ACCESS 241-FXO

ACCESS 241 · ACCESS 211

VoIP GATEWAY

(AC-241-FXO·AC-241·AC-211)

ADMINISTRATOR GUIDE

Revision History

Revision	Date	Description
C	August 2005	Added AC-241 to AC-211 UG. Adapted for Version 4.56.
D	September 2005	Added AC-241-FXO. Adapted for AC-241FXO version 5.1, AC-241 and AC-211 version 4.57

Table of Contents

1 OVERVIEW 1-1

1.1 ACCESS 241-FXO OVERVIEW 1-1
1.1.1 Access 241-FXO Front Panel 1-2
1.1.2 Access 241-FXO Rear Panel 1-3
1.2 ACCESS 241 OVERVIEW 1-4
1.2.1 Access 241 Front Panel 1-4
1.2.2 Access 241 Rear Panel 1-5
1.3 ACCESS 211 OVERVIEW 1-6
1.3.1 Access 211 Front Panel 1-6
1.3.2 Access 211 Rear Panel 1-7
1.4 FEATURES 1-8
1.4.1 Gateway Audio Channel Features 1-8
1.4.2 Connectivity Features 1-8
1.5 HOW TO GET HELP 1-9

2 GATEWAY INSTALLATION 2-1

2.1 PRE-INSTALLATION REQUIREMENTS 2-1
2.1.1 Equipment Requirements 2-2
2.1.2 Telephones and Accessories 2-2
2.2 ACCESS 241-FXO VOIP GATEWAY INSTALLATION 2-4
2.3 ACCESS 241 VOIP GATEWAY INSTALLATION 2-6
2.4 ACCESS 211 VOIP GATEWAY INSTALLATION WITH A SINGLE PC 2-8
2.5 ACCESS 211 VOIP GATEWAY INSTALLATION WITH A HOME NETWORK 2-10
2.6 WALL-MOUNTING THE GATEWAY UNIT 2-11

3 THEORY OF OPERATION 3-1

3.1 USING THE DIAL PLAN FOR SIP, H.323 AND PSTN 3-1
3.1.1 Types of Dial Plans 3-1
3.1.2 Default Dial Plan 3-1
3.1.3 Dial Plan Syntax 3-2
3.1.4 Dial Plan Examples 3-3
3.2 UNDERSTANDING DHCP 3-5
3.2.1 When Should Clients Use DHCP 3-6
3.3 UNDERSTANDING NAT AND NAPT 3-6
3.4 UNDERSTANDING NTP 3-7
3.4.1 Daylight Saving Time (Summer Time) 3-7
3.5 UNDERSTANDING PPP OVER ETHERNET (PPPOE) 3-8
3.5.1 Protocol Overview 3-8
3.5.2 Discovery Stage 3-8
3.5.3 PPP Session Stage 3-9
3.6 UNDERSTANDING SYSLOG 3-10
3.6.1 Remote Logging 3-10
3.7 UNDERSTANDING DNS RESOLVER 3-11

4 INITIAL SETUP 4-13

4.1 KEYPAD CONFIGURATION 4-13
4.2 KEYPAD CONFIGURATION FOR MGCP 4-14

5 UPGRADING FIRMWARE AND DOWNLOADING CONFIGURATION FILES 5-1

5.1 MANUALLY DOWNLOADING THE FILE USING TELNET 5-2
5.2 MANUALLY DOWNLOADING THE FILE USING THE WEB 5-3

5.3 DHCP AUTOMATIC CONFIGURATION....5-4
5.3.1 Setting DHCP Automatic Configuration via the Web....5-4
5.3.2 Setting DHCP Automatic Configuration via Telnet....5-7
5.4 FIXED (PROVISIONED) HTTP OR TFTP AUTOMATIC CONFIGURATION....5-8
5.4.1 Setting the TFTP/HTTP Server "Root" Configuration File via the Web....5-8
5.4.2 Setting the TFTP Server "Root" Configuration File via Telnet....5-8
5.5 CREATING AND ENCRYPTING CONFIGURATION FILES....5-9

6 CONFIGURING THE GATEWAY VIA WEB....6-1

7 WAN CONFIGURATION VIA WEB....7-1

7.1 DEFAULT WAN CONFIGURATION....7-1
7.2 WAN STATUS PAGE....7-1
7.3 ASSIGNING AN IP ADDRESS TO THE GATEWAY....7-2
7.4 ENABLING POINT-TO-POINT PROTOCOL OVER ETHERNET (PPPOE)....7-5
7.5 ENABLING THE POINT-TO-POINT TUNNELING PROTOCOL (PPTP)....7-6
7.6 MAC SPOOFING....7-8
7.7 AUTOCONFIGURATION....7-8

8 LAN CONFIGURATION VIA WEB....8-1

8.1 DEFAULT LAN CONFIGURATION....8-1
8.2 CONFIGURING LAN SETTINGS....8-1
8.3 DHCP SERVER CONFIGURATION....8-3
8.4 PORT FORWARDING....8-6
8.5 IPSEC NAT TRAVERSE....8-8

9 SECURITY CONFIGURATION VIA WEB....9-1

9.1 DEFAULT SECURITY CONFIGURATION....9-1
9.2 SETTING THE PASSWORD....9-1
9.3 CONFIGURING ADVANCED AND DHCP SECURITY....9-2
9.4 ENABLING/DISABLING CONFIGURATION VIA TELNET OR HTTP....9-4
9.5 SETTING THE "ROOT" FILE ENCRYPTION KEY....9-5
9.6 SETTING THE "GENERAL" CONFIGURATION FILE ENCRYPTION KEY....9-6

10 MISCELLANEOUS CONFIGURATION VIA WEB....10-1

10.1 DEFAULT MISCELLANEOUS CONFIGURATION....10-1
10.2 CLOCK LOCALIZATION....10-4
10.3 LOCAL SETTINGS....10-5
10.4 SYSLOG SERVER CONFIGURATION....10-6
10.5 SENDING DEVICE INFORMATION TO THE SYSLOG SERVER....10-7
10.6 PORT PROTOCOL CONFIGURATION....10-8
10.7 SIP ADVANCED CALLING FEATURES AND KEY SEQUENCE CONFIGURATION....10-10
10.8 RING TONES CONFIGURATION....10-15
10.8.1 Ring Names and Cadences....10-15
10.8.2 Call Waiting Tone Cadence Patterns....10-17
10.8.3 Call Progress Tones....10-19

11 VOICE AND MANAGEMENT SERVICES CONFIGURATION VIA WEB....11-1

11.1 DEFAULT VOICE AND MANAGEMENT SERVICES CONFIGURATION....11-1
11.2 CONFIGURING VOICE AND MANAGEMENT SERVICES....11-2

12 CONFIGURING VLANS VIA WEB....12-1

12.1 DEFAULT VLAN CONFIGURATION....12-1
12.2 CONFIGURING VLAN....12-1

13 PROTOCOL H.323 CONFIGURATION VIA WEB....13-1

13.1 DEFAULT H.323 CONFIGURATION....13-1
13.2 SETTING THE H.323 CONFIGURATION....13-1

13.3 DTMF SIGNALING 13-3
13.4 AUDIO/CODEC CONFIGURATION 13-4

14 PROTOCOL MGCP CONFIGURATION VIA WEB 14-1

14.1 DEFAULT MGCP CONFIGURATION 14-1
14.2 SETTING THE MGCP CONFIGURATION 14-2
14.3 RTP TELEPHONE EVENT (RFC2833) CONFIGURATION 14-3
14.4 AUDIO/CODEC CONFIGURATION 14-5

15 PROTOCOL SIP CONFIGURATION VIA WEB 15-1

15.1 DEFAULT SIP CONFIGURATION 15-1
15.2 SIP SERVER CONFIGURATION 15-2
15.2.1 SIP Server Settings 15-2
15.2.2 Gateway Settings 15-3
15.2.3 NAT Settings 15-5
15.2.4 STUN Server Settings 15-5
15.3 SIP EXTENSIONS 15-6
15.4 LINE 1 AND LINE 2 STATUS AND CONFIGURATION 15-8
15.4.1 Line1 and Line2 Status 15-8
15.4.2 Line1 and Line2 Configuration 15-9
15.5 LINE3 CONFIGURATION (AC-241-FXO ONLY) 15-11
15.6 AUDIO/CODEC CONFIGURATION 15-12
15.7 SELECTING A PREFERRED CODEC FOR SIP 15-13

16 COMPLETING THE GATEWAY CONFIGURATION VIA WEB 16-1

17 CONFIGURING THE GATEWAY VIA TELNET 17-1

17.1 COMMAND MODES 17-1
17.1.1 Enable Mode 17-1
17.1.2 Commands Mode 17-2
17.1.3 Report Mode 17-2
17.1.4 Statistics Mode 17-3
17.1.5 Download Mode 17-3
17.1.6 Configuration Modes 17-4
17.2 GENERAL COMMANDS 17-5
17.3 USING THE CLI COMMANDS 17-6

18 WAN CONFIGURATION VIA TELNET 18-1

18.1 DEFAULT WAN CONFIGURATION 18-1
18.2 WAN CONFIGURATION COMMANDS 18-1
18.2.1 Entering into WAN Configuration Mode 18-2
18.2.2 Enabling DHCP 18-2
18.2.3 Setting the IP Address of the WAN Interface 18-3
18.2.4 Setting the Subnet Mask of the WAN Interface 18-3
18.2.5 Setting the Default Gateway of the WAN Interface 18-4
18.2.6 Setting the IP Address of the DNS Server 18-4
18.2.7 Setting the Host Name 18-4
18.2.8 Setting the Domain Name 18-5
18.2.9 Setting the Automatic Configuration ID 18-5
18.2.10 Enabling the Use of DHCP Options 66, 67 18-5
18.2.11 Enabling the Auto Config Mode 18-6
18.2.12 Setting the TFTP/HTTP Server IP Address 18-6
18.2.13 Setting the File Name 18-7
18.3 WAN DISPLAYING COMMANDS 18-7
18.3.1 Displaying all the WAN Configuration 18-8
18.3.2 Displaying the Status of the DHCP Server 18-9
18.3.3 Displaying the IP address of the WAN Interface 18-9
18.3.4 Displaying the Subnet Mask of the WAN Interface 18-9

