID
1	1	1	1-31	1100	1	0
2	2	2	1-31	2200	2	0

5. In the 'Trunk Group Settings' page (refer to "Configuring the Trunk Group Settings" on page 197), configure 'Per Account' registration for Trunk Group ID #1 (without serving IP Group).

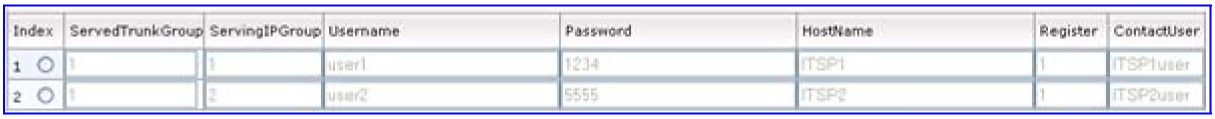
Figure 7-7: Configuring Trunk Group #1 for Registration per Account in Trunk Group Settings Page



	Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	Cyclic Ascending	Per Account			username

6. In the 'Account Table' page (refer to "Configuring the Account Table" on page 204), configure the two Accounts for PBX trunk registration to ITSPs using the same Trunk Group (i.e., ID #1), but different serving IP Groups #1 and #2. For each account, define user name, password, and hostname, and ContactUser. The Register messages use different URI's (Hostname and ContactUser) in the From, To, and Contact headers per ITSP. Enable registration for both accounts. .

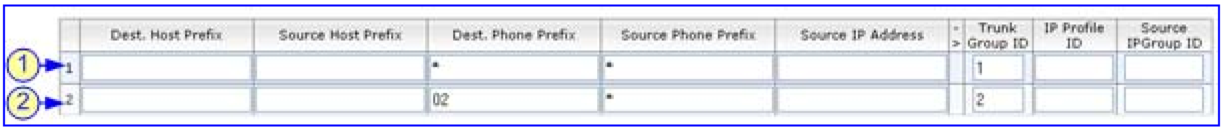
Figure 7-8: Configuring Accounts for PBX Registration to ITSPs in Account Table Page



Index		ServedTrunkGroup	ServingIPGroup	Username	Password	HostName	Register	ContactUser
1	○	1	1	user1	1234	ITSP1	1	ITSP1user
2	○	1	2	user2	5555	ITSP2	1	ITSP2user

7. In the 'IP to Trunk Group Routing' page (refer to "IP to Trunk Group Routing" on page 181), configure IP-to-Tel routing for calls from ITSPs to Trunk Group ID #1 (see 1 below) and from the device to the local PSTN (see 2 below).

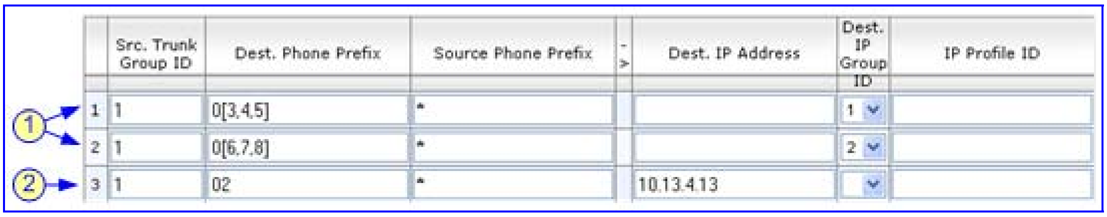
Figure 7-9: Configuring ITSP-to-Trunk Group #1 Routing in IP to Trunk Group Table Page



	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Trunk Group ID	IP Profile ID	Source IPGroup ID
1			*	*			1		
2			02	*			2		

8. In the 'Tel to IP Routing' page (refer to "Tel to IP Routing Table" on page 175), configure Tel-to-IP routing rules for calls to ITSPs (see 1 below) and to local PSTN (see 2 below) .

Figure 7-10: Configuring Tel-to-IP Routing to ITSPs in Tel to IP Routing Table Page



	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Dest. IP Group ID	IP Profile ID
1	1	0[3,4,5]	*			1	
2	1	0[6,7,8]	*			2	
3	1	02	*		10.13.4.13		

7.15 Working with Supplementary Services

The device supports the following supplementary services:

- Call Hold and Retrieve (refer to "Call Hold and Retrieve" on page 377).
- Call Transfer (refer to "Call Transfer" on page 377).
- Call Forward: when a callRerouting IE is received in a FACILITY message in response to an outgoing SETUP message, the device sends a 3xx response to the IP side, including the callRerouting destination number - only applicable to QSIG protocol
- Call Waiting

The device SIP users are only required to enable the Hold and Transfer features. By default, the Call Forward (supporting 30x redirecting responses) and Call Waiting (receipt of 182 response) features are enabled.

Notes:

- All call participants must support the specific supplementary service that is used.
- When working with certain application servers (such as BroadSoft's BroadWorks) in client server mode (the application server controls all supplementary services and keypad features by itself), the device's supplementary services must be disabled.

7.15.1 Call Hold and Retrieve

Hold and Retrieve:

- The party that initiates the hold is called the *holding* party; the other party is called the *held* party. The device can't initiate Call Hold, but it can respond to hold requests and as such, it's a help party.
- After a successful Hold, the holding party hears a Dial tone (HELD_TONE defined in the device's Call Progress Tones file).
- After a successful retrieve, the voice is connected again.
- The hold and retrieve functionalities are implemented by Re-INVITE messages. The IP address 0.0.0.0 as the connection IP address or the string 'a=inactive' in the received Re-INVITE SDP cause the device to enter Hold state and to play the Held tone (configured in the device) to the PBX/PSTN. If the string 'a=sendonly' is received in the SDP message, the device stops sending RTP packets, but continues to listen to the incoming RTP packets. Usually, the remote party plays, in this scenario, Music on Hold (MOH) and the device forwards the MOH to the held party.

You can also configure the device to keep a call on-hold for a user-defined time after which the call is disconnected, using the *ini* file parameter HeldTimeout (refer to "Supplementary Services" on page 159).

7.15.2 Call Transfer

There are two types of call transfers:

- **Consultation Transfer:**

  The common way to perform a consultation transfer is as follows:

  In the transfer scenario there are three parties: Party A = transferring, Party B = transferred, Party C = transferred to.

  - A Calls B.
  - B answers.
  - A presses the hook-flash button and places B on-hold (party B hears a hold tone).
  - A dials C.
  - After A completes dialing C, A can perform the transfer by on-hooking the A phone.
  - After the transfer is complete, B and C parties are engaged in a call.

  The transfer can be initiated at any of the following stages of the call between A and C:

  - Just after completing dialing C phone number - transfer from setup.
  - While hearing Ringback – transfer from alert.
  - While speaking to C - transfer from active.

- **Blind Transfer:**

  Blind transfer is performed after we have a call between A and B, and party A decides to immediately transfer the call to C without speaking with C. The result of the transfer is a call between B and C (just like consultation transfer only skipping the consultation stage).

Note: The device doesn't initiate call transfer, it only responds to call transfer requests.

8 Networking Capabilities

8.1 Ethernet Interface Configuration

The device's Ethernet connection can be configured (using the *ini* file parameter EthernetPhyConfiguration) for one of the following modes:

- **Manual mode:**
  - 10Base-T Half-Duplex or 10Base-T Full-Duplex
  - 100Base-TX Half-Duplex or 100Base-TX Full-Duplex
- **Auto-Negotiation:** chooses common transmission parameters such as speed and duplex mode

The Ethernet connection should be configured according to the following recommended guidelines:

- When the device's Ethernet port is configured for Auto-Negotiation, the opposite port must also operate in Auto-Negotiation. Auto-Negotiation falls back to Half-Duplex mode when the opposite port is not in Auto-Negotiation mode, but the speed (i.e., 10/100Base-T or 1000Base-TX) in this mode is always configured correctly. Configuring the device to Auto-Negotiation mode while the opposite port is set manually to Full-Duplex is invalid as it causes the device to fall back to Half-Duplex mode while the opposite port is Full-Duplex. Any mismatch configuration can yield unexpected functioning of the Ethernet connection.
- When configuring the device's Ethernet port manually, the same mode (i.e., Half Duplex or Full Duplex) and speed must be configured on the remote Ethernet port. In addition, when the device's Ethernet port is configured manually, it is invalid to set the remote port to Auto-Negotiation**.** Any mismatch configuration can yield unexpected functioning of the Ethernet connection.
- It's recommended to configure the port for best performance and highest bandwidth (i.e., Full Duplex with 100Base-TX), but at the same time adhering to the guidelines listed above.

Note that when remote configuration is performed, the device should be in the correct Ethernet setting prior to the time this parameter takes effect. When, for example, the device is configured using BootP/TFTP, the device performs many Ethernet-based transactions prior to reading the *ini* file containing this device configuration parameter. To resolve this problem, the device always uses the last Ethernet setup mode configured. In this way, if you want to configure the device to operate in a new network environment in which the current Ethernet setting of the device is invalid, you should first modify this parameter in the current network so that the new setting holds next time the device is restarted. After reconfiguration has completed, connect the device to the new network and restart it. As a result, the remote configuration process that occurs in the new network uses a valid Ethernet configuration.

8.2 Ethernet Interface Redundancy

The device supports an Ethernet redundancy scheme. At the beginning of the start-up procedure, the device tests whether the 'primary' Ethernet interface is connected, by checking the existence of the Ethernet link carrier. If it's connected, the start-up procedure commences as usual. If not, the start-up application tries the 'secondary' Ethernet interface. If this interface is connected, the whole start-up procedure is performed using it. If both interfaces are not connected, the start-up procedure commences using the parameters, tables, and software residing on the device's non-volatile memory. Note that Ethernet switchover occurs only once during the start-up procedure (at the beginning). If the Ethernet interface fails after the selection is made, the device does not switch over to the second port.

After start-up is complete and the operational software is running, the device continues to use the Ethernet port used for software upload. The device switches over from one Ethernet port to the other each time an Ethernet link carrier-loss is detected on the active Ethernet port, and if the Ethernet link of the other port is operational. Switchover occurs only once per link loss (i.e., the 'secondary' interface stays the active one even if the 'primary' interface has returned to life). After start-up, the device generates a gratuitous ARP message each time a switchover occurs.

For correct functionality of the redundancy mechanism, it's recommended to configure both links to the same mode. It is essential that both link partners (primary and secondary) have the same capabilities. This ensures that whenever a switchover occurs, the device is able to provide at least the same Ethernet services as were provided prior to the switchover. In addition, it's recommended to set the physical secondary link prior to resetting the device (since the MAC configuration cannot be changed thereafter).

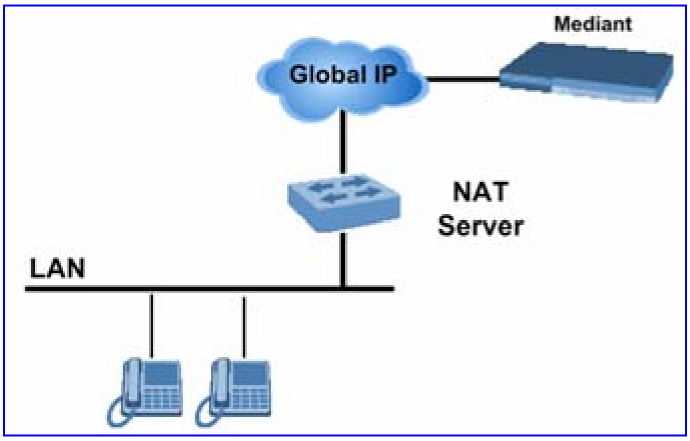
Note that since the two Ethernet ports use the same MAC address, the external switches connected to the device can in some cases create a noticeable switchover delay due to their internal switching logic, though at the device level, the switchover delay is minimal (milliseconds).