18.3.5 Displaying the IP Address of the DNS Server 18-10
18.3.6 Displaying the Host Name of the Unit 18-10
18.3.7 Displaying the Domain Name of the Unit 18-10
18.3.8 Displaying the DHCP Automatic Configuration ID 18-11
18.3.9 Displaying the DHCP Options 66, 67 Status 18-11
18.3.10 Displaying the Auto Config Mode Status 18-11
18.3.11 Displaying the TFTP\HTTP Server's IP Address 18-12
18.3.12 Displaying the File Name 18-12

19 LAN CONFIGURATION VIA TELNET 19-1

19.1 DEFAULT LAN CONFIGURATION 19-1
19.2 LAN CONFIGURATION COMMANDS 19-1
19.2.1 Entering into LAN Configuration Mode 19-1
19.2.2 Setting the IP Address of the LAN Interface 19-2
19.2.3 Setting the Subnet Mask of the LAN Interface 19-2
19.3 LAN DISPLAYING COMMANDS 19-2
19.3.1 Displaying all the LAN Configuration 19-3
19.3.2 Displaying the IP Address of the LAN Interface 19-3
19.3.3 Displaying the Subnet Mask of the LAN Interface 19-3

20 SECURITY CONFIGURATION VIA TELNET 20-1

20.1 DEFAULT SECURITY CONFIGURATION 20-1
20.2 SECURITY CONFIGURATION COMMANDS 20-1
20.2.1 Entering into Security Configuration Mode 20-2
20.2.2 Enabling Advanced Security 20-2
20.2.3 Enabling DHCP Security 20-2
20.2.4 Setting Management IP Addresses 20-3
20.3 SECURITY DISPLAYING COMMANDS 20-3
20.3.1 Displaying all the Security Parameters 20-4
20.3.2 Displaying the Advanced Security Status 20-4
20.3.3 Displaying the DHCP Security Status 20-5
20.3.4 Displaying the Management IP Addresses 20-5

21 HTTP CONFIGURATION VIA TELNET 21-1

21.1 DEFAULT HTTP CONFIGURATION 21-1
21.2 HTTP CONFIGURATION COMMANDS 21-1
21.2.1 Entering into HTTP Configuration Mode 21-1
21.2.2 Enabling/Disabling Configuration via HTTP 21-2
21.3 HTTP DISPLAYING COMMANDS 21-2
21.3.1 Displaying the HTTP Configuration Status 21-2

22 CONFIGURING VLANS VIA TELNET 22-3

22.1 DEFAULT VLAN CONFIGURATION 22-3
22.2 VLAN CONFIGURATION COMMANDS 22-3
22.2.1 Entering into VLAN Configuration Mode 22-4
22.2.2 Enabling Using VLANs 22-4
22.2.3 Creating a New VLAN 22-5
22.2.4 Deleting an Existing VLAN 22-5
22.2.5 Adding Ports to a VLAN and Setting the Port's Default VLAN 22-5
22.2.6 Removing Ports from a VLAN 22-6
22.2.7 Assigning VLAN and Priority Tag to the Management Packets 22-6
22.2.8 Assigning VLAN and Priority Tag VoIP Call Session Start Frames 22-7
22.2.9 Assigning VLAN, Priority Tag and ToS to the Outgoing RTP Frames 22-7
22.3 VLAN DISPLAYING COMMANDS 22-7
22.3.1 Displaying the VLAN Configuration 22-8
22.3.2 Displaying the Service VLAN Configuration 22-8

23 INTERFACE CONFIGURATION VIA TELNET 23-1

23.1 DEFAULT INTERFACE CONFIGURATION 23-1
23.2 INTERFACE CONFIGURATION COMMANDS 23-1
23.2.1 Entering into Interface Configuration Mode 23-1
23.2.2 Setting the Interface's State 23-2
23.2.3 Setting the Interface's Duplex Speed 23-2
23.2.4 Enabling Flow Control on the Interface 23-3
23.3 INTERFACE DISPLAYING COMMANDS 23-3
23.3.1 Displaying the Specified Interface Configuration 23-3
23.3.2 Displaying the Configuration of all the Interfaces 23-4

24 EXECUTING REPORTS VIA TELNET 24-1

24.1 REPORTS COMMANDS 24-1
24.1.1 Entering into Report Mode 24-1
24.1.2 Entering into Statistics Mode 24-2
24.1.3 Displaying the Interfaces' Statistics 24-2
24.1.4 Clearing the Interfaces' Statistics 24-5
24.1.5 Entering into Download Mode 24-5
24.1.6 Displaying the Configuration Download Status 24-5

25 PROTOCOL H.323 CONFIGURATION VIA TELNET 25-1

25.1 DEFAULT H.323 CONFIGURATION 25-1
25.2 H.323 CONFIGURATION COMMANDS 25-1
25.2.1 Entering into H.323 Configuration Mode 25-2
25.2.2 Setting the Gatekeeper IP Address 25-2
25.2.3 Setting the Dial Plan Matching String 25-2
25.2.4 Setting the Phone Number of Line 1 25-3
25.2.5 Setting the Phone Number of Line 2 25-3
25.2.6 Setting the Caller ID for Line 1 25-3
25.2.7 Setting the Caller ID for Line 2 25-4
25.3 H.323 DISPLAYING COMMANDS 25-4
25.3.1 Displaying all the H.323 Configuration 25-5
25.3.2 Displaying the Gatekeeper IP Address 25-5
25.3.3 Displaying the Dial Plan Matching String 25-5
25.3.4 Displaying the Phone Number of Line 1 25-5
25.3.5 Displaying the Phone Number of Line 2 25-5
25.3.6 Displaying the Caller ID for Line 1 25-6
25.3.7 Displaying the Caller ID for Line 2 25-6

26 PROTOCOL MGCP CONFIGURATION VIA TELNET 26-1

26.1 DEFAULT MGCP CONFIGURATION 26-1
26.2 MGCP CONFIGURATION COMMANDS 26-1
26.2.1 Entering into MGCP Configuration Mode 26-2
26.2.2 Setting the Call Agent's IP Address 26-2
26.2.3 Setting the Call Agent's Port 26-2
26.2.4 Setting the Endpoint Domain Name 26-3
26.3 MGCP DISPLAYING COMMANDS 26-3
26.3.1 Displaying the Call Agent's IP Address 26-3
26.3.2 Displaying the Call Agent's IP Address 26-4
26.3.3 Displaying the Call Agent's Port 26-4
26.3.4 Displaying the Endpoint Domain Name 26-4
26.3.5 Displaying the Phone line Status 26-5

27 PROTOCOL SIP CONFIGURATION VIA TELNET 27-1

27.1 DEFAULT SIP CONFIGURATION 27-2
27.2 SIP CONFIGURATION COMMANDS 27-2
27.2.1 Entering into SIP Configuration Mode 27-3
27.2.2 Setting the SIP Server's IP Address 27-3
27.2.3 Setting the SIP Server's Port Number 27-4

27.2.4 Setting the SIP Server's Domain Name 27-4
27.2.5 Enabling/Disabling Sending REGISTER Request 27-4
27.2.6 Setting the Dial Plan Matching String 27-5
27.2.7 Setting the SIP Call Control Transport Protocol 27-5
27.2.8 Setting the Phone Number of Line 1 27-6
27.2.9 Setting the Phone Number of Line 2 27-6
27.2.10 Setting the Caller ID for Line 1 27-6
27.2.11 Setting the Caller ID for Line 2 27-7
27.2.12 Setting the SIP Port for Line 1 27-7
27.2.13 Setting the SIP Port for Line 2 27-7
27.2.14 Setting the AEC for Line 1 27-8
27.2.15 Setting the AEC for Line 2 27-8
27.2.16 Setting the User Name for Line 1 27-8
27.2.17 Setting the User Name for Line 2 27-9
27.2.18 Setting the Password for Line 1 27-9
27.2.19 Setting the Password for Line 2 27-9
27.2.20 Setting the NAT IP Address 27-10
27.2.21 Setting the RTP/RTCP Port Base 27-10
27.2.22 Setting the STUN Server IP Address 27-10
27.2.23 Setting the STUN Server Port 27-11
27.3 SIP DISPLAYING COMMANDS 27-11
27.3.1 Displaying all the SIP Configuration 27-12
27.3.2 Displaying the SIP Server's IP Address 27-13
27.3.3 Displaying the SIP Server's Port Number 27-13
27.3.4 Displaying the SIP Server's Domain Name 27-13
27.3.5 Displaying the Sending REGISTER Request Status 27-14
27.3.6 Displaying the Dial Plan 27-14
27.3.7 Displaying the SIP Call Control Transport Protocol 27-14
27.3.8 Displaying the Phone Number of Line 1 27-15
27.3.9 Displaying the Phone Number of Line 2 27-15
27.3.10 Displaying the Caller ID for Line 1 27-15
27.3.11 Displaying the Caller ID for Line 2 27-15
27.3.12 Displaying the SIP Port for Line 1 27-16
27.3.13 Displaying the SIP Port for Line 2 27-16
27.3.14 Displaying the AEC for Line 1 27-16
27.3.15 Displaying the AEC for Line 2 27-17
27.3.16 Displaying the User Name for Line 1 27-17
27.3.17 Displaying the User Name for Line 2 27-17
27.3.18 Showing if a Password for Line 1 Exists 27-18
27.3.19 Showing if a Password for Line 2 Exists 27-18
27.3.20 Displaying the NAT IP Address 27-18
27.3.21 Displaying the RTP/RTCP Port Base 27-18
27.3.22 Displaying the STUN Server IP Address 27-19
27.3.23 Displaying the STUN Server Port 27-19
27.3.24 Displaying the Phone-line Status 27-19
27.3.25 Displaying the Phone-line Status for Pulse Metering 27-20