8.3 NAT (Network Address Translation) Support

Network Address Translation (NAT) is a mechanism that maps a set of internal IP addresses used within a private network to global IP addresses, providing transparent routing to end hosts. The primary advantages of NAT include (1) Reduction in the number of global IP addresses required in a private network (global IP addresses are only used to connect to the Internet); (2) Better network security by hiding its internal architecture.

The following figure illustrates the device's supported NAT architecture.

Figure 8-1: NAT Architecture



The design of SIP creates a problem for VoIP traffic to pass through NAT. SIP uses IP addresses and port numbers in its message body and the NAT server can't modify SIP messages and therefore, can't change local to global addresses. Two different streams traverse through NAT: signaling and media. A device (located behind a NAT) that initiates a signaling path has problems in receiving incoming signaling responses (they are blocked by the NAT server). Furthermore, the initiating device must notify the receiving device where to send the media.

To resolve these issues, the following mechanisms are available:

- STUN (refer to "STUN" on page 381)
- First Incoming Packet Mechanism (refer to "First Incoming Packet Mechanism" on page 382)
- RTP No-Op packets according to the avt-rtp-noop draft (refer to "No-Op Packets" on page 382)

For information on SNMP NAT traversal, refer to the *Product Reference Manual*.

8.3.1 STUN

Simple Traversal of UDP through NATs (STUN), based on RFC 3489 is a client / server protocol that solves most of the NAT traversal problems. The STUN server operates in the public Internet and the STUN clients are embedded in end-devices (located behind NAT). STUN is used both for the signaling and the media streams. STUN works with many existing NAT types and does not require any special behavior.

STUN enables the device to discover the presence (and types) of NATs and firewalls located between it and the public Internet. It provides the device with the capability to determine the public IP address and port allocated to it by the NAT. This information is later embedded in outgoing SIP / SDP messages and enables remote SIP user agents to reach the device. It also discovers the binding lifetime of the NAT (the refresh rate necessary to keep NAT 'Pinholes' open).

On startup, the device sends a STUN Binding Request. The information received in the STUN Binding Response (IP address:port) is used for SIP signaling. This information is updated every user-defined period (NATBindingDefaultTimeout).

At the beginning of each call and if STUN is required (i.e., not an internal NAT call), the media ports of the call are mapped. The call is delayed until the STUN Binding Response (that includes a global IP:port) for each media (RTP, RTCP and T.38) is received.

To enable STUN, perform the following:

- Enable the STUN feature using either the Web interface (refer to "Configuring the Application Settings" on page 57) or the *ini* file (set EnableSTUN to 1).
- Define the STUN server address using one of the following methods:
  - Define the IP address of the primary and the secondary (optional) STUN servers using either the Web interface (refer to "Configuring the Application Settings" on page 57) or the *ini* file (STUNServerPrimaryIP and STUNServerSecondaryIP). If the primary STUN server isn't available, the device attempts to communicate with the secondary server.
  - Define the domain name of the STUN server using the *ini* file parameter StunServerDomainName. The STUN client retrieves all STUN servers with an SRV query to resolve this domain name to an IP address and port, sort the server list, and use the servers according to the sorted list.
- Use the *ini* file parameter NATBindingDefaultTimeout to define the default NAT binding lifetime in seconds. STUN is used to refresh the binding information after this time expires.

Notes:

- STUN only applies to UDP (doesn't support TCP and TLS).
- STUN can't be used when the device is located behind a symmetric NAT.
- Use either the STUN server IP address (STUNServerPrimaryIP) or domain name (STUNServerDomainName) method, with priority to the first one.

8.3.2 First Incoming Packet Mechanism

If the remote device resides behind a NAT device, it's possible that the device can activate the RTP/RTCP/T.38 streams to an invalid IP address / UDP port. To avoid such cases, the device automatically compares the source address of the incoming RTP/RTCP/T.38 stream with the IP address and UDP port of the remote device. If the two are not identical, the transmitter modifies the sending address to correspond with the address of the incoming stream. The RTP, RTCP and T.38 can thus have independent destination IP addresses and UDP ports.

You can disable the NAT mechanism by setting the *ini* file parameter DisableNAT to 1. The two parameters EnableIpAddrTranslation and EnableUdpPortTranslation allow you to specify the type of compare operation that occurs on the first incoming packet. To compare only the IP address, set EnableIpAddrTranslation to 1, and EnableUdpPortTranslation to 0. In this case, if the first incoming packet arrives with only a difference in the UDP port, the sending addresses won't change. If both the IP address and UDP port need to be compared, then both parameters need to be set to 1.

8.3.3 No-Op Packets

The device's No-Op packet support can be used to verify Real-Time Transport Protocol (RTP) and T.38 connectivity, and to keep NAT bindings and Firewall pinholes open. The No-Op packets are available for sending in RTP and T.38 formats.

You can control the activation of No-Op packets by using the *ini* file parameter NoOpEnable. If No-Op packet transmission is activated, you can control the time interval in which No-Op packets are sent in the case of silence (i.e., no RTP or T.38 traffic). This is performed using the *ini* file parameter NoOpInterval. For a description of the RTP No-Op *ini* file parameters, refer to "Networking Parameters" on page 260.

- **RTP No-Op:** The RTP No-Op support complies with IETF's draft-wing-avt-rtp-noop-03.txt (titled 'A No-Op Payload Format for RTP'). This IETF document defines a No-Op payload format for RTP. The draft defines the RTP payload type as dynamic. You can control the payload type with which the No-Op packets are sent. This is performed using the RTPNoOpPayloadType *ini* parameter (refer to "Networking Parameters" on page 260). AudioCodes' default payload type is 120.
- **T.38 No-Op:** T.38 No-Op packets are sent only while a T.38 session is activated. Sent packets are a duplication of the previously sent frame (including duplication of the sequence number).

Note: Receipt of No-Op packets is always supported.

8.4 IP Multicasting

The device supports IP Multicasting level 1 according to RFC 2236 (i.e., IGMP version 2) for RTP channels. The device is capable of transmitting and receiving Multicast packets.

8.5 Robust Reception of RTP Streams

This mechanism filters out unwanted RTP streams that are sent to the same port number on the device. These multiple RTP streams can result from traces of previous calls, call control errors, and deliberate attacks. When more than one RTP stream reaches the device on the same port number, the device accepts only one of the RTP streams and rejects the rest of the streams.

The RTP stream is selected according to the following: The first packet arriving on a newly opened channel sets the source IP address and UDP port from which further packets are received. Thus, the source IP address and UDP port identify the currently accepted stream. If a new packet arrives whose source IP address or UDP port are different to the currently accepted RTP stream, one of the following occurs:

- The device reverts to the new RTP stream when the new packet has a source IP address and UDP port that are the same as the remote IP address and UDP port that were stated during the opening of the channel.
- The packet is dropped when the new packet has any other source IP address and UDP port.

8.6 Multiple Routers Support

Multiple routers support is designed to assist the device when it operates in a multiple routers network. The device learns the network topology by responding to Internet Control Message Protocol (ICMP) redirections and caches them as routing rules (with expiration time).

When a set of routers operating within the same subnet serve as devices to that network and intercommunicate using a dynamic routing protocol, the routers can determine the shortest path to a certain destination and signal the remote host the existence of the better route. Using multiple router support, the device can utilize these router messages to change its next hop and establish the best path.

Note: Multiple Routers support is an integral feature that doesn’t require configuration.

8.7 Simple Network Time Protocol Support

The Simple Network Time Protocol (SNTP) client functionality generates requests and reacts to the resulting responses using the NTP version 3 protocol definitions (according to RFC 1305). Through these requests and responses, the NTP client synchronizes the system time to a time source within the network, thereby eliminating any potential issues should the local system clock 'drift' during operation. By synchronizing time to a network time source, traffic handling, maintenance, and debugging become simplified for the network administrator.

The NTP client follows a simple process in managing system time: the NTP client requests an NTP update, receives an NTP response, and then updates the local system clock based on a configured NTP server within the network.

The client requests a time update from a specified NTP server at a specified update interval. In most situations, this update interval is every 24 hours based on when the system was restarted. The NTP server identity (as an IP address) and the update interval are user-defined using either the Web interface (refer to "Configuring the Application Settings" on page 57), the *ini* file (NTPServerIP and NTPUpdateInterval respectively), or an SNMP MIB object (refer to the *Product Reference Manual*).

When the client receives a response to its request from the identified NTP server, it must be interpreted based on time zone or location offset that the system is to a standard point of reference called the Universal Time Coordinate (UTC). The time offset that the NTP client uses is configurable using the Web interface (refer to "Configuring the Application Settings" on page 57), the *ini* file (NTPServerUTCOffset), or via an SNMP MIB object (refer to the *Product Reference Manual*).

If required, the clock update is performed by the client as the final step of the update process. The update is performed in such a way as to be transparent to the end users. For instance, the response of the server may indicate that the clock is running too fast on the client. The client slowly robs bits from the clock counter to update the clock to the correct time. If the clock is running too slow, then in an effort to catch the clock up, bits are added to the counter, causing the clock to update quicker and catch up to the correct time. The advantage of this method is that it does not introduce any disparity in the system time that is noticeable to an end user or that could corrupt call timeouts and timestamps.

8.8 IP QoS via Differentiated Services (DiffServ)

DiffServ is an architecture providing different types or levels of service for IP traffic. DiffServ (according to RFC 2474) offers the capability to prioritize certain traffic types depending on their priority, thereby, accomplishing a higher-level QoS at the expense of other traffic types. By prioritizing packets, DiffServ routers can minimize transmission delays for time-sensitive packets such as VoIP packets.

The device can be configured to set a different DiffServ value to IP packets according to their class-of-service: Network, Premium Media, Premium Control, Gold, and Bronze. The DiffServ parameters are described in "Networking Parameters" on page 260.

For the mapping of an application to its class-of-service, refer to "IEEE 802.1p/Q (VLANs and Priority)" on page 385.

8.9 VLANS and Multiple IPs

8.9.1 Multiple IPs

Media, Control, and Management (OAMP) traffic in the device can be assigned one of the following IP addressing schemes:

- **Single IP address for all traffic** (i.e., for Media, Control, and OAMP).
- **Separate IP address for each of the three traffic types:** The different traffic types are separated into three dedicated networks. Instead of a single IP address, the device is assigned three IP addresses and subnet masks, each relating to a different traffic type. This architecture enables you to integrate the device into a three-network environment that is focused on security and segregation. Each entity in the device (e.g., Web and RTP) is mapped to a single traffic type (according to the table in "IEEE 802.1p/Q (VLANs and Priority)" on page 385) in which it operates.

- **Dual IP mode:** The device is assigned two IP addresses for the different traffic types. One IP address is assigned to a combination of two traffic types (Media and Control, OAMP and Control, or OAMP and Media), while the other IP address is assigned to whichever traffic type not included in this combination. For example, a typical scenario using this mode includes one IP address assigned to Control and OAMP, and another IP address assigned to Media.

For detailed information on integrating the device into a VLAN and multiple IPs network, refer to "Getting Started with VLANS and Multiple IPs" on page 387. For detailed information on configuring the multiple IP parameters, refer to "Networking Parameters" on page 260.

Notes:

- A default Gateway is supported only for the Media traffic type; for Control and OAM traffic, use the 'IP Routing' table (refer to "Configuring the IP Routing Table" on page 62).
- The IP address and subnet mask used in the Single IP Network mode are used for the OAM traffic type in the Multiple IP Network mode.

8.9.2 IEEE 802.1p/Q (VLANs and Priority)

The Virtual Local Area Network (VLAN) mechanism enables the device to be integrated into a VLAN-aware environment that includes switches, routers and endpoints. When in VLAN-enabled mode, each packet is tagged with values that specify its priority (class-of-service / IEEE 802.1p) and the identifier (traffic type) of the VLAN to which it belongs (Media, Control, or OAMP / IEEE 802.1Q).

The class-of-service (CoS) mechanism can be utilized to accomplish Ethernet Quality of Service (QoS). Packets sent by the device to the Ethernet network are divided into five different-priority classes (Network, Premium Media, Premium Control, Gold, and Bronze). The priority of each class is determined by a corresponding *ini* file parameter.

Traffic type tagging can be used to implement Layer 2 VLAN security. By discriminating traffic into separate and independent domains, the information is preserved within the VLAN. Incoming packets received from an incorrect VLAN are discarded.

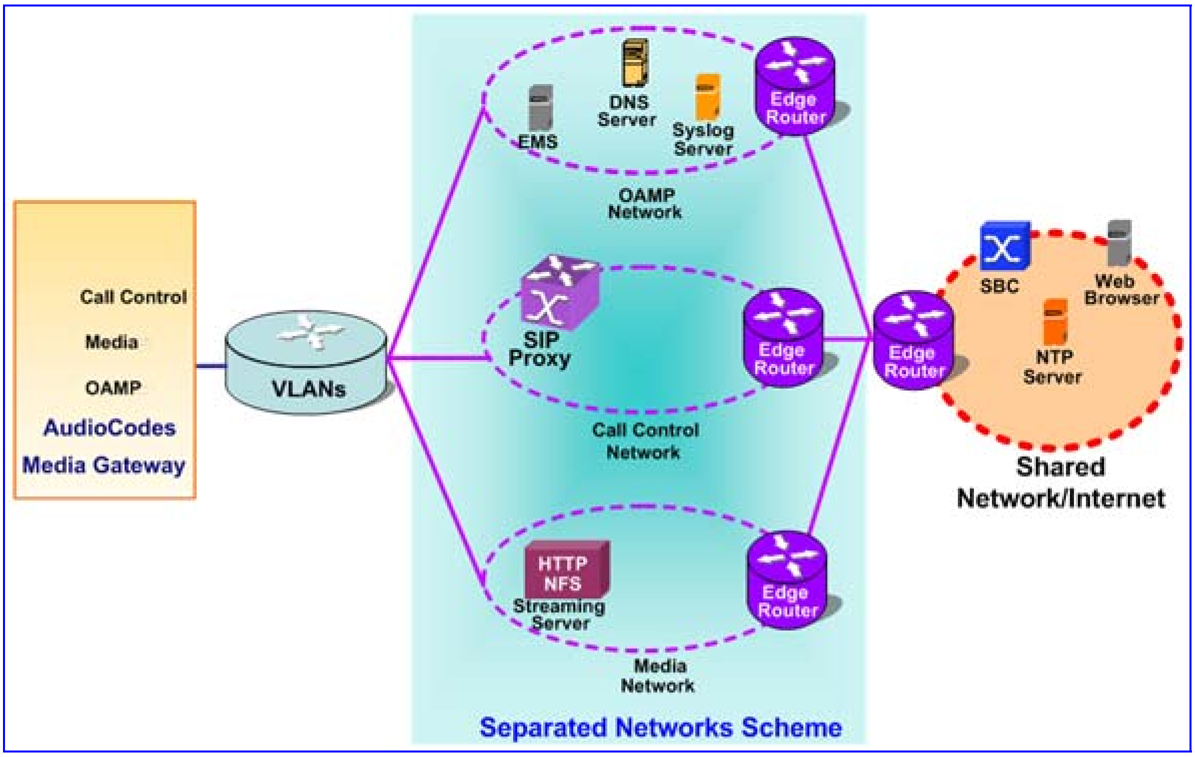
The traffic tagging mechanism is as follows:

- **Outgoing packets (from the device to the switch):** All outgoing packets are tagged, each according to its interface (Control, Media or OAMP). If the device’s native VLAN ID is identical to one of the other IDs (usually to the OAMP's VLAN ID), this ID (e.g., OAMP) is set to zero on outgoing packets (VlanSendNonTaggedOnNative set to 0). This method is called Priority Tagging (p tag without Q tag). If the parameter VlanSendNonTaggedOnNative is set to 1, the device sends regular packets (with no VLAN tag).

- **Incoming packets (from the switch to the device):** The switch sends all packets intended for the device (according to the switch’s configuration) to the device without altering them. For packets whose VLAN ID is identical to the switch’s PVID, the switch removes the tag and sends a packet. The device accepts only packets that have a VLAN ID identical to one of its interfaces (Control, Media or OAMP). Packets with a VLAN ID that is 0 or untagged packets are accepted only if the device’s native VLAN ID is identical to the VLAN ID of one of its interfaces. In this case, the packets are sent to the relevant interface. All other packets are rejected.

Media traffic type is assigned 'Premium media' CoS, Management traffic type is assigned 'Bronze' CoS, and Control traffic type is assigned 'Premium control' CoS. For example, RTP/RTCP traffic is assigned the Media VLAN ID and 'Premium media' CoS, whereas Web traffic is assigned the Management VLAN ID and 'Bronze' CoS. Each of these parameters can be configured with a 802.1p/Q value: traffic type to VLAN ID, and CoS to 802.1p priority.

Figure 8-2: Multiple Network Interfaces and VLANs



Notes:

- For security, the VLAN mechanism is activated only when the device is loaded from the flash memory. Therefore, when using BootP: Load an *ini* file with VlanMode set to 1 and SaveConfiguration set to 1. Then (after the device is active) reset the device with TFTP disabled or by using any method except for BootP.
- For information on how to configure VLAN parameters, refer to "Configuring the IP Settings" on page 50.
-
- The device must be connected to a VLAN-aware switch and the switch's PVID must be equal to the device's native VLAN ID.

The mapping of an application to its CoS and traffic type is shown in the table below:

Table 8-1: Traffic / Network Types and Priority

Application	Traffic / Network Types	Class-of-Service (Priority)
Debugging interface	Management	Bronze
Telnet	Management	Bronze

Application	Traffic / Network Types	Class-of-Service (Priority)
DHCP	Management	Network
Web server (HTTP)	Management	Bronze
SNMP GET/SET	Management	Bronze
Web server (HTTPS)	Management	Bronze
IPSec IKE	Determined by the service	Determined by the service
RTP traffic	Media	Premium media
RTCP traffic	Media	Premium media
T.38 traffic	Media	Premium media
SIP	Control	Premium control
SIP over TLS (SIPS)	Control	Premium control
Syslog	Management	Bronze
ICMP	Management	Determined by the initiator of the request
ARP listener	Determined by the initiator of the request	Network
SNMP Traps	Management	Bronze
DNS client	DNS (EnableDNSasOAM)	Network
NTP	NTP (EnableNTPasOAM)	Depends on traffic type: ▪ Control: Premium control ▪ Management: Bronze
NFS	NFSServers_VlanType in the NFSServers table	Gold

8.9.3 Getting Started with VLANS and Multiple IPs

By default, the device operates without VLANs and multiple IPs, using a single IP address, subnet mask and default Gateway IP address. This section provides an example of the configuration required to integrate the device into a multiple IPs network withVLANs, using the Web interface (refer to "Integrating Using the Web Interface" on page 388) and *ini* file (refer to "Integrating Using the ini File" on page 390). The following table shows an example configuration used in this subsection:

Table 8-2: Example of VLAN and Multiple IPs Configuration

Network Type	IP Address	Subnet Mask	Default Gateway IP Address	VLAN ID	External Routing Rule
OAMP	10.31.174.50	255.255.0.0	0.0.0.0	4	83.4.87.X
Control	10.32.174.50	255.255.0.0	0.0.0.0	5	130.33.4.6
Media	10.33.174.50	255.255.0.0	10.33.0.1	6	--

Notes:

- The values provided in this section are only used as an example.
- Since a default Gateway is available only for the Media network, for the device to be able to communicate with an external device/network on its OAMP and Control networks, IP routing rules must be used.

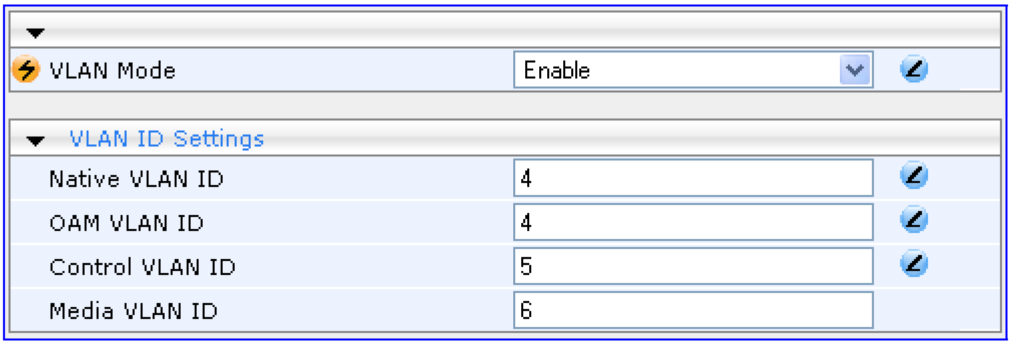
8.9.3.1 Integrating Using the Web Interface

The procedure below describes how to integrate the device into a multiple IPs network withVLANs, using the Web interface.