28 GENERAL COMMANDS MODE 28-1

28.1 GENERAL COMMANDS 28-1
28.1.1 Entering into Commands Mode 28-1
28.1.2 Rebooting the Gateway 28-1
28.1.3 Setting the Configuration to the Factory Defaults 28-2
28.1.4 Downloading Image or Configuration File Using TFTP\HTTP 28-2
28.1.5 Sending Data to Syslog via Telnet 28-3
28.1.6 Sending Pings 28-3

29 USING THE GATEWAY 29-1

29.1 FIRST CALL 29-1

29.2 PLACING CALLS 29-1
29.3 ADDING UNITS TO THE NETWORK 29-1
29.4 ADVANCED CALLING FEATURES FOR SIP 29-2
29.4.1 Call Waiting 29-2
29.4.2 Conference Call 29-2
29.4.3 Forward a Call 29-2
29.4.4 Attended Transfer Call 29-2
29.4.5 Blind Transfer Call 29-3
29.4.6 Hold 29-3
29.4.7 Conditional Call Forwarding 29-3
29.4.8 Do Not Disturb (DND) 29-3
29.4.9 Redialing of Last Received Call 29-3
29.4.10 Block Last Received Call 29-3
29.4.11 Auto Redial 29-3
29.4.12 Block Sending CID per Call 29-4
29.4.13 Anonymous Caller Rejection (ACR) 29-4
29.4.14 Support for Pulse Metering per Telephone Line 29-4
29.4.15 SIP Line Problem Tone Indicator 29-4
29.5 ADVANCED CALLING FEATURES FOR H.323 29-4
29.5.1 Call Waiting 29-4
29.5.2 Conference Call 29-5
29.5.3 Forward a Call 29-5
29.5.4 Transfer Call 29-5
29.5.5 Hold 29-5
29.6 ADVANCED CALLING FEATURES FOR MGCP 29-5
29.7 PSTN (FXO) CALLING 29-6
29.7.1 Outgoing PSTN Calls 29-6
29.7.2 Receiving PSTN Calls 29-6
29.7.3 Call Waiting 29-6
29.7.4 Conference Call 29-6

1 Overview

This Administrator's guide provides complete instructions for installing, configuring and managing the Access 241-FXO, Access 241 and Access 211 (Catalog number AC-241-FXO, AC-241 and AC-211) VoIP Gateways. The manual is intended for the VoIP service provider or for any technical body implementing a VoIP network. This chapter includes an overview of the products and information for obtaining technical assistance. The following chapters include brief installation instructions and full configuration and software-upgrade instructions for using and managing the Access 241-FXO/Access 241/Access 211 VoIP Gateways.

Throughout this guide, the Access 241-FXO, Access 241 and Access 211 will be referred to as "the Gateway", excluding cases when referring specifically to the AC-241-FXO, AC-241 or the AC-211.

1.1 Access 241-FXO Overview

The Access 241-FXO (AC-241-FXO) is a terminal Voice-over-IP (VoIP) WAN gateway and telephone adaptor for internet, Intranet and public telephone network communications. The Access 241-FXO integrates voice, routing and switching capabilities eliminating the need to connect a PC to a home router or switch when adding VoIP services on top of an existing broadband connection.

The Access 241-FXO has two independent phone ports (FXS) and one PSTN port (FXO).

- The FXS phone ports enable you to connect one or two independent analog telephone or fax lines.
- The PSTN (FXO) port is used to connect to the Public Switched Telephone Network. (PSTN).

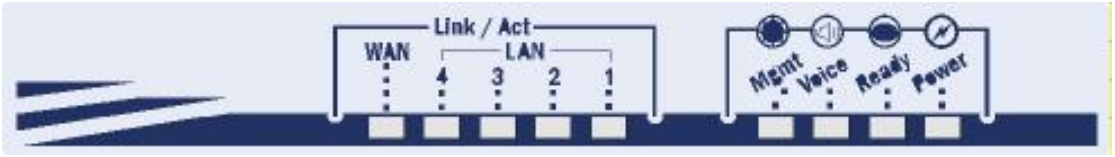
The combination of both FXS and FXO ports enables the user to communicate over the internet, using one of the standard VoIP protocols, and over the public telephone network.

The Access 241-FXO has 1 WAN and 4 LAN ports; all are 10/100Mbps Ethernet ports. The WAN port connects to your modem and the LAN ports connect to up to 4 PCs.

1.1.1 Access 241-FXO Front Panel

The Access 241-FXO Gateway's front panel contains nine LEDs:

- Five link LEDs indicate Link and Activity status for the WAN and LAN ports. Steady glow indicates Link, and blinking indicates Activity.



- Four status LEDs provide operating information explained in the following table.

1.1.1.1 Access 241-FXO Status LED Indicators

LED	Mode	H.323, MGCP, SIP Status	Downloader Status
Power	Steady glow	Power OK	Power OK
Ready	Blinking	Application OK	Loader OK
Voice	Steady glow	Gateway registered with Gatekeeper / Call Agent / SIP Server	
Mngt	Blinking	Management activity	Management activity
LAN (1,2,3,4)	Steady Glow	Link is up	Link is up
	Blinking	LAN Activity	LAN Activity
WAN	Steady Glow	Link is up	Link is up
	Blinking	WAN Activity	WAN Activity

1.1.2 Access 241-FXO Rear Panel

The rear panel contains the phone connectors, one WAN, four LAN connectors and the input DC power connector, as shown in the following figure. The PSTN socket on the left is designed to provide a public telephone network connection.

CAUTION **Never connect the Phone1 and Phone2 connectors to the public telephone outlet, or to each other. Only the PSTN connector may be connected to the public telephone outlet.**

1.2 Access 241 Overview

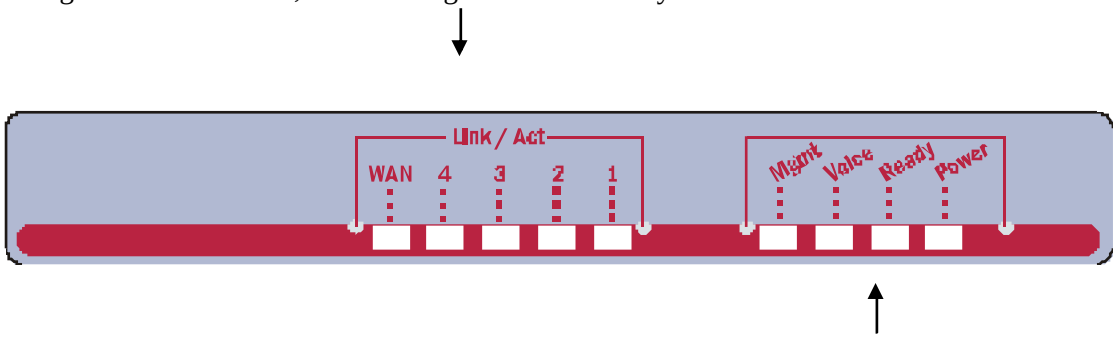
The Access 241 (AC-241) is a terminal Voice-over-IP (VoIP) WAN gateway device. This device integrates voice, routing and switching capabilities eliminating the need to connect a PC to a home router or switch when adding VoIP services on top of an existing broadband connection. The Access 241 has two phone ports, which enable to connect one or two independent analog telephone or Fax lines and communicate over the Internet or Intranet.

The Access 241 has 1 WAN and 4 LAN ports; all are 10/100Mbps Ethernet ports. The WAN port connects to your modem and the LAN ports connect to up to 4 PCs.

1.2.1 Access 241 Front Panel

The Access 241 Gateway's front panel contains nine LEDs:

- Five link LEDs indicate Link and Activity status for the WAN and LAN ports. Steady glow indicates Link, and blinking indicates Activity.



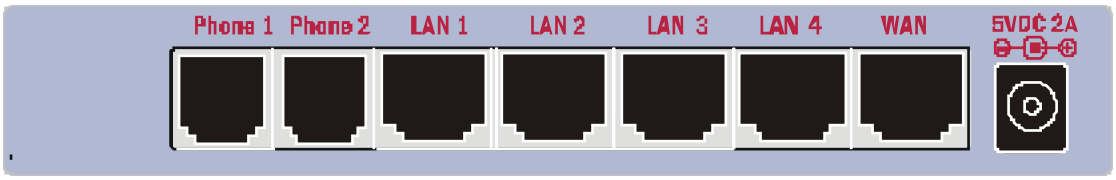
- Four status LEDs provide operating information. LEDs are explained below.

1.2.1.1 Access 241 Status LED Indicators

LED	Mode	H.323, MGCP, SIP Status	Downloader Status
Power	Steady glow	Power OK	Power OK
Ready	Blinking	Application OK	Loader OK
Voice	Steady glow	Gateway registered with Gatekeeper / Call Agent / SIP Server	
Mngt	Blinking	Management activity	Management activity
LAN (1,2,3,4)	Steady Glow	Link is up	Link is up
	Blinking	LAN Activity	LAN Activity
WAN	Steady Glow	Link is up	Link is up
	Blinking	WAN Activity	WAN Activity

1.2.2 Access 241 Rear Panel

The rear panel contains the phone connectors, one WAN, four LAN connectors and the input DC power connector, as shown in the following figure. The optional Life Line socket on the left is designed to provide a public network connection in the event of power failure.



CAUTION **Never connect the Phone connectors to the public telephone outlet, or to each other.**

1.3 Access 211 Overview

The Access 211 (AC-211) is a terminal Voice-over-IP (VoIP) WAN gateway device. This device integrates voice and routing capabilities eliminating the need to connect a PC to a home router when adding VoIP services on top of an existing broadband connection.