➢ **To integrate the device into a multiple IPs network withVLANs using the Web interface, take these 6 steps:**

1. Access the Web interface (refer to "Accessing the Web Interface" on page 20).
2. Use the Software Upgrade Wizard (refer to "Software Upgrade Wizard" on page 236) to load and *burn* the firmware version to the device (VLANs and multiple IPs support is available only when the firmware is burned to flash).
3. Configure the VLAN parameters by completing the following steps:
   a. Open the 'IP Settings' page (refer to "Configuring the IP Settings" on page 50).
   b. Modify the VLAN parameters to correspond to the values shown in the following figure:

Figure 8-3: VLAN Configuration in the IP Settings Page



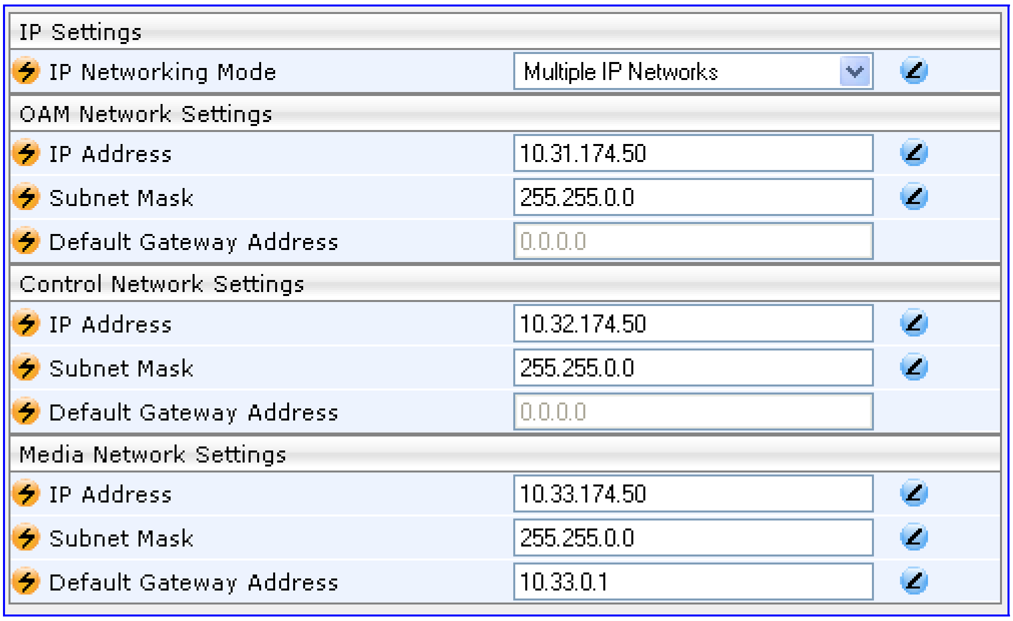
VLAN Mode	Enable
VLAN ID Settings	
Native VLAN ID	4
OAM VLAN ID	4
Control VLAN ID	5
Media VLAN ID	6

   c. Click the **Submit** button to save your changes.

4. Configure the multiple IP parameters by completing the following steps:

a. In the ‘IP Settings’ page, modify the IP parameters to correspond to the values shown in the figure below. Note that the OAM, Control, and Media Network Settings parameters appear only after you select the options ‘Multiple IP Networks’ or 'Dual IP' in the field ‘IP Networking Mode’.

Figure 8-4: OAM, Control, Media IP Configuration in the IP Settings Page

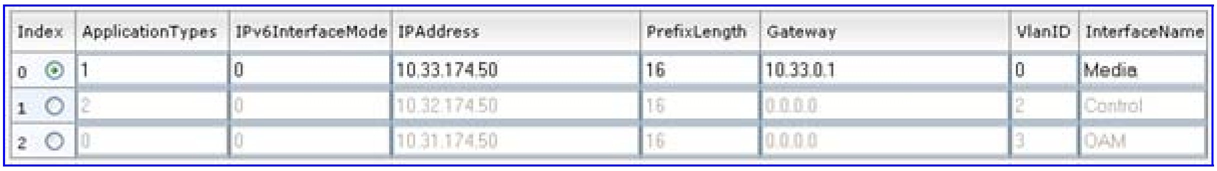


IP Settings

IP Networking Mode	Multiple IP Networks
OAM Network Settings	
IP Address	10.31.174.50
Subnet Mask	255.255.0.0
Default Gateway Address	0.0.0.0
Control Network Settings	
IP Address	10.32.174.50
Subnet Mask	255.255.0.0
Default Gateway Address	0.0.0.0
Media Network Settings	
IP Address	10.33.174.50
Subnet Mask	255.255.0.0
Default Gateway Address	10.33.0.1

Instead of configuring in the ‘IP Settings’ page, you can use the 'Multiple Interface Table' page, which is accessed from the ‘IP Settings’ page by clicking the right-arrow ➡ button alongside the label 'Multiple Interface Table' (refer to "Configuring the Multiple Interface Table" on page 53). The 'Multiple Interface Table' page provides greater configuration flexibility whereby you can also assign VLANs to the different interfaces.

Figure 8-5: Multiple Interface Table Page



Index		ApplicationTypes	IPv6InterfaceMode	IPAddress	PrefixLength	Gateway	VlanID	InterfaceName
0	●	1	0	10.33.174.50	16	10.33.0.1	0	Media
1	○	2	0	10.32.174.50	16	0.0.0.0	2	Control
2	○	0	0	10.31.174.50	16	0.0.0.0	3	OAM

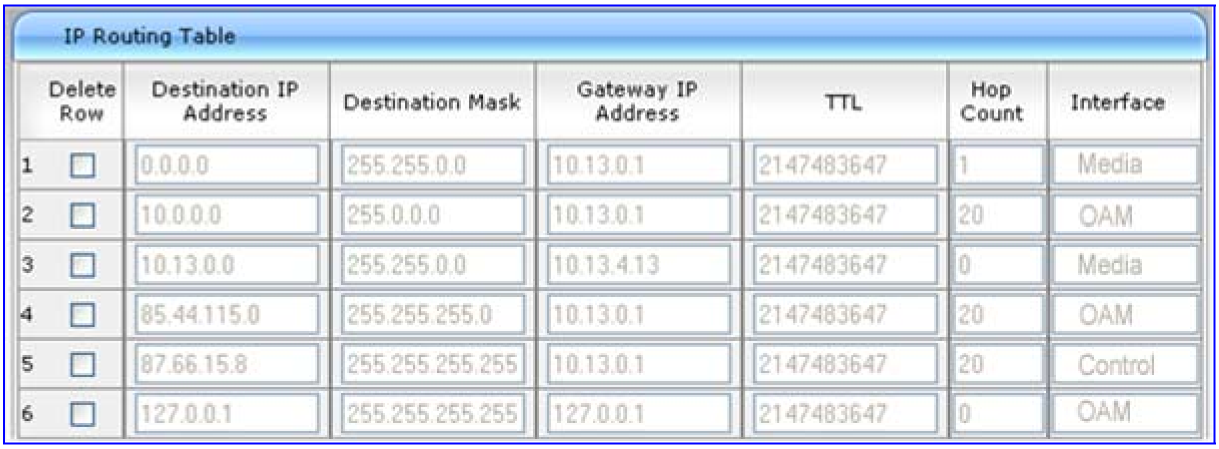
b. Click the **Submit** button to save your changes.

Note: Configure the OAM parameters only if the OAM networking parameters are different from the networking parameters used in the Single IP Network mode.

5. Configure the 'IP Routing' table to define static routing rules for the OAMP and Control networks, since a default gateway isn’t supported on these networks:

a. Open the ‘IP Routing Table’ page (refer to "Configuring the IP Routing Table" on page 62).

Figure 8-6: Static Routes for OAM/Control in IP Routing Table



IP Routing Table

	Delete Row	Destination IP Address	Destination Mask	Gateway IP Address	TTL	Hop Count	Interface
1	□	0.0.0.0	255.255.0.0	10.13.0.1	2147483647	1	Media
2	□	10.0.0.0	255.0.0.0	10.13.0.1	2147483647	20	OAM
3	□	10.13.0.0	255.255.0.0	10.13.4.13	2147483647	0	Media
4	□	85.44.115.0	255.255.255.0	10.13.0.1	2147483647	20	OAM
5	□	87.66.15.8	255.255.255.255	10.13.0.1	2147483647	20	Control
6	□	127.0.0.1	255.255.255.255	127.0.0.1	2147483647	0	OAM

b. Use the **Add New Entry** to add the routing rules listed in the following table:

Destination IP Address	Destination Mask	Gateway IP Address	Hop Count	Interface
87.66.15.8	255.255.255.255	10.13.0.1	20	Control
85.44.115.50	255.255.255.0	10.31.0.1	20	OAMP

6. Save your changes to flash memory (refer to "Saving Configuration" on page 230) and reset the device (refer to "Resetting the Device" on page 228).

8.9.3.2 Integrating Using the ini File

The procedure below describes how to integrate the device into a multiple IPs network with VLANs, using the *ini* file. The procedure below is based on the example setup described in "Getting Started with VLANS and Multiple IPs" on page 387.

➢ To integrate the device into a multiple IPs network withVLANs using the *ini* file, take these 3 steps:

1. Prepare an *ini* file (using the *ini* file table parameter InterfaceTable) with relevant parameters:

   - If the BootP/TFTP utility and the OAMP interface are located on the same network, the Native VLAN ID (VlanNativeVlanId) must be equal to the OAMP VLAN ID (VlanOamVlanId), which in turn must be equal to the PVID of the switch port to which the device is connected. Therefore, set the PVID of the switch port to 4 (in this example).
   - Configure the OAMP parameters only if the OAMP networking parameters are different from the networking parameters used in the Single IP Network mode.
   - The 'IP Routing' table is required to define static routing rules for the OAMP and Control networks since a default Gateway isn’t supported for these networks.

Below is an example of an *ini* file containing VLAN and Multiple IPs parameters:

```
; Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable IPv6InterfaceMode, InterfaceTable IPAddress,
InterfaceTable PrefixLength, InterfaceTable Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0 = 0, 0, 10.31.174.50, 16, 0.0.0.0, 4, OAMP;
InterfaceTable 0 = 1, 0, 10.33.174.50, 16, 10.33.0.1, 6, Media;
InterfaceTable 0 = 2, 0, 10.32.174.50, 16, 0.0.0.0, 5, Control;
[\InterfaceTable]
; VLAN related parameters:
VlanMode = 1
VlanNativeVlanId=4
; Routing Table Configuration:
; IP Routing table parameters
RoutingTableDestinationsColumn = 130.33.4.6, 83.4.87.6
RoutingTableDestinationMasksColumn = 255.255.255.255 ,
255.255.255.0
RoutingTableGatewaysColumn = 10.32.0.1 , 10.31.0.1
RoutingTableInterfacesColumn = 2,0
RoutingTableHopsCountColumn = 20,20
; Class Of Service parameters:
VlanNetworkServiceClassPriority = 7
VlanPremiumServiceClassMediaPriority = 6
VlanPremiumServiceClassControlPriority = 6
VlanGoldServiceClassPriority = 4
VlanBronzeServiceClassPriority = 2
NetworkServiceClassDiffServ = 48
PremiumServiceClassMediaDiffServ = 46
PremiumServiceClassControlDiffServ = 40
GoldServiceClassDiffServ = 26
BronzeServiceClassDiffServ = 10
; Application Type for applications:
EnableDNSasOAM = 1
EnableSCTPasControl = 1
EnableNTPasOAM = 1
```

2. Use the BootP/TFTP utility (refer to the *Product Reference Manual*) to load and *burn* the firmware version and the *ini* file you prepared in the previous step to the device (multiple IPs and VLANs support is available only when the firmware is burned to flash).

3. Reset the device after disabling it on the BootP/TFTP utility.

Instead of using the *ini* file table parameter InterfaceTable, you can configure multiple IPs and VLANs using the individual *ini* file parameters, as shown below:

```
; VLAN Configuration
VlanMode=1
VlanOamVlanId=4
VlanNativeVlanId=4
VlanControlVlanId=5
VlanMediaVlanID=6
; Multiple IPs Configuration
EnableMultipleIPs=1
LocalMediaIPAddress=10.33.174.50
LocalMediaSubnetMask=255.255.0.0
LocalMediaDefaultGW=10.33.0.1
LocalControlIPAddress=10.32.174.50
LocalControlSubnetMask=255.255.0.0
LocalControlDefaultGW=0.0.0.0
LocalOAMPAddress=10.31.174.50
LocalOAMSubnetMask=255.255.0.0
LocalOAMDefaultGW=0.0.0.0
; IP Routing table parameters
RoutingTableDestinationsColumn = 130.33.4.6, 83.4.87.6
RoutingTableDestinationMasksColumn = 255.255.255.255,
255.255.255.0
RoutingTableGatewaysColumn = 10.32.0.1 , 10.31.0.1
RoutingTableInterfacesColumn = 1 , 0
RoutingTableHopsCountColumn = 20,20
```

9 Advanced PSTN Configuration

This section discusses advanced PSTN configurations.