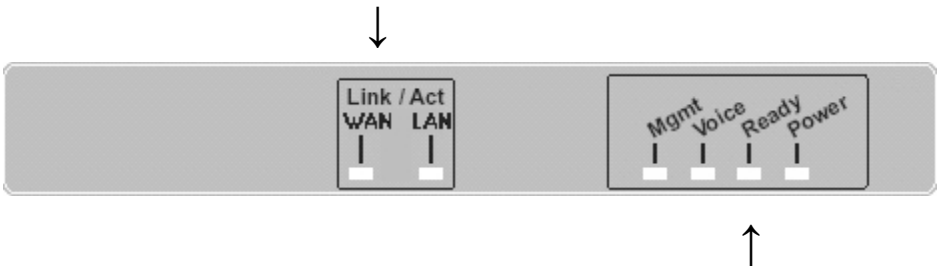
The Access 211 has two phone ports, which enable you to connect one or two independent regular telephone or Fax lines and communicate over the Internet or Intranet. In addition, you can connect a regular telephone line to the Gateway's Lifeline port. This ensures continuous telephone service in the event of a power outage or a VoIP network failure.

The Access 211 has one WAN and one LAN port, both are 10/100Mbps Ethernet ports. The WAN port connects to the modem and the LAN port connects to the PC.

1.3.1 Access 211 Front Panel

The Access 211 Gateway's front panel contains six LEDs:

- Two link LEDs indicate Link and Activity status for the WAN and LAN. Steady glow indicates Link, and blinking indicates Activity.



- Four status LEDs provide operating information. All LEDs are explained below.

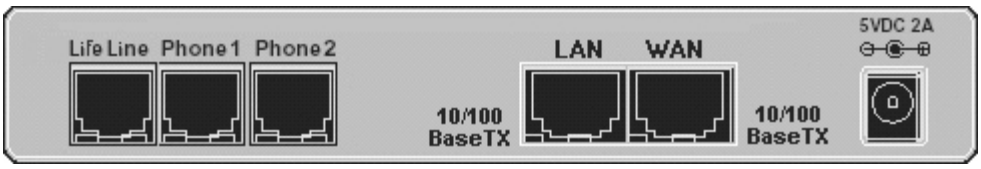
1.3.1.1 Access 211 Status LED Indicators

LED	Mode	H.323, MGCP, SIP Status	Downloader Status
Power	Steady glow	Power OK	Power OK
Ready	Blinking	Application OK	Loader OK
Voice	Steady glow	Gateway registered with Gatekeeper / Call Agent / SIP Server	
Mngt	Blinking	Management activity	Management activity
LAN	Steady Glow	Link is up	Link is up
	Blinking	LAN Activity	LAN Activity

LED	Mode	H.323, MGCP, SIP Status	Downloader Status
WAN	Steady Glow	Link is up	Link is up
	Blinking	WAN Activity	WAN Activity

1.3.2 Access 211 Rear Panel

The rear panel contains the phone connectors, the LAN and WAN connectors and the input DC power connector, as shown in the following figure. The optional Life Line socket on the left is designed to provide a public network connection in the event of power failure.



CAUTION **Never connect the Phone connectors to the public telephone outlet, or to each other. Only the Life Line connector may be connected to the public telephone outlet.**

1.4 Features

1.4.1 Gateway Audio Channel Features

The Gateway implements an audio channel and has the following features:

- SIP voice protocol support RFC 2543 and RFC 3261.
- Voice protocol MGCP 1.0 RFC 2705 and RFC 3435 and Packet Cable NCS 1.0.
- H.323 stack fully compatible with the ITU H.323 version 2 and selected sections of version 4.
- Dial plan for FXS outgoing calls.
- Access 241-FXO has advanced dial plan for FXO outgoing calls.
- Voice coding G.711 or G.723.1 or G729A/B or G726.
- Traffic shaping – rate limit that ensures superior voice quality by dynamically limiting the bandwidth of the data so that voice will get the required bandwidth.
- Full-duplex acoustic echo cancellation with an effective 64ms tail length, -18dB network echo cancellation (volume control).
- Comfort noise generation and voice activity detection.
- Advanced error and packet loss concealment technology.
- Fax/Modem Tone Detection including T.38 support.
- DTMF tone generation and detection.
- Call tone generation.
- Caller ID generation.

  On-hook and off-hook (CID with call waiting)

  FSK (Bellcore), optional DTMF (Sweden, Denmark).
- Call Hold, Transfer and Waiting.
- Call Forwarding.
- 3-way call (conference).
- Extremely flexible dial plan options.

1.4.2 Connectivity Features

- Access 211 has two 10/100Base-TX Ethernet ports with automatic crossover detection (one WAN and one LAN).
- Access 241-FXO and Access 241 have five 10/100Base-TX Ethernet ports with automatic crossover detection (one WAN and four LAN).
- Supports eight 802.1Q compatible tagged VLANs for voice and management.
- Supports assigning priority to voice frames with the 802.1 Priority tag or TOS field.

- WAN DHCP client compliant IP address.
- Embedded HTTP server for remote Web browser-based configuration.
- NAT for LAN local devices.
- DHCP server for LAN clients.
- PPPoE support for DSL.
- PPTP support.
- Telnet.
- Support of TFTP and HTTP software upgrades.
- Display LEDs for status monitoring.

1.5 How to Get Help

For technical support, please contact your local distributor who supplied the unit.

2 Gateway Installation

2.1 Pre-Installation Requirements

Before you begin to install the Gateway, make sure that the operating environment meets the physical conditions suitable for such equipment (see operating temperature and humidity specifications in Table 2-1).

Table 2-1: Specifications

Dimensions:	4.75”(W) x 7.36”(L) x 1.77”(H) 120(W) x 187(L) x 45(H) mm
Weight:	1.32 lbs (0.6 kg)
Operating temperature:	0°C - 45°C (32°F - 113°C)
Humidity:	10% - 90% non-condensing
Access 211 and Access 241 Power Source:	5 VDC@2A – External power supply
Access 241-FXO Power Source:	5 VDC@2.6 A – External power supply
Emission and safety regulations:	FCC Class B, UL, CUL, CE

2.1.1 Equipment Requirements

To set up and use the Gateway module, you need:

- Optionally, a PC or a laptop computer with a LAN card, a web browser and Telnet.
- A 10/100BaseTX (RJ-45) Ethernet cable (supplied) to connect the Gateway to the PC.
- A 10/100BaseTX (RJ-45) Ethernet cable (supplied by your broadband access provider) for the Ethernet connection from the Gateway to your router or modem.
- For Access 241-FXO and Access 241, additional 10/100BaseTX (RJ-45) Ethernet cables to connect additional PCs.
- For Access 241-FXO – a phone cable for PSTN connection.
- The call management devices and applications appropriate for the call protocol installed on the VoIP Gateway (H.323, MGCP, or SIP).
- One or Two telephones with DTMF (tone signal) capability (not supplied).
- An AC/5VDC power adapter (supplied).

2.1.2 Telephones and Accessories

The Gateway supports all standard analog DTMF telephones and accessories, including:

- Single-line touch-tone telephones.
- Multiple-line touch-tone telephones.
- Touch-tone telephones with redial or speed-dial features.
- Phones or accessories that support Caller ID.
- Answering machines with touch-tone support.
- Phones or accessories that support Distinctive Ring.
- Fax machine

NOTE **Pulse-dial telephones and accessories are not supported.**

When using the Gateway and the attached telephone set(s), basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

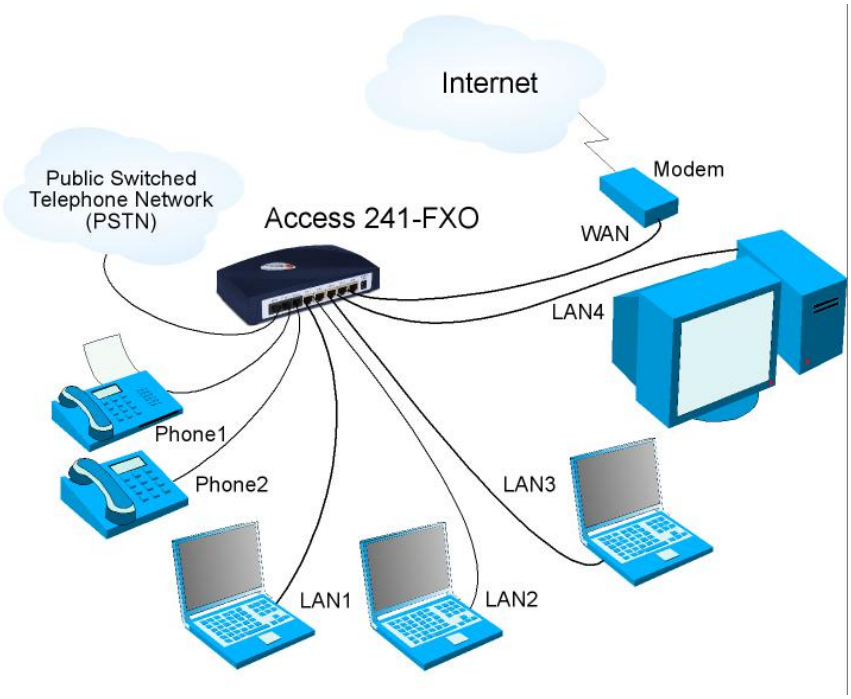
1. **Do not use this equipment near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.**
2. **Avoid using the equipment during an electrical storm. There may be a remote risk of electric shock from lightning.**
3. **Do not use the attached telephone to report a gas leak in the vicinity of the leak.**

The Access 241-FXO, Access241 and Access 211 **Gateway must be powered by an external UL listed limited power source or Class II power source (AC/DC adapter), rated input: 100 -240 V, 47-63Hz, 0.5A, output: 5VDC @ 2A.**

The phone ports (Phone1 and Phone2) are intended for indoor connections only and must not be connected to the Public Telecommunication Network. ONLY the PSTN or the Life Line port can be connected to the Public Telecommunication Network

To reduce the risk of fire, use only No. 26 AWG or larger gauge wires to connect the PSTN and Life Line port to the Telecommunication Network.