9.1 Clock Settings

In a traditional TDM service network such as PSTN, both ends of the TDM connection must be synchronized. If synchronization is not achieved, voice frames are either dropped (to prevent a buffer overflow condition) or inserted (to prevent an underflow condition). In both cases, connection quality and reliability is affected.

The device's clock settings can be configured to one of the following:

- Generate its own timing signals
- Use an internal clock
- Recover a clock from one of the PSTN E1/T1 trunks

➢ **To use the device's internal clock source, configure the following parameters:**

- TDMBusClockSource = 1
- ClockMaster = 1 (for all trunks)

➢ **To use the recovered clock option, configure the following parameters:**

- TDMBusClockSource = 4
- ClockMaster_x = 0 (for all ‘slave’ trunks connected to PBX#1)
- ClockMaster_x = 1 (for all ‘master’ trunks connected to PBX#2)

The above assumes that the device recovers its internal clock from one of the ‘slave’ trunks connected to PBX#1 and provides clock to PBX#2 on its ‘master’ trunks. In addition, it's necessary to define from which of the ‘slave’ trunks the device recovers its clock:

- TDMBusPSTNAutoClockEnable = 1 (device automatically selects one of the connected ‘slave’ trunks)
  - Or -
- TDMBusLocalReference = # (trunk number, where 0 is the first trunk - and the default)

Notes:

- To configure the TDM Bus Clock Source parameters using the Web interface, refer to "Configuring the TDM Bus Settings" on page 218.
- When the device is used in a ‘non-span’ configuration, the internal device clock must be used (as explained above).

9.2 Release Reason Mapping

This section describes the available mapping mechanisms of SIP responses to Q.850 Release Causes and vice versa. The existing mapping of ISDN Release Causes to SIP Responses is described in "Fixed Mapping of ISDN Release Reason to SIP Response" on page 394 and "Fixed Mapping of SIP Response to ISDN Release Reason" on page 396. To override this hard-coded mapping and flexibly map SIP responses to ISDN Release Causes, use the *ini* file (CauseMapISDN2SIP and CauseMapSIP2ISDN, as described in "ISDN and CAS Interworking-Related Parameters" on page 307) or the Web interface (refer to "Release Cause Mapping" on page 189).

It is also possible to map the less commonly used SIP responses to a single default ISDN Release Cause. Use the parameter DefaultCauseMapISDN2IP (described in "ISDN and CAS Interworking-Related Parameters" on page 307) to define a default ISDN Cause that is always used except when the following Release Causes are received: Normal Call Clearing (16), User Busy (17), No User Responding (18) or No Answer from User (19). This mechanism is only available for Tel-to-IP calls.

9.2.1 Reason Header

The device supports the Reason header according to RFC 3326. The Reason header conveys information describing the disconnection cause of a call:

- **Sending Reason header:** If a call is disconnected from the Tel side (ISDN), the Reason header is set to the received Q.850 cause in the appropriate message (BYE / CANCEL / final failure response) and sent to the SIP side. If the call is disconnected because of a SIP reason, the Reason header is set to the appropriate SIP response.
- **Receiving Reason header:** If a call is disconnected from the IP side and the SIP message includes the Reason header, it is sent to the Tel side according to the following logic:
  - If the Reason header includes a Q.850 cause, it is sent as is.
  - If the Reason header includes a SIP response:
    - If the message is a final response, the response status code is translated to Q.850 format and passed to ISDN.
    - If the message isn’t a final response, it is translated to a Q.850 cause.
  - When the Reason header is received twice (i.e., SIP Reason and Q.850), the Q.850 takes precedence over the SIP reason and is sent to the Tel side.

9.2.2 Fixed Mapping of ISDN Release Reason to SIP Response

The following table describes the mapping of ISDN release reason to SIP response.

Table 9-1: Mapping of ISDN Release Reason to SIP Response

ISDN Release Reason	Description	SIP Response	Description
1	Unallocated number	404	Not found
2	No route to network	404	Not found
3	No route to destination	404	Not found
6	Channel unacceptable	406*	Not acceptable

ISDN Release Reason	Description	SIP Response	Description
7	Call awarded and being delivered in an established channel	500	Server internal error
16	Normal call clearing	-*	BYE
17	User busy	486	Busy here
18	No user responding	408	Request timeout
19	No answer from the user	480	Temporarily unavailable
21	Call rejected	403	Forbidden
22	Number changed w/o diagnostic	410	Gone
26	Non-selected user clearing	404	Not found
27	Destination out of order	502	Bad gateway
28	Address incomplete	484	Address incomplete
29	Facility rejected	501	Not implemented
30	Response to status enquiry	501*	Not implemented
31	Normal unspecified	480	Temporarily unavailable
34	No circuit available	503	Service unavailable
38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable
43	Access information discarded	502*	Bad gateway
44	Requested channel not available	503*	Service unavailable
47	Resource unavailable	503	Service unavailable
49	QoS unavailable	503*	Service unavailable
50	Facility not subscribed	503*	Service unavailable
55	Incoming calls barred within CUG	403	Forbidden
57	Bearer capability not authorized	403	Forbidden
58	Bearer capability not presently available	503	Service unavailable
63	Service/option not available	503*	Service unavailable
65	Bearer capability not implemented	501	Not implemented
66	Channel type not implemented	480*	Temporarily unavailable
69	Requested facility not implemented	503*	Service unavailable
70	Only restricted digital information bearer capability is available	503*	Service unavailable
79	Service or option not implemented	501	Not implemented
81	Invalid call reference value	502*	Bad gateway

ISDN Release Reason	Description	SIP Response	Description
82	Identified channel does not exist	502*	Bad gateway
83	Suspended call exists, but this call identity does not	503*	Service unavailable
84	Call identity in use	503*	Service unavailable
85	No call suspended	503*	Service unavailable
86	Call having the requested call identity has been cleared	408*	Request timeout
87	User not member of CUG	503	Service unavailable
88	Incompatible destination	503	Service unavailable
91	Invalid transit network selection	502*	Bad gateway
95	Invalid message	503	Service unavailable
96	Mandatory information element is missing	409*	Conflict
97	Message type non-existent or not implemented	480*	Temporarily not available
98	Message not compatible with call state or message type non-existent or not implemented	409*	Conflict
99	Information element non-existent or not implemented	480*	Not found
100	Invalid information elements contents	501*	Not implemented
101	Message not compatible with call state	503*	Service unavailable
102	Recovery of timer expiry	408	Request timeout
111	Protocol error	500	Server internal error
127	Interworking unspecified	500	Server internal error

***** Messages and responses were created because the 'ISUP to SIP Mapping' draft doesn't specify their cause code mapping.

9.2.3 Fixed Mapping of SIP Response to ISDN Release Reason

The following table describes the mapping of SIP response to ISDN release reason.

Table 9-2: Mapping of SIP Response to ISDN Release Reason

SIP Response	Description	ISDN Release Reason	Description
400*	Bad request	31	Normal, unspecified
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected

SIP Response	Description	ISDN Release Reason	Description
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service/option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication required	21	Call rejected
408	Request timeout	102	Recovery on timer expiry
409	Conflict	41	Temporary failure
410	Gone	22	Number changed w/o diagnostic
411	Length required	127	Interworking
413	Request entity too long	127	Interworking
414	Request URI too long	127	Interworking
415	Unsupported media type	79	Service/option not implemented
420	Bad extension	127	Interworking
480	Temporarily unavailable	18	No user responding
481*	Call leg/transaction doesn't exist	127	Interworking
482*	Loop detected	127	Interworking
483	Too many hops	127	Interworking
484	Address incomplete	28	Invalid number format
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
488	Not acceptable here	31	Normal, unspecified
500	Server internal error	41	Temporary failure
501	Not implemented	38	Network out of order
502	Bad gateway	38	Network out of order
503	Service unavailable	41	Temporary failure
504	Server timeout	102	Recovery on timer expiry
505*	Version not supported	127	Interworking
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number
606*	Not acceptable	38	Network out of order

***** Messages and responses were created because the 'ISUP to SIP Mapping' draft doesn't specify their cause code mapping.

9.3 ISDN Overlap Dialing

Overlap dialing is a dialing scheme used by several ISDN variants to send and / or receive called number digits one after the other (or several at a time). This is in contrast to en-bloc dialing in which a complete number is sent.

The device can optionally support ISDN overlap dialing for incoming ISDN calls for the entire device by setting the *ini* file parameter ISDNRxOverlap to 1, or per E1/T1 span by setting ISDNRxOverlap_x to 1 (where *x* represents the number of the trunk). For configuring ISDN overlap dialing using the Web interface, refer to "Configuring the Trunk Settings" on page 82.

To play a Dial tone to the ISDN user side when an empty called number is received, set ISDNINCallsBehavior = 65536 (bit #16). This results in the Progress Indicator to be included in the SetupAck ISDN message.

The device stops collecting digits (for ISDN-to-IP calls) when:

- The sending device transmits a ‘sending complete’ IE in the ISDN Setup or the following INFO messages to signal that no more digits are going to be sent.
- The inter-digit timeout (configured by the parameter TimeBetweenDigits) expires. The default for this timeout is 4 seconds.
- The maximum allowed number of digits (configured by the parameter MaxDigits) is reached. The default is 30 digits.
- A match is found with the defined digit map (configured by the parameter, DigitMapping).

Relevant parameters (described in "PSTN Parameters" on page 303):

- ISDNRxOverlap
- ISDNRxOverlap_x
- TimeBetweenDigits
- MaxDigits
- ISDNInCallsBehavior
- DigitMapping

9.4 ISDN Non-Facility Associated Signaling (NFAS)

In regular T1 ISDN trunks, a single 64 kbps channel carries signaling for the other 23 B-channels of that particular T1 trunk. This channel is called the D-channel and usually resides on timeslot # 24. The ISDN Non-Facility Associated Signaling (NFAS) feature enables the use of a single D-channel to control multiple PRI interfaces.

With NFAS it is possible to define a group of T1 trunks, called an NFAS group, in which a single D-channel carries ISDN signaling messages for the entire group. The NFAS group’s B-channels are used to carry traffic such as voice or data. The NFAS mechanism also enables definition of a backup D-channel on a different T1 trunk, to be used if the primary D-channel fails.

The NFAS group can comprise up to 10 T1 trunks. Each T1 trunk is called an ‘NFAS member’. The T1 trunk whose D-channel is used for signaling is called the ‘Primary NFAS Trunk’. The T1 trunk whose D-channel is used for backup signaling is called the ‘Backup NFAS Trunk’. The primary and backup trunks each carry 23 B-channels while all other NFAS trunks each carry 24 B-channels.

The device supports up to 9 NFAS groups. Each group must contain different T1 trunks.

The NFAS group is identified by an NFAS GroupID number (possible values are 1 to 9). To assign a number of T1 trunks to the same NFAS group, use the *ini* file parameter NFASGroupNumber_x = groupID (where *x* is the physical trunk ID (0 to the maximum number of trunks) or the Web interface (refer to "Configuring the Trunk Settings" on page 82).