2.2 Access 241-FXO VoIP Gateway Installation



1. Unpack the Gateway unit.
2. Verify you have the components listed in the Equipment Requirements list above.
3. Place the Gateway on a desktop or other level surface, or mount it on a wall. Choose a location that is near the devices to be connected and close to an electrical outlet. If you want to mount the unit on the wall, refer to Wall-Mounting the Gateway Unit.
4. Connect the WAN port on the Gateway's rear panel to the Ethernet socket on your broadband modem using an Ethernet cable.
5. Connect a LAN port on the Gateway's rear panel to the network socket on your PC using an Ethernet cable.
6. Connect additional PCs to the other LAN ports as described in the previous step.
7. Use Phone cables to connect the telephones to the Phone1 and Phone2 ports on the rear of the Gateway. (If your provider enables only one phone line, connect the phone to the Phone1 port)

   It is possible to connect up to five phones in parallel to each phone port. To do so, connect a 5-way splitter to the phone port

8 Connect the Phone cable from the PSTN wall socket to the Gateway's PSTN port.

9. Verify that all system components are properly installed. Make sure that all cable connectors are securely positioned in the appropriate ports.
10. Connect the power adapter to the Gateway's power connector on the rear of the unit. Connect the power adapter to a wall socket.
11. Check that the Power LED on the Gateway's front panel glow steadily.
12. Turn on the PCs. For each PC perform the following:

12a. If you are using a DSL modem, you will need to enable PPPoE on the Gateway and disable PPPoE on the PC. To enable PPPoE on the Gateway:

1) Open the web browser and put the IP of the Gateway in the address field (the factory default IP address of the LAN interface is 192.168.100.1).
2) In the vertical menu bar on the left of the Gateway Web page, select **WAN**. The **WAN Status** page appears.
3) In the horizontal menu bar of the **WAN** page, select **PPPoE**. The **WAN PPPoE Configuration** page appears.
4) Select **Yes** in the **Enable PPPoE** drop-down list box.
5) Fill in the username and password in the **Authentication** fields as supplied by your DSL provider. Optionally you can enter the service name for the requested service. To select a specific provider, enter his access name in the AC name field.
6) Click **Save PPPoE Settings**.
7) After entering and saving all configurations, you must reset the Gateway. In the vertical menu bar of the current page, select **Reset**. The **Reset** page appears.
8) Select **Power on reset** and click the Reset button. The Gateway power cycles and the application's home page opens with the new configuration settings.

For more information refer to Enabling Point-to-Point Protocol over Ethernet (PPPoE).

12b. If you are using a cable modem, note that some cable modems need to be powered off and then on after being connected to the Gateway. For such modems you can also power off the Gateway and then power on for faster connection.

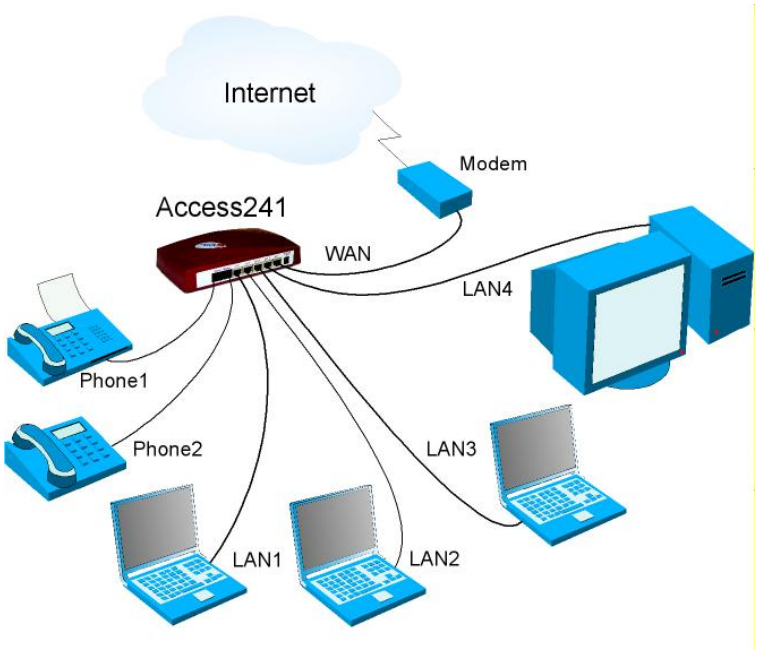
13. Wait for the Voice LED on the Gateway front panel to glow, indicating connection to your Internet and VoIP providers. It may take a minute or two for these connections to be established.

14. Verify that your broadband Internet service functions properly.

15. Pick up the phone on each line to verify that you can hear the dial tone.

Once the installation is complete and the unit is configured, you can use your Gateway for telephone calls and for the Internet, assuming there is a VoIP connection.

2.3 Access 241 VoIP Gateway Installation



1. Unpack the Access 241 Gateway unit.
2. Verify you have the components listed in the Equipment Requirements list above.
3. Place the Gateway on a desktop or other level surface, or mount it on a wall. Choose a location that is near the devices to be connected and close to an electrical outlet. If you want to mount the unit on the wall, refer to Wall-Mounting the Gateway Unit.
4. Connect the WAN port on the Gateway's rear panel to the Ethernet socket on your broadband modem using an Ethernet cable.
5. Connect the LAN port on the Gateway's rear panel to the network socket on your PC using an Ethernet cable.
6. Connect additional PCs to the other LAN ports as described in the previous step.
7. Use Phone cables to connect the telephones to the Phone1 and Phone2 ports on the rear of the Gateway. (If your provider enables only one phone line, connect the phone to the Phone1 port)

   It is possible to connect up to five phones in parallel to each phone port. To do so, connect a 5-way splitter to the phone port. (If your provider enables only one phone line, use the Phone1 port on the Gateway).
8. Verify that all system components are properly installed. Make sure that all cable connectors are securely positioned in the appropriate ports.
9. Connect the power adapter to the Gateway's power connector on the rear of the unit. Connect the power adapter to a wall socket.
10. Check that the Power LED on the Gateway's front panel glows steadily.

12. Turn on the PCs. For each PC perform the following:

12a. If you are using a DSL modem, you will need to enable PPPoE on the Gateway and disable PPPoE on the PC. To enable PPPoE on the Gateway:

   9) Open the web browser and put the IP of the Gateway in the address field (the

factory default IP address of the LAN interface is 192.168.100.1).

10) In the vertical menu bar on the left of the Gateway Web page, select **WAN**. The **WAN Status** page appears.

11) In the horizontal menu bar of the **WAN** page, select **PPPoE**. The **WAN PPPoE Configuration** page appears.

12) Select **Yes** in the **Enable PPPoE** drop-down list box.

13) Fill in the username and password in the **Authentication** fields as supplied by your DSL provider. Optionally you can enter the service name for the requested service. To select a specific provider, enter his access name in the AC name field.

14) Click **Save PPPoE Settings**.

15) After entering and saving all configurations, you must reset the Gateway. In the vertical menu bar of the current page, select **Reset**. The **Reset** page appears.

16) Select **Power on reset** and click the Reset button. The Gateway power cycles and the application's home page opens with the new configuration settings.

For more information, see Enabling Point-to-Point Protocol over Ethernet (PPPoE).

12b. If you are using a cable modem, note that some cable modems need to be powered off and then on after being connected to the Gateway. For such modems you can also power off the Gateway and then power on for faster connection.

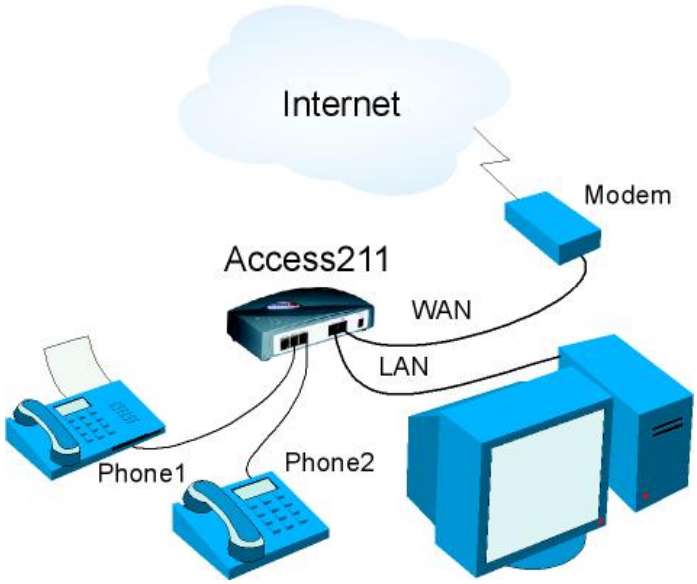
13. Wait for the Voice LED on the Gateway front panel to glow, indicating connection to your Internet and VoIP providers. It may take a minute or two for these connections to be established.

14. Verify that your broadband Internet service functions properly.

15. Pick up the phone on each line to verify that you can hear the dial tone.

Once the installation is complete and the unit is configured, you can use your Gateway for telephone calls and for the Internet, assuming there is a VoIP connection.

2.4 Access 211 VoIP Gateway Installation with a Single PC



1. Unpack the Gateway unit.
2. Verify you have the components listed in the Required Equipment list above.
3. Place the Gateway on a desktop or other level surface, or mount it on a wall. Choose a location that is near the devices to be connected and close to a wall socket.