The parameter ‘DchConfig_x = Trunk_type’ defines the type of NFAS trunk. Trunk_type is set to 0 for the primary trunk, to 1 for the backup trunk, and to 2 for an ordinary NFAS trunk. ‘x’ depicts the physical trunk ID (0 to the maximum number of trunks). You can also use the Web interface (refer to "Configuring the Trunk Settings" on page 82).

For example, to assign the first four T1 trunks to NFAS group #1, in which trunk #0 is the primary trunk and trunk #1 is the backup trunk, use the following configuration:

```
NFASGroupNumber 0 = 1
NFASGroupNumber 1 = 1
NFASGroupNumber 2 = 1
NFASGroupNumber 3 = 1
DchConfig 0 = 0             ;Primary T1 trunk
DchConfig 1 = 1             ;Backup T1 trunk
DchConfig 2 = 2             ;24 B-channel NFAS trunk
DchConfig 3 = 2             ;24 B-channel NFAS trunk
```

The NFAS parameters are described in "PSTN Parameters" on page 303.

9.4.1 NFAS Interface ID

Several ISDN switches require an additional configuration parameter per T1 trunk that is called ‘Interface Identifier’. In NFAS T1 trunks, the Interface Identifier is sent explicitly in Q.931 Setup / Channel Identification IE for all NFAS trunks, except for the B-channels of the Primary trunk (refer to note below).

The Interface ID can be defined per member (T1 trunk) of the NFAS group, and must be coordinated with the configuration of the Switch. The default value of the Interface ID is identical to the number of the physical T1 trunk (0 for the first trunk, 1 for the second T1 trunk, and so on, up to the maximum number of trunks).

To define an explicit Interface ID for a T1 trunk (that is different from the default), use the following parameters:

- ISDNIBehavior_x = 512 (x = 0 to the maximum number of trunks identifying the device's physical trunk)
- ISDNNFASInterfaceID_x = ID (x = 0 to 255)

Notes:

- Usually the Interface Identifier is included in the Q.931 Setup/Channel Identification IE only on T1 trunks that doesn’t contain the D-channel. Calls initiated on B-channels of the Primary T1 trunk, by default, don’t contain the Interface Identifier. Setting the parameter ISDNIBehavior_x to 2048’ forces the inclusion of the Channel Identifier parameter also for the Primary trunk.
- The parameter ISDNNFASInterfaceID_x = ID can define the ‘Interface ID’ for any Primary T1 trunk, even if the T1 trunk is not a part of an NFAS group. However, to include the Interface Identifier in Q.931 Setup/Channel Identification IE configure ISDNIBehavior_x = 2048 in the *ini* file.

9.4.2 Working with DMS-100 Switches

The DMS-100 switch requires the following NFAS Interface ID definitions:

- InterfaceID #0 for the Primary trunk
- InterfaceID #1 for the Backup trunk
- InterfaceID #2 for a 24 B-channel T1 trunk
- InterfaceID #3 for a 24 B-channel T1 trunk, and so on for subsequent T1 trunks

For example, if four T1 trunks on a device are configured as a single NFAS group with Primary and Backup T1 trunks that is used with a DMS-100 switch, the following parameters should be used:

```
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0     ;Primary T1 trunk
DchConfig_1 = 1     ;Backup T1 trunk
DchConfig_2 = 2     ;B-Channel NFAS trunk
DchConfig_3 = 2     ;B-channel NFAS trunk
```

If there is no NFAS Backup trunk, the following configuration should be used:

```
ISDNNFASInterfaceID_0 = 0
ISDNNFASInterfaceID_1 = 2
ISDNNFASInterfaceID_2 = 3
ISDNNFASInterfaceID_3 = 4
ISDNIBehavior = 512   ;This parameter should be added because of
;ISDNNFASInterfaceID coniguration above
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0     ;Primary T1 trunk
DchConfig_1 = 2     ;B-Channel NFAS trunk
DchConfig_2 = 2     ;B-Channel NFAS trunk
DchConfig_3 = 2     ;B-channel NFAS trunk
```

9.4.3 Creating an NFAS-Related Trunk Configuration

The procedures for creating and deleting an NFAS group must be performed in the correct order, as described below.

➢ To create an NFAS Group, take these 3 steps:

1. If there's a backup ('secondary') trunk for this group, it must be configured first.
2. Configure the primary trunk before configuring any NFAS ('slave') trunk.
3. Configure NFAS ('slave') trunks.

➢ To stop / delete an NFAS Group, take these 3 steps:

1. Stop or delete (by setting ProtocolType to 0, i.e., 'None') all NFAS ('slave') trunks.
2. Stop or delete (by setting ProtocolType to 0, i.e., 'None') the backup trunk if a backup trunk exists.
3. Stop or delete (by setting ProtocolType to 0, i.e., 'None') the primary trunk.

Notes:

- All trunks in the group must be configured with the same values for trunk parameters TerminationSide, ProtocolType, FramingMethod, and LineCode.
- After stopping or deleting the backup trunk, delete the group and then reconfigure it.
- NFAS groups cannot be configured on-the-fly.

9.5 Redirect Number and Calling Name (Display)

The following tables define the device's redirect number and calling name (Display) support for various PRI variants according to NT (Network Termination) / TE (Termination Equipment) interface direction:

Table 9-3: Calling Name (Display)

NT/TE Interface	DMS-100	NI-2	4/5ESS	Euro ISDN	QSIG
NT-to-TE	Yes	Yes	Yes	Yes	Yes
TE-to-NT	Yes	Yes	Yes	No	Yes

Table 9-4: Redirect Number

NT/TE Interface	DMS-100	NI-2	4/5ESS	Euro ISDN	QSIG
NT-to-TE	Yes	Yes	Yes	Yes	Yes
TE-to-NT	Yes	Yes	Yes	Yes*****	Yes

***** When using ETSI DivertingLegInformation2 in a Facility IE (not Redirecting Number IE).

9.6 Automatic Gain Control (AGC)

Automatic Gain Control (AGC) adjusts the energy of the output signal to a required level (i.e., volume). This feature compensates for near-far gain differences. AGC estimates the energy of the incoming signal (from the IP or PSTN, determined by the parameter AGCRedirection), calculates the essential gain, and then performs amplification. Feedback ensures that the output signal is not clipped. You can define the required Gain Slope in decibels per second (using the parameter AGCGainSlop) and the required signal energy threshold (using the parameter AGCTargetEnergy).

When the AGC first detects an incoming signal, it begins operating in Fast Mode, which allows the AGC to adapt quickly when a conversation starts. This means that the Gain Slope is 8 dB/sec for the first 1.5 seconds. After this period, the Gain Slope is changed to the user-defined value. You can disable or enable the AGC's Fast Mode feature, using the *ini* file parameter AGCDisableFastAdaptation. After Fast Mode is used, the signal should be off for two minutes in order to have the feature turned on again.

To configure AGC, refer to "Configuring the IPmedia Settings" on page 76.

10 Tunneling Applications

This section discusses TDM and QISG tunneling, supported by the device.

10.1 TDM Tunneling

The device's TDM Tunneling feature allows you to tunnel groups of digital trunk spans or timeslots (B-channels) over the IP network. TDM Tunneling utilizes the device's internal routing (without Proxy control) capabilities to receive voice and data streams from TDM (E1/T1/J1/) spans or individual timeslots, convert them into packets, and then transmit them over the IP network (using point-to-point or point-to-multipoint device distributions). A device opposite it (or several devices when point-to-multipoint distribution is used) converts the IP packets back into TDM traffic. Each timeslot can be targeted to any other timeslot within a trunk in the opposite device.

When TDM Tunneling is enabled ('Enable TDM Tunneling' parameter is set to 'Enable' on the originating device -- refer to "Configuring the Digital Gateway Parameters" on page 207), the originating device automatically initiates SIP calls from all enabled B-channels belonging to the E1/T1/J1 spans that are configured with the protocol type ‘Transparent’ (for ISDN trunks) or ‘Raw CAS’ (for CAS trunks). The called number of each call is the internal phone number of the B-channel from where the call originates. The 'IP to Trunk Group Routing' table (refer to "IP to Trunk Group Routing" on page 181) is used to define the destination IP address of the terminating device. The terminating device automatically answers these calls if its E1/T1 protocol type is set to ‘Transparent’ (ProtocolType = 5) or ‘Raw CAS’ (ProtocolType = 3 for T1 and 9 for E1) and the parameter ChannelSelectMode is set to 0 (By Phone Number).

Note: It's possible to configure both devices to also operate in symmetric mode. To do so, set EnableTDMOverIP to 1 and configure the 'Tel to IP Routing' tables in both devices. In this mode, each device (after it's reset) initiates calls to the second device. The first call for each B-channel is answered by the second device.

The device continuously monitors the established connections. If for some reason, one or more calls are released, the device automatically re-establishes these ‘broken’ connections. In addition, when a failure in a physical trunk or in the IP network occurs, the device re-establishes the tunneling connections when the network is restored.

Note: It's recommended to use the keep-alive mechanism for each connection, by activating the ‘session expires’ timeout and using Re-INVITE messages.

By utilizing the ‘Profiles’ mechanism (refer to "Configuring the Profile Definitions" on page 190), you can configure the TDM Tunneling feature to choose different settings based on a timeslot or groups of timeslots. For example, you can use low-bit-rate vocoders to transport voice and ‘Transparent’ coder to transport data (e.g., for D-channel). You can also use Profiles to assign ToS (for DiffServ) per source -- a timeslot carrying data or signaling is assigned a higher priority value than a timeslot carrying voice.

For tunneling of E1/T1 CAS trunks, set the protocol type to 'Raw CAS' (ProtocolType = 3 / 9) and enable RFC 2833 CAS relay mode ('CAS Transport Type' parameter is set to 'CAS RFC2833 Relay' -- refer to "Configuring the Voice Settings" on page 66).

Note: For TDM over IP, the 'Caller ID Transport Type' parameter must be set to 'Disable', i.e., transparent (refer to "Configuring the Fax / Modem / CID Settings" on page 67).

Below is an example of *ini* files for two devices implementing TDM Tunneling for four E1 spans. Note that in this example both devices are dedicated to TDM tunneling.