   If you want to mount the unit on the wall, refer to Wall-Mounting the Gateway Unit.
4. Connect the WAN port on the Gateway's rear panel to the Ethernet socket on your broadband modem using an Ethernet 10/100BaseTX (RJ-45) cable.
5. Connect the LAN port on the Gateway's rear panel to the network socket on your PC using an Ethernet 10/100BaseTX (RJ-45) cable.
6. Use Phone cables to connect the telephones to the Phone1 and Phone2 ports on the rear of the Gateway. (If your provider enables only one phone line, connect the phone to the Phone1 port)

   It is possible to connect up to five phones in parallel to each phone port. To do so, connect a 5-way splitter to the phone port. (If your provider enables only one phone line, use the Phone1 port on the Gateway).
7. Verify that all system components are properly installed. Make sure that all cable connectors are securely positioned in the appropriate ports.
8. Connect the power adapter to the Gateway's power connector on the rear of the unit. Connect the power adapter to a wall socket.
9. Check that the Power LED on the Gateway's front panel glows steadily.
10. Turn on the PCs. For each PC perform the following:

10a. If you are using a DSL modem, you will need to enable PPPoE on the Gateway and

disable PPPoE on the PC. To enable PPPoE on the Gateway:

1) Open the web browser and put the IP of the Gateway in the address field (the factory default IP address of the LAN interface is 192.168.100.1).
2) In the vertical menu bar on the left of the Gateway Web page, select WAN. The WAN Status page appears.
3) In the horizontal menu bar of the WAN page, select PPPoE. The WAN PPPoE Configuration page appears.
4) Select Yes in the Enable PPPoE drop-down list box.
5) Fill in the username and password in the Authentication fields as supplied by your DSL provider. Optionally you can enter the service name for the requested service. To select a specific provider, enter his access name in the AC name field.
6) Click Save PPPoE Settings.
7) After entering and saving all configurations, you must reset the Gateway. In the vertical menu bar of the current page, select Reset. The Reset page appears.
8) Select Power on reset and click the Reset button. The Gateway power cycles and the application's home page opens with the new configuration settings.

For more information, see section Enabling Point-to-Point Protocol over Ethernet (PPPoE).

10b. If you are using a cable modem, note that some cable modems need to be powered off and then on after being connected to the Gateway. For such modems you can also power off the Gateway and then power on for faster connection.

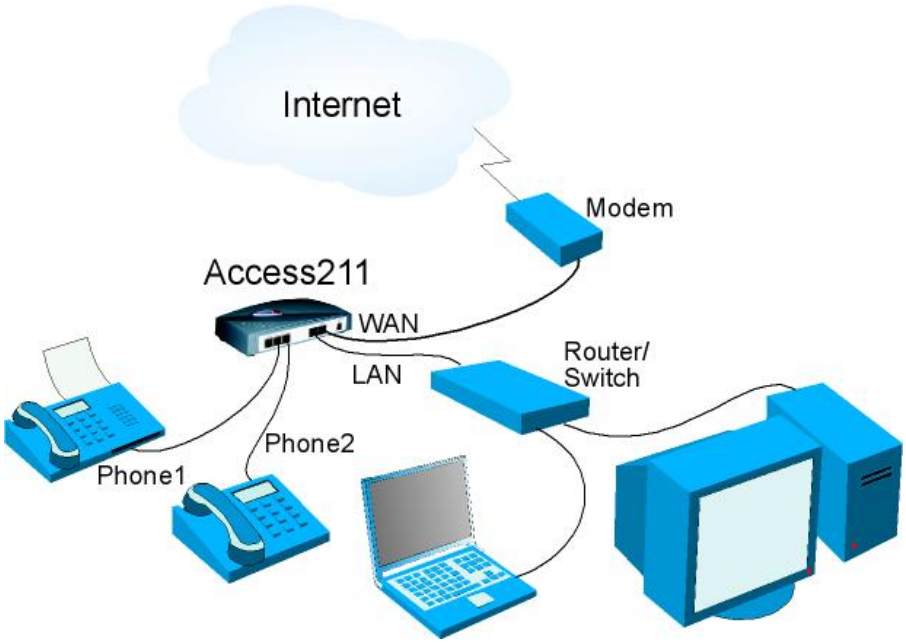
11. Wait for the Voice LED on the Gateway's front panel to glow, indicating connection to your Internet and VoIP providers. It may take a minute or two for these connections to be established.

12. Verify that your broadband Internet service functions properly.

13. Pick up the phone on each line to verify that you can hear the dial tone.

Once the installation is complete and the unit is configured, you can use your Gateway for telephone calls and for the Internet, assuming there is a VoIP connection.

2.5 Access 211 VoIP Gateway Installation with a Home Network



1. Unpack the Gateway unit.
2. Verify you have the components listed in the Equipment Requirements list above.
3. Place the Gateway on a desktop or other level surface, or mount it on a wall. Choose a location that is near the devices to be connected and close to a wall socket. If you want to mount the unit on the wall, refer to Wall-Mounting the Gateway Unit.
4. Connect the WAN port on the Gateway's rear panel to the Ethernet socket on your broadband modem with an Ethernet 10/100BaseTX (RJ-45) cable.
5. Connect the LAN port on the Gateway's rear panel to an open Ethernet LAN port on your router or switch using the supplied Ethernet 10/100BaseTX (RJ-45) cable, in accordance with the instructions provided with your router or switch.
6. Connect the phones to the Phone1 and Phone2 sockets on the Gateway rear panel with RJ-11 Phone cables. Up to five phones in parallel may be connected to each port. (If your provider enables only one phone line, use the Phone1 port).
7. Verify that all system components are properly installed. Make sure that all cable connectors are securely positioned in the appropriate ports.
8. Connect the power adapter to the power connector of the Gateway and to a wall socket.
9. Check that the Power LED on the Gateway front panel glows steadily.

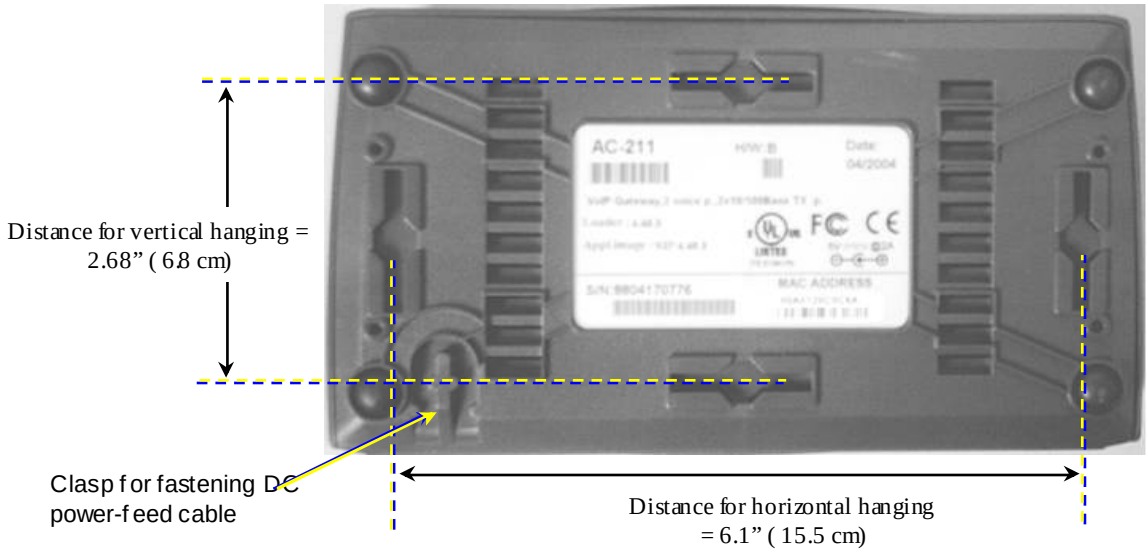
   If you are using a DSL modem, you will need to enable PPPoE as described in Enabling Point-to-Point Protocol over Ethernet (PPPoE), and disable PPPoE on your router.

10 If the Voice protocol parameters are configured, wait for the Voice LED on the Gateway front panel to glow, indicating connection to your Internet and VoIP providers. It may take a minute or two for these connections to be established.

11. Reset your router and verify that your broadband modem and your router are working. Verify that your broadband Internet service functions properly.
12. Pick up the phone on each line to verify that you can hear the dial tone.

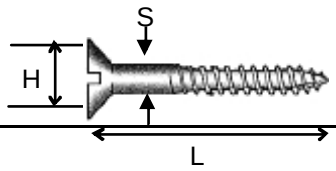
2.6 Wall-Mounting the Gateway Unit

In order to mount the unit on the wall, use two wood screws 6.1" (15.5 cm) apart for horizontal positioning or 2.68" (6.8 cm) apart for vertical positioning. Use screws as specified below. Holes for mounting on the wall are situated at the bottom of the unit, as shown in the following figure.



Mounting Screws Maximum Dimensions

Head diameter (H):	Max 9 mm (0.35")
Shank diameter (S):	Max 3.5 mm (0.138")
Length (L):	25-30 mm (1"-1.2")



3 Theory of Operation

3.1 Using the Dial Plan for SIP, H.323 and PSTN

A Dial Plan enables the gateway to recognize a complete telephone number. The gateway compares the dialed key sequence to the Dial Plan. Once a match is detected, the call is transferred to the relevant communications provider - in the case of an FXS sequence, it is passed to a SIP server / Gatekeeper, which translates it to an IP address and in the case of an FXO sequence, it is passed to the PSTN.

The Dial Plan applies to out going calls only.

3.1.1 Types of Dial Plans

There are two types of dial plans:

- The FXS Dial Plan – is utilized for voice over IP communication.
- The FXO Dial Plan – is utilized for PSTN communication.

Both dial plans are based on the same dialing rules and syntax.

The Dial Plans are supported by the following gateways:

Table 3-1: Dial Plans Supported by Gateways

Dial Plan	Access 241-FXO	Access 241	Access 211
FXS	√	√	√
FXO	√	--	--

The Access 241-FXO initially compares the dialed key sequence to its FXO Dial Plan. If it does not match, it will subsequently compare the dialed key sequence to the FXS Dial Plan. The default FXO dial plan for the Access 241-FXO is null. The dialing rules described in the following sections are demonstrated on the FXS Dial Plan but also apply to the FXO Dial Plan, except when noted.

3.1.2 Default Dial Plan

3.1.2.1 FXO Default Dial Plan

The default FXO dial plan is NULL. The administrator must configure a Dial Plan that meets the customer's needs. The Dial Plan must use the appropriate syntax as described in Dial Plan Syntax.

3.1.2.2 FXS Default Dial Plan

The FXS default dial plan includes strings separated by the vertical bar character "|".