Terminating Side:

```
EnableTDMOverIP = 1
;E1 TRANSPARENT 31
ProtocolType 0 = 5
ProtocolType 1 = 5
ProtocolType 2 = 5
ProtocolType_3 = 5
[PREFIX]
FORMAT PREFIX Index = PREFIX DestinationPrefix,
PREFIX_DestAddress, PREFIX_SourcePrefix, PREFIX_ProfileId,
PREFIX MeteringCode, PREFIX DestPort;
Prefix 1 = '*,10.8.24.12';
[\PREFIX]

;IP address of the device in the opposite
;location
;Channel selection by Phone number.
ChannelSelectMode = 0
;Profiles can be used do define different coders per B-channels
;such as Transparent
;coder for B-channels (timeslot 16) that carries PRI ;signaling.
[TrunkGroup]
FORMAT TrunkGroup Index = TrunkGroup TrunkGroupNum,
TrunkGroup FirstTrunkId, TrunkGroup LastTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup FirstPhoneNumber, TrunkGroup ProfileId,
TrunkGroup Module;
TrunkGroup 1 = 0,0,0,1,31,1000,1;
TrunkGroup 1 = 0,1,1,1,31,2000,1;
TrunkGroup 1 = 0,2,2,1,31,3000,1;
TrunkGroup 1 = 0,3,3,1,31,4000,1;
TrunkGroup 1 = 0,0,0,16,16,7000,2;
TrunkGroup 1 = 0,1,1,16,16,7001,2;
TrunkGroup 1 = 0,2,2,16,16,7002,2;
TrunkGroup 1 = 0,3,3,16,16,7003,2;
[/TrunkGroup]
[CoderName]
FORMAT CoderName Index = CoderName Type, CoderName PacketInterval,
CoderName rate, CoderName PayloadType, CoderName Sce;
CoderName 0 = 'g7231';
CoderName 1 = 'Transparent';
CoderName 5 = 'g7231';
CoderName 6 = 'Transparent';
[/CoderName]
[TelProfile]
FORMAT TelProfile Index = TelProfile ProfileName,
TelProfile TelPreference, TelProfile CodersGroupID,
TelProfile IsFaxUsed, TelProfile JitterBufMinDelay,
TelProfile JitterBufOptFactor, TelProfile IPDiffServ,
TelProfile SigIPDiffServ, TelProfile DtmfVolume,
TelProfile InputGain, TelProfile VoiceVolume,
TelProfile EnableReversePolarity,
TelProfile EnableCurrentDisconnect,
TelProfile EnableDigitDelivery, TelProfile EnableEC,
TelProfile MWIAnalog, TelProfile MWIDisplay,
TelProfile FlashHookPeriod, TelProfile EnableEarlyMedia,
TelProfile ProgressIndicator2IP;
TelProfile 1 = voice,$$,1,$$,$$,$$,$$,$$,$$,$$;
TelProfile 2 = data,$$,2,$$,$$,$$,$$,$$,$$,$$;
[\TelProfile]
```

Originating Side:

```
;E1 TRANSPARENT 31
ProtocolType 0 = 5
ProtocolType 1 = 5
ProtocolType 2 = 5
ProtocolType 3 = 5
;Channel selection by Phone number.
ChannelSelectMode = 0
[TrunkGroup]
FORMAT TrunkGroup Index = TrunkGroup TrunkGroupNum,
TrunkGroup FirstTrunkId, TrunkGroup LastTrunkId,
TrunkGroup FirstBChannel, TrunkGroup LastBChannel,
TrunkGroup FirstPhoneNumber, TrunkGroup ProfileId,
TrunkGroup Module;
TrunkGroup 0 = 0,0,0,1,31,1000,1;
TrunkGroup 0 = 0,1,1,1,31,2000,1;
TrunkGroup 0 = 0,2,2,1,31,3000,1;
TrunkGroup 0 = 0,3,1,31,4000,1;
TrunkGroup 0 = 0,0,0,16,16,7000,2;
TrunkGroup 0 = 0,1,1,16,16,7001,2;
TrunkGroup 0 = 0,2,2,16,16,7002,2;
TrunkGroup 0 = 0,3,3,16,16,7003,2;
[\TrunkGroup]
[CoderName]
FORMAT CoderName Index = CoderName Type, CoderName PacketInterval,
CoderName rate, CoderName PayloadType, CoderName Sce;
CoderName 1 = 'g7231';
CoderName 2 = 'Transparent';
[\CoderName]
[TelProfile]
FORMAT TelProfile Index = TelProfile ProfileName,
TelProfile TelPreference, TelProfile CodersGroupID,
TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay,
TelProfile JitterBufOptFactor, TelProfile IPDiffServ,
TelProfile SigIPDiffServ, TelProfile DtmfVolume,
TelProfile_InputGain, TelProfile_VoiceVolume,
TelProfile EnableReversePolarity,
TelProfile EnableCurrentDisconnect,
TelProfile_EnableDigitDelivery, TelProfile_EnableEC,
TelProfile MWIAnalog, TelProfile MWIDisplay,
TelProfile FlashHookPeriod, TelProfile EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile 1 = voice,$$,1,$$,$$,$$,$$,$$,$$,$$
TelProfile 2 = data,$$,2,$$,$$,$$,$$,$$,$$,$$
[\TelProfile]
```

10.2 QSIG Tunneling

The device supports QSIG tunneling over SIP according to IETF draft 'Tunnelling of QSIG over SIP' (draft-elwell-sipping-qsig-tunnel-03) and the ECMA-355/ISO/IEC 22535 standard. This method enables all QSIG messages to be sent as raw data in corresponding SIP messages using a dedicated message body. This mechanism is useful for two QSIG subscribers (connected to the same or different QSIG PBX) to communicate with each other over an IP network. Tunneling is supported in both directions (Tel-to-IP and IP-to-Tel).

The term tunneling means that messages are transferred ‘as is’ to the remote side without being converted (QSIG→SIP→QSIG). The advantage of tunneling over QSIG-to-SIP interworking is that by using interworking, QSIG functionality can only be partially achieved. When tunneling is used, all QSIG capabilities are supported, whereas the tunneling medium (the SIP network) does not need to process these messages.

QSIG messages are transferred in SIP messages in a separate Multipurpose Internet Mail Extensions (MIME) body. Therefore, if a message contains more than one body (e.g., SDP and QSIG), multipart MIME must be used. The Content-Type of the QSIG tunneled message is ‘application/QSIG’. In addition, the device adds a Content-Disposition header in the following format:

```
Content-Disposition: signal; handling=required.
```

- **Call setup (originating device):** The QSIG SETUP request is encapsulated in the SIP INVITE message without being altered. After the SIP INVITE request is sent, the device doesn’t encapsulate the subsequent QSIG message until a SIP 200 OK response is received. If the originating device receives a 4xx, 5xx, or 6xx response, it disconnects the QSIG call with a ‘no route to destination’ cause.
- **Call setup (terminating device):** After the terminating device receives a SIP INVITE request with a 'Content-Type: application/QSIG', it sends the encapsulated QSIG SETUP message to the Tel side and sends a 200 OK response (no 1xx response is sent) to IP. The 200 OK response includes an encapsulated QSIG CALL PROCEEDING message (without waiting for a CALL PROCEEDING message from the Tel side). If tunneling is disabled and the incoming INVITE includes a QSIG body, a 415 response is sent.
- **Mid-call communication:** After the SIP connection is established, all QSIG messages are encapsulated in SIP INFO messages.
- **Call tear-down:** The SIP connection is terminated once the QSIG call is complete. The RELEASE COMPLETE message is encapsulated in the SIP BYE message that terminates the session.

To enable QSIG tunneling, set the parameter EnableQSIGTunneling to 1 on both the originating and terminating devices, and the parameter ISDNDuplicateQ931BuffMode to 128 (duplicate all messages) (both parameters are described in "ISDN and CAS Interworking-Related Parameters" on page 307).

11 Supplied SIP Software Package

The table below lists the standard SIP software package supplied with the SIP device.

Table 11-1: Supplied Software Package

File Name	Description
Ram.cmp file	
Mediant_SIP_xxx.cmp	Image file containing the software for the Mediant 2000.
ini files	
Mediant_SIP_T1.ini	Sample ini file for Mediant 2000 E1 device.
Mediant_SIP_E1.ini	Sample ini file for Mediant 2000 T1 device.
Usa_tones_xx.dat	Default loadable Call Progress Tones dat file
Usa_tones_xx.ini	Call Progress Tones ini file (used to create dat file)
voice_prompts.dat	Sample loadable Voice Prompts dat file
Utilities	
DConvert	TrunkPack Downloadable Conversion Utility - to create Call Progress Tones, Voice Prompts, and CAS files
ACSyslog	Syslog server
BootP	BootP/TFTP configuration utility
CAS Protocol Files	Used for various signaling types, such as E_M_WinkTable.dat
MIB Files	MIB library for SNMP browser
CAS Capture Tool	Utility that is used to convert CAS traces to textual form
ISDN Capture Tool	Utility that is used to convert ISDN traces to textual form

Reader’s Notes

12 Selected Technical Specifications

The technical specifications of the Mediant 2000 is listed in the table below:

Note: All specifications in this document are subject to change without prior notice.

Table 12-1: Mediant 2000 Functional Specifications

Function	Specification
Trunk & Channel Capacity	
Capacity with E1	1, 2, 4, 8 or 16 E1 spans, supporting channel capacity as follows: ▪ 30 Channels on 1 E1 span with gateway-1 only ▪ 60 Channels on 2 E1 spans with gateway-1 only ▪ 120 Channels on 4 E1 spans with gateway-1 only ▪ 240 Channels on 8 E1 spans with gateway-1 only ▪ 480 Channels on 16 E1 spans with gateway-1 and gateway-2 **Note:** Channel capacity depends on configuration settings.
Capacity with T1	1, 2, 4, 8 or 16 T1 spans, supporting channel capacity as follows: ▪ 24 Channels on 1 T1 span with gateway-1 only ▪ 48 Channels on 2 T1 spans with gateway-1 only ▪ 96 Channels on 4 T1 spans with gateway-1 only ▪ 192 Channels on 8 T1 spans with gateway-1 only ▪ 384 Channels on 16 T1 spans with gateway-1 and gateway-2 **Note:** Channel capacity depends on configuration settings.
Voice & Tone Characteristics	
Voice Compression	G.711 PCM at 64 kbps µ-law/A-law; EG.711 µ-law/A-law at 64 kbps; G.723.1 MP-MLQ at 5.3 or 6.3 kbps; G.726 at 32 kbps ADPCM; G.729 CS-ACELP 8 kbps Annex A / B; EVRC; AMR; Transparent; GSM Full Rate; Microsoft GSM; iLBC; QCELP
Silence Suppression	▪ G.723.1 Annex A ▪ G.729 Annex B ▪ PCM and ADPCM: Standard Silence Descriptor (SID) with Proprietary Voice Activity Detection (VAD) and Comfort Noise Generation (CNG)
Packet Loss Concealment	G.711 appendix 1; G.723.1; G.729 a/b
Echo Cancellation	G.165 and G.168 2000, configurable tail length per device from 32 to 128 msec
DTMF Detection and Generation	Dynamic range 0 to -25 dBm, compliant with TIA 464B and Bellcore TR-NWT-000506.