(>#|[2-9]XXXxxxxxx|1[2-9]xxxxxxxxx|x.T)

Once a match between one of the strings and the keys that have been dialed is reached, the Gateway contacts the SIP Server\Gatekeeper and attempts to make a call. The default dial plan includes the string [2-9]xxxxxxxxx meaning that dialed numbers can be 10 digits long starting with any digit in the range 2-9. The string x.T (or x.t) in the default dial plan means that after any dialed number and a pause of 4 seconds an attempt to make a call is made. The user can use the default dial plan or set up an alternative plan.

To set the dial plan when using the H.323 protocol via Web, see Setting the H.323 Configuration. To set the dial plan when using the H.323 protocol via Telnet, see Setting the Dial Plan Matching String.

To set the dial plan when using the SIP protocol via Web, see SIP Server Configuration. To set the dial plan when using the SIP protocol via Telnet, see Setting the Dial Plan Matching String.

3.1.3 Dial Plan Syntax

A Dial Plan is a case insensitive character string or a list of strings. When creating a character string, there are many parameters to consider. The following are examples of these considerations:

- Country code
- Area code
- Office phone that operates through central phone system (e.g. dial 9 before the phone number)

Any telephone keypad character is allowed:

| "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "9" | "#" | "*" |

Table 3-2 lists the Dial Plan characters.

Table 3-2: The Dial Plan Characters

Character(s)	Description
x	One of the allowed telephone keypad (except * and #).
T or *t*	Short for *Timer*. Implies a four-second delay, and can only be used at the end of a string.
x.	Implies any number of characters (none or more).
>#	Defines the character # as a terminating character. When dialing # the dialed number preceding the character # is immediately sent.

Character(s)	Description
	The terminating character can only be entered after at least one user-dialed digit. Optionally the Dial Plan >* can be used to define the character * as the terminating character.
[character1-character2]	Defines any character in the range between character1 and character2.
P or p	Short for *Prefix*. Defines a prefix rule.
R or r	Short for *Replace*. Defines a replace rule.
|	Used to separate between multiple possible Dial Plans.

3.1.4 Dial Plan Examples

This section describes the following dial plan examples:

Simple Dial Plan; Basic Dial Plan; Complex Dial Plan; Prefix Rule Dial Plan; Replace Rule Dial Plan.

3.1.4.1 Simple Dial Plan Example

The simple dial plan example allows dialing of seven-digit numbers (e.g. 2233445) or an operator on 0. The dial plan is:

0*T*|*xxxxxxx*,

meaning that a match is produced if you dial zero followed by a four-second delay, or if you dial any seven-digit number.

3.1.4.2 Basic Dial Plan Example

The basic dial plan allows dialing of any number of digits. The dial plan is:

x.T

This ensures a match against one or more digits. A match is produced when a delay of about 4 seconds follows any number of dialed digits.

3.1.4.3 Complex Dial Plan Example

Table 3-3 lists the complex dial plan characters.

Table 3-3: The Complex Dial Plan Characters

Character(s)	Description
>#	The # character defined as a terminating character.
0*T*	Local operator on 0.

Character(s)	Description
00*T*	Long distance operator on 00.
[3-5]*xxx*	Four-digit local extension numbers starting with 3, 4, or 5.
8xxxxxxx	Seven-digit local numbers prefixed with 8.
91xxxxxxxxx	Ten-digit long distance numbers prefixed with 91.
9011*x.T*	International numbers starting with 9011 with zero or more digits.
*x.T	numbers starting with * with zero or more digits

The complete syntax scheme of this dial plan is

(>#|0T|00T|[3-5]xxx|8xxxxxxx|91xxxxxxxxx|9011x.T|*x.T)

3.1.4.4 Prefix Rule Dial Plan

Dial Plan Prefix is used to add a user defined prefix to the head of the dialed number.

Syntax: **p(***STRING1***)***STRING2*

If a dialed number matches string1, string2 is added to the head of the dialed number.

Example: **p(2x.t)00**

Adds digits 00 to any dialed number beginning with the digit 2.

3.1.4.5 Replace Rule Dial Plan

Dial Plan Replace can be used to prevent a dialed sequence from being sent or a dialed sequence can be replaced by another sequence.

Syntax: **r(***STRING,STRING2***)***STRING3*.

If a dialed number matches string1+string2, string1 is replaced by string3.

Example 1**: r(0,x.t)33**

Replaces leading 0 with 33 in a dialed number of any string beginning with zero.

Example 2: **r([1-3]0,xxx)**

Removes the digits 10, 20 or 30 from dialed numbers of format 10xxx, 20xxx or 30xxx.

Example 3: **r(1)345678**

Shortcut. Dialing 1 will be replaced with the number 345678.

3.2 Understanding DHCP

DHCP (Dynamic Host Configuration Protocol) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP, based on the Bootstrap Protocol (BOOTP), adds the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of BOOTP relay agents and DHCP participants can interoperate with BOOTP participants.

DHCP provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP Server to a host and a mechanism for allocating network addresses to hosts.

DHCP is built on a client-server model, where designated DHCP Server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. Throughout the remainder of this document, the term **server** refers to a host providing initialization parameters through DHCP, and the term **client** refers to a host requesting initialization parameters from a DHCP Server.

DHCP supports three mechanisms for IP address allocation:

- *Automatic allocation* - DHCP assigns a permanent IP address to a client.

- *Dynamic allocation* - DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). Dynamic allocation allows automatic reuse of an address that is no longer needed by the client to which it was assigned. Thus, dynamic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses. Dynamic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network where IP addresses are scarce and it is important to reclaim them when old clients are retired.

- *Manual allocation* - a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator. Manual allocation allows DHCP to be used to eliminate the error-prone process of manually configuring hosts with IP addresses in environments where (for whatever reasons) it is desirable to manage IP address assignment outside of the DHCP mechanisms.

As shown in Figure 3-1, the parameter negotiation starts with a DHCPDISCOVER broadcast message from the client seeking a DHCP Server. The DHCP Server responds with a DHCPOFFER unicast message offering configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client. The client returns a DHCPREQUEST broadcast message requesting the offered IP address from the DHCP Server. The DHCP Server responds with a DHCPACK unicast message confirming that the IP address has been allocated to the client.

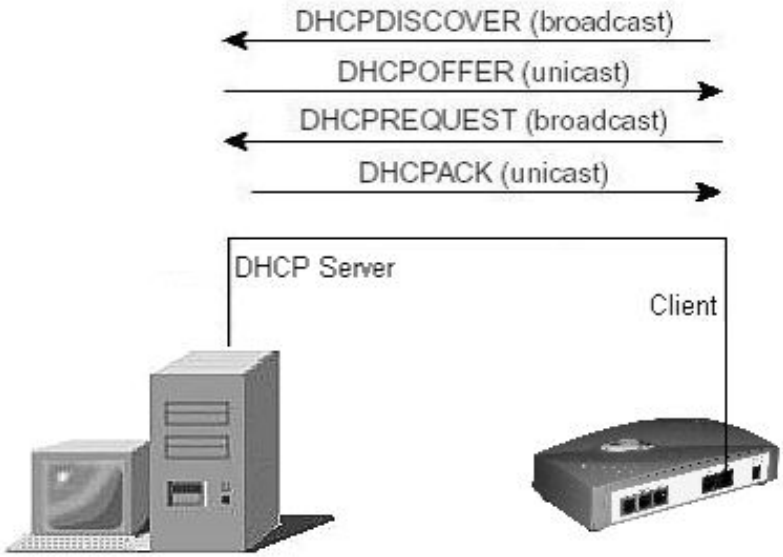


Figure 3-1: Obtaining an IP Address from a DHCP Server

The client may suggest values for the IP address and lease time in the DHCPDISCOVER message. The client may include the *requested IP address* option to suggest that a particular IP address be assigned, and may include the *IP address lease time* option to suggest the lease time it would like to have. The *requested IP address* option is to be filled in only in a DHCPREQUEST message when the client is verifying network parameters obtained previously.

If a server receives a DHCPREQUEST message with an invalid *requested IP address*, the server should respond to the client with a DHCPNAK message and may choose to report the problem to the system administrator. The server may include an error message in the *message* option.

For setting the Gateway as DHCP client on the WAN interface via Telnet see WAN Configuration Commands and via Web see Assigning an IP Address to the Gateway.

3.2.1 When Should Clients Use DHCP

A client should use DHCP to reacquire or verify its IP address and network parameters whenever the local network parameters may have changed (e.g. at the Gateway boot time or after a disconnection from the local network), as the local network configuration may change without the client's or user's knowledge.

If a client has knowledge of a previous network address and is unable to contact a local DHCP Server, the client may continue to use the previous network address until the lease for that address expires. If the lease expires before the client can contact a DHCP Server, the client must immediately discontinue use of the previous network address and may inform local users of the problem.

3.3 Understanding NAT and NAPT

The goal of the Network Address Translator (NAT) is to provide functionality as if the private network had globally unique addresses and the NAT device was not present. Basic NAT

allows a one-to-one mapping between one private address and one public address. In its simplest configuration, the NAT operates on a router connecting two networks together. One of these networks (designated as inside) is addressed with either private or obsolete addresses that need to be converted into legal addresses before packets are forwarded onto the other network (designated as outside). The translation operates in conjunction with routing, so that NAT can simply be enabled on a customer-side Internet access router when translation is desired.

NAPT (Network Port Address Translator) maps a single public address to one or many internal addresses and all network IP addresses on the connected computers are local and cannot be seen by the outside world.

NAT with Port Address Translation (NAPT) is an extension to NAT in that NAPT uses TCP/UDP ports in addition to network addresses (IP addresses) to map many private network addresses to a single outside address.

For setting the NAPT on the Gateway LAN interface via Web see Port Forwarding.

3.4 Understanding NTP

The NTP is designed to synchronize clocks among devices in a network. NTP runs over User Datagram Protocol (UDP), which runs over IP. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP is a tiered time distribution system with redundancy capability. NTP measures delays within the network and within the algorithms on the machine on which it is running. Using these tools and techniques, it is able to synchronize clocks to within milliseconds of each other when connected on a Local Area Network and within hundreds of milliseconds of each other when connected to a Wide Area Network. The tiered nature of the NTP time distribution tree enables a user to choose the accuracy needed by selecting a level (stratum) within the tree for machine placement. A time server placed higher in the tree (lower stratum number), provides a higher likelihood of agreement with the UTC time standard.