Function	Specification
DTMF Transport (in-band)	Mute, transfer in RTP payload or relay in compliance with RFC 2833
Answer Detector	Answer detection
Answer Machine Detector	Detects whether voice or an answering machine is answering the call. **Note:** When implementing Answer Machine Detector, channel capacity may be reduced.
Call Progress Tone Detection and Generation	32 tones: single tone, dual tones or AM tones, programmable frequency & amplitude; 64 frequencies in the range 300 to 1980 Hz, 1 to 4 cadences per tone, up to 4 sets of ON/OFF periods
Output Gain Control	-32 dB to +31 dB in steps of 1 dB
Input Gain Control	-32 dB to +31 dB in steps of 1 dB
Fax and Modem Transport Modes	
Real time Fax Relay	▪ Group 3 real-time fax relay up to 14400 bps with automatic fallback ▪ Tolerant network delay (up to 9 seconds round trip delay) ▪ T.30 (PSTN) and T.38 (IP) compliant (real-time fax) ▪ CNG tone detection & Relay per T.38 ▪ Answer tone (CED or AnsAm) detection & Relay per T.38
Fax Transparency	Automatic fax bypass (pass-through) to G.711, ADPCM or NSE bypass mode
Modem Transparency	Automatic switching (pass-through) to PCM, ADPCM or NSE bypass mode for modem signals (V.34 or V.90 modem detection)
Protocols	
VoIP Signaling Protocol	SIP RFC 3261
Communication Protocols	▪ RTP/RTCP packetization ▪ IP stack (UDP, TCP, RTP) ▪ Remote Software load (TFTP, HTTP and HTTPS)
Telephony Protocols	▪ PRI (ETSI Euro ISDN, ANSI NI2, 4/5ESS, DMS 100, QSIG, Japan INS1500, Australian Telecom, New Zealand Telecom, Hong Kong Variant, Korean MIC) ▪ E1/T1 CAS protocols: MFC R2, E&M wink start ▪ Immediate start, delay start, loop start, ground start ▪ Feature Group B, D for E1/T1
In-Band Signaling	▪ DTMF (TIA 464A) ▪ MF-R1, MFC R2 ▪ User-defined Call Progress Tones
Interfaces	
Telephony Interface	1, 2, 4, 8 or 16 E1/T1/J1 Balanced 120/100 Ohm, or 75 Ohm using a BNC to RJ-45 dual E1/T1 G.703 Balun adapter. **Note:** The following Balun adaptors were tested and certified by AudioCodes: ▪ Manufacture Name: AC&E (Part Number: B04040072) ▪ Manufacture Name: RIT (Part Number: R3712271)

Function	Specification
Network Interface	Two 10/100Base-TX, half or full duplex with auto-negotiation
RS-232 Interface	RS-232 terminal interface provided by DB-9 connector on rear panel (available only on the 1, 2 and 4-span configurations)
LED Indicators	
LED Indications on Front Panel	Power, ACT/Fail, T1/E1 status, LAN status, Swap ready indication
Connectors & Switches	
Rear Panel	
Trunks 1 to 8 and 9 to 16	Two 50-pin female Telco connectors (DDK57AE-40500-21D) or 8 RJ-48c connectors for trunks 1 to 8 only
Ethernet 1 and 2	Two 10/100Base-TX, RJ-45 shielded connectors
RS-232	DB-9 Console port
AC Power	▪ Standard IEC320 Appliance inlet ▪ Dual (fully redundant) power supply (optional)
DC Power	▪ 2-pin terminal block (screw connection type) suitable for field wiring applications connecting DC Power connector MSTB2.5/2-STF (5.08 mm) from Phoenix Contact ▪ Bonding and earthing: 6-32-UNC screw is provided - correct ring terminal and 16 AWG wire minimum must be used ▪ Or crimp connection (refer to note below) **Note:** To meet UL approval, customers **must** fulfill the criteria below: 2-pin terminal block (crimp connection type) comprising a Phoenix Contact ▪ Adaptor: Shroud MSTBC2,5/2-STZF-5,08 ▪ Contacts: MSTBC-MT0,5-1,0 ▪ Cable: 18 AWG x 1.5 m length
Physical	
AC Power Supply	▪ Universal 90 to 260 VAC 1A max, 47-63 Hz ▪ Dual redundant power supply (optional)
AC Power Consumption	▪ 1 or 2 span: 39.7 W ▪ 4 spans: 42.1 W (approx.) ▪ 8 spans: 45.3 W
DC Power Supply (optional)	36 to 72 VDC (nominal 48 VDC), 4A max, floating input
DC Power Consumption	▪ 1 or 2 span: 28.8 W ▪ 4 spans: 32.8 W ▪ 8 spans: 36.4 W
Environmental (DC)	▪ Operating Temp: 0 to 40°C (32 to 104°F) ▪ Short Term Operating Temp (per NEBS): 0 to 55°C (32 to 131°F) ▪ Storage: -40 to 70°C (-40 to 158°F) ▪ Humidity: 10 to 90% non-condensing

Function	Specification
Environmental (AC)	▪ Operating Temp: 0 to 40°C (32 to 104°F) ▪ Storage: -40 to 70°C (-40 to 158°F) ▪ Humidity: 10 to 90% non-condensing
Hot Swap	▪ cPCI blades are full hot-swappable ▪ Power supplies are redundant, but not hot-swappable
Enclosure Dimensions	445 x 44 x 300 mm (17.5 x 1.75 x 12 inches)
Weight	Approx. 4.8 kg fully populated (16 spans); 4.2 kg for 1 span
Installation	1U 19-inch 2-slot cPCI chassis; rack-, shelf-, or desktop-mount options. Rack mount using two side brackets - 2 additional (rear) side brackets optional
cPCI Blade	
Control Processor	Motorola PowerQUICC 8260
Control Processor Memory	SDRAM 64* - 128 MB (*on 60-channel models)
Signal Processors	AudioCodes AC486 VoIP DSP based on TI DSP TMS5541 – each core at 133 MHz
PCI Bus Interface	33 MHz, 32 bit, slave mode (PICMG 2.0 revision 2.1)
Physical	6U single cPCI slot. PICMG 2.0, R2.1 and R2.16 and R.3.0 CompactPCI™ blade
Supply Voltages and Power Consumption (typical)	▪ 480 channels: 40.7 W; 3 A at 5 V; 7.8 A at 3.3 V ▪ 240 channels: 24 W; 1.5 A at 5 V; 5 A at 3.3 V ▪ 120 channels: 18.4 W; 0.9 A at 5 V; 4.2 A at 3.3 V
Environmental	Humidity: 10 to 90% non-condensing
Cooling	▪ 500 Linear Feet per Minute (LFM) at 50°C ambient temp. supporting 480 ports ▪ 400 LFM at 50°C ambient temp. supporting 400 ports ▪ 300 LFM at 50 °C ambient temp. supporting 240 ports
Diagnostics	
Front panel Status LEDs	▪ E1/T1 status ▪ LAN status ▪ Status of device (Fail, ACT, Power, and Swap Ready)
Syslog events	Supported by Syslog Server, per RFC 3164 IETF standard.
SNMP MIBs and Traps	SNMP v2c; SNMP v3
Management	
Configuration	Configuration of device using Web browser or *ini* files
Management and Maintenance	▪ SNMP v2c; SNMP v3 ▪ Syslog (RFC 3164) ▪ Web Management (via HTTP or HTTPS) ▪ Telnet

Function	Specification
Type Approvals	
Telecommunication Standards	▪ IC CS03; FCC part 68 ▪ Chassis and Host telecom card comply with IC CS03; FCC part 68; CTR 4, CTR 12 & CTR 13; JATE; TS.016; TSO; Anatel, Mexico Telecom, Russia CCC, ASIF S016, ASIF S038
Safety and EMC Standards	▪ UL 60 950-1, FCC part 15 Class B, (Class A with SUN 2080 CPU card) ▪ CE Mark: EN 55022 Class B (Class A with SUN 2080 CPU card), EN 60950-1, EN 55024, EN 300 386 ▪ TS001
Environmental	▪ NEBS Level 3: GR-63-Core, GR-1089-Core, Type 1 & 3. Approved for DC powered version ▪ Complies with ETS 301019; ETS 300019-1, -2, -3. (T 1.1, T 2.3, T3.2) ▪ Approved for AudioCodes or DC powered versions

Reader’s Notes

13 Glossary

Table 13-1: Glossary of Terms

Term	Meaning
ADPCM	Adaptive Differential PCM - voice compression
AIS	Alarm Indication Signal
A-law	Standard companding algorithm, used in European digital communications systems to optimize the dynamic range of an analog signal for digitizing.
AMD	Answering Machine Detection
AOR	Address of Record
AWG	American Wire Gauge
bps	Bits per second
BootP	AudioCodes Proprietary Bootstrap Loader Utility
CAS	Channel Associated Signaling
CoS	Class of Service
CMP	Compressed File (device Firmware)
cPCI	Compact PCI (Industry Standard)
CPT	Call Progress Tones
dB	Decibels
DHCP	Dynamic Host Control Protocol
DID	Direct Inward Dial
DiffServ	Differentiated Services
DNS	Domain Name System (or Server)
DR	Debug Recording
DS1	1.544 Mbps USA Digital Transmission System (see E1 and T1)
DSP	Digital Signal Processor (or Processing)
DTMF	Dual Tone Multiple Frequency (Touch Tone)
E1	2.048 Mbps European Digital Transmission System (see T1)
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
GRUU	Globally Routable User Agent URIs
ICMP	Internet Control Message Protocol
IE	Information Element (ISDN layer 3 protocol, basic building block)
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange (for IPSec)
IP	Internet Protocol
IPSec	IP Security

Term	Meaning
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITU	International Telecommunications Union
ITU-T	Telecommunications section of the ITU
IVR	Interactive Voice Response
Jitter	Variation of interpacket timing interval
kbps	Kilobit per second. 1,000 bits per second
LAPD	Line Access Protocol for the D-channel
LFA	Loss of Frame Alignment
LOF	Loss of Frame
Mbps	Megabit per second. Million bits per second
MIB	Management Information Base
MLPP	Multilevel Precedence and Preemption
ms or msec	Millisecond; a thousandth part of a second
MSCML	Media Server Control Markup Language
NT	Network Termination (ISDN)
MWI	Message Waiting Indicator
NAPTR	Naming Authority Pointer
NAT	Network Address Translation
NFAS	Non-Facility Associated Signalling (ISDN PRI)
NFS	Network File System
NPI	Numbering Plan Indicator
NTP	Network Time Protocol
OAMP	Operations, Administration, Maintenance and Provisioning
OSI	Open Systems Interconnection (Industry Standard)
PBX	Private Branch Exchange
PCI	Personal Computer Interface (Industry Standard)
PCM	Pulse-Code Modulation
PI	Progress Indicator
PKI	Public-Key Infrastructures
POTS	Plain Old Telephone System or Service
PRT	Prerecorded Tones (File)
PRI	Primary Rate Interface (ISDN)
PSTN	Public Switched Telephone Network
PVID	Port VLAN ID (VLAN ID assignment to Ethernet packet by switch)
QoS	Quality of Service

Term	Meaning
RAI	Remote Alarm Indication
RFC	Request for Comment issued by IETF
RTCP	Real-Time Transport (RTP) Control Protocol
RTP	Real-Time Transport Protocol
SA	Security Associations (contains encryption keys and profile used by IPSec to encrypt the IP stream)
SAS	Stand Alone Survivability Feature
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMDI	Simplified Message Desk Interface
SME	Small and Medium-sized Enterprise
SNMP	Simple Network Management Protocol
SRTP	Secure Real-Time Transport Protocol
SRV	Service Record
SSH	Secure Shell
SSL	Secure Socket Layer (also known as Transport Layer Security (TLS))
STUN	Simple Traversal of UDP through NATs
T1	1.544 Mbps USA Digital Transmission System (see E1 and DS1)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment (ISDN)
TDM	Time-Division Multiplexing
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TON	Type of Numbering
UA	SIP User Agent
UDP	User Datagram Protocol
URI (SIP URIs)	SIP Uniform Resource Indicators
VBD	Voice-band data
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VoP	Voice over Packet(s)
VP	Voice Prompts (File)
VPN	Virtual Private Network
µ-Law	A companding algorithm, used in the digital telecommunication systems

AudioCodes

Mediant™ Media Gateways

SIP

Mediant 2000

User's Manual

Version 5.6

AudioCodes

www.audiocodes.com