You should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time by using an encrypted authentication mechanism.

NTP has become a standard for Internet time synchronization. Most importantly, there are more than 100000 free NTP time servers in the world.

For setting the IP address of the NTP server via Web see Clock Localization.

3.4.1 Daylight Saving Time (Summer Time)

You can configure your Gateway to observe the Daylight Saving Time (DST) in your area. This way, whenever the system time is updated using a time server located in a different time area, it will be automatically corrected with the local DST time offset.

The DST is followed by the U.S. standards. You can have the Gateway advance the clock one hour at 2:00 a.m. on the first Sunday in April and move back the clock one hour at 2:00 a.m. on the last Sunday in October. You can also explicitly specify the start and end dates and times and whether or not the time adjustment recurs every year.

For enabling automatically adjust the internal clock to daylight saving time according to the local time zone via Web see Clock Localization.

3.5 Understanding PPP over Ethernet (PPPoE)

RFC 2516 describes the PPP over Ethernet (PPPoE), which provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator. With this model, each host utilizes its own PPP stack and the user is presented with a familiar user interface. Access control, billing and type of service can be done on a per-user, rather than a per-site, basis.

To provide a point-to-point connection over Ethernet, each PPP session must learn the Ethernet address of the remote peer, as well as establish a unique session identifier. PPPoE includes a discovery protocol that provides this. To set the PPPoE parameters via Web, see Enabling Point-to-Point Protocol over Ethernet (PPPoE).

3.5.1 Protocol Overview

PPPoE has two distinct stages:

1. **Discovery**

   When a Host wishes to initiate a PPPoE session, it must first perform Discovery to identify the Ethernet MAC address of the peer and establish a PPPoE SESSION_ID. While PPP defines a peer-to-peer relationship, Discovery is inherently a client-server relationship. In the Discovery process, a Host (the client) discovers an Access Concentrator (the server). Based on the network topology, there may be more than one Access Concentrator that the Host can communicate with. The Discovery stage allows the Host to discover all Access Concentrators and then select one. When Discovery is completed successfully, both the Host and the selected Access Concentrator have the information they will use to build their point-to-point connection over Ethernet.

2. **PPP Session**

   The Discovery stage remains stateless until a PPP session is established. Once a PPP session is established, both the Host and the Access Concentrator must allocate the resources for a PPP virtual interface.

3.5.2 Discovery Stage

The Discovery stage comprises four steps (see Figure 3-2). When these steps are completed, both peers know the PPPoE SESSION_ID and the peer's Ethernet address, which together define the PPPoE session uniquely. The steps consist of the Host broadcasting an Initiation packet, one or more Access Concentrators sending Offer packets, the Host sending a unicast Session Request packet to the selected Access Concentrator and the selected Access Concentrator sending a Confirmation packet. When the Host receives the Confirmation packet, it may proceed to the PPP

Session Stage. When the Access Concentrator sends the Confirmation packet, it may proceed to the PPP Session Stage.

The ETHER_TYPE field in all Discovery Ethernet frames is set to the value 0x8863.

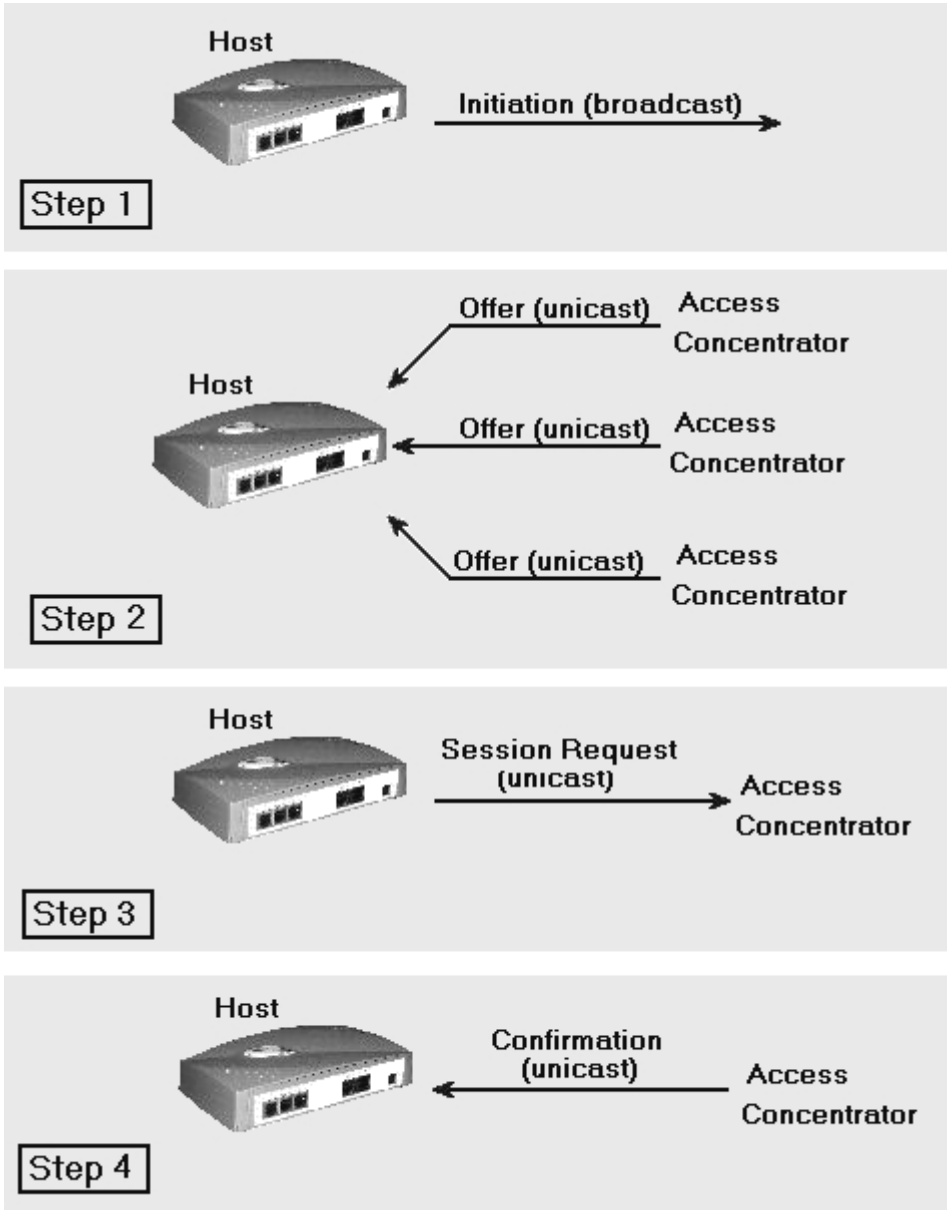


Figure 3-2: The Four Steps of the PPPoE Discovery Stage

3.5.3 PPP Session Stage

Once the PPPoE session begins, PPP data is sent as in any other PPP encapsulation. All Ethernet packets are unicast. The ETHER_TYPE field is set to 0x8864. The PPPoE payload contains a PPP frame. The frame begins with the PPP Protocol-ID.

3.6 Understanding Syslog

The system message logging can save messages in a Syslog server. The system message logging facility has the following features:

- It provides you with logging information for monitoring and troubleshooting.
- It allows you to select the types of logging information to be captured.
- It allows you to select the destination of captured logging information.

You can specify which system messages should be executed, based on their severity level (see Table 3-4). You can monitor system messages by viewing the logs on a Syslog server.

Table 3-4: Log Message Severity Levels

Severity Level	Keyword	Description
0	emergency	Internal error occurred. The Gateway reached a crash state and cannot continue to operate.
1	alert	Internal error occurred. The Gateway might operate incorrectly.
2	critical	Internal error or non supported event occurred.
3	error	Error on a setting done by user.
4	warning	Warning on a setting done by user.
5	notification	Notifies on configuration setting.
6	information	Informs on state changes.
7	debug	Debug message to be used by Technical Support.

For setting the Syslog server IP address and the log message severity level via Web see Syslog Server Configuration.

3.6.1 Remote Logging

To enable remote logging on UNIX Syslog host facility, follow these steps:

1. Configure the Syslog host to accept and log messages.
2. Enable remote logging by using the **enable syslog** command.
3. Configure remote logging by using the following command:

```
config syslog {add} <ipaddress> <facility> {<severity>}
```

Specify the following:

— *ipaddress* — The IP address of the Syslog host.

— *facility* — The Syslog facility level for local use. Options include **local0** through **local7**.

— *severity* — Filters the log to display message with the selected severity or higher (more critical).

Severities include (in order) **emergency**, **critical**, **alert**, **error**, **warning**, **notice**, **info**, and **debug**. If not specified, all messages are sent to the Syslog host.

3.7 Understanding DNS Resolver

The Domain Name System (DNS) is the means by which Internet domain names are located and translated into Internet Protocol addresses. A domain name is a mnemonic "handle" to an Internet address.

Because it would be impractical to maintain a central list of domain name/IP address correspondences, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. There is probably a DNS server within close geographic proximity to your access provider that maps the domain names in your Internet requests or forwards them to other servers in the Internet.

Figure 3-3 demonstrates how the DNS operates. The client enters a domain name (www.domainname.com) into his browser. The browser contacts the Client's ISP to obtain the IP address corresponding to the domain name. The ISP first tries to find the answer in its own "cached" data. If it finds the answer, it returns it to the client's browser. Since the ISP isn't in charge of the DNS, and is just acting as a "DNS relay", the answer is marked "non-authoritative". If the answer is not found or if it is too old (past the TTL), the ISP DNS contacts the nameservers for the domain directly for the answer. If the nameservers are not known, the ISP looks for the information at the 'root servers', or 'registry servers'. For com/net/org, these start with *a.gtld-servers.net*.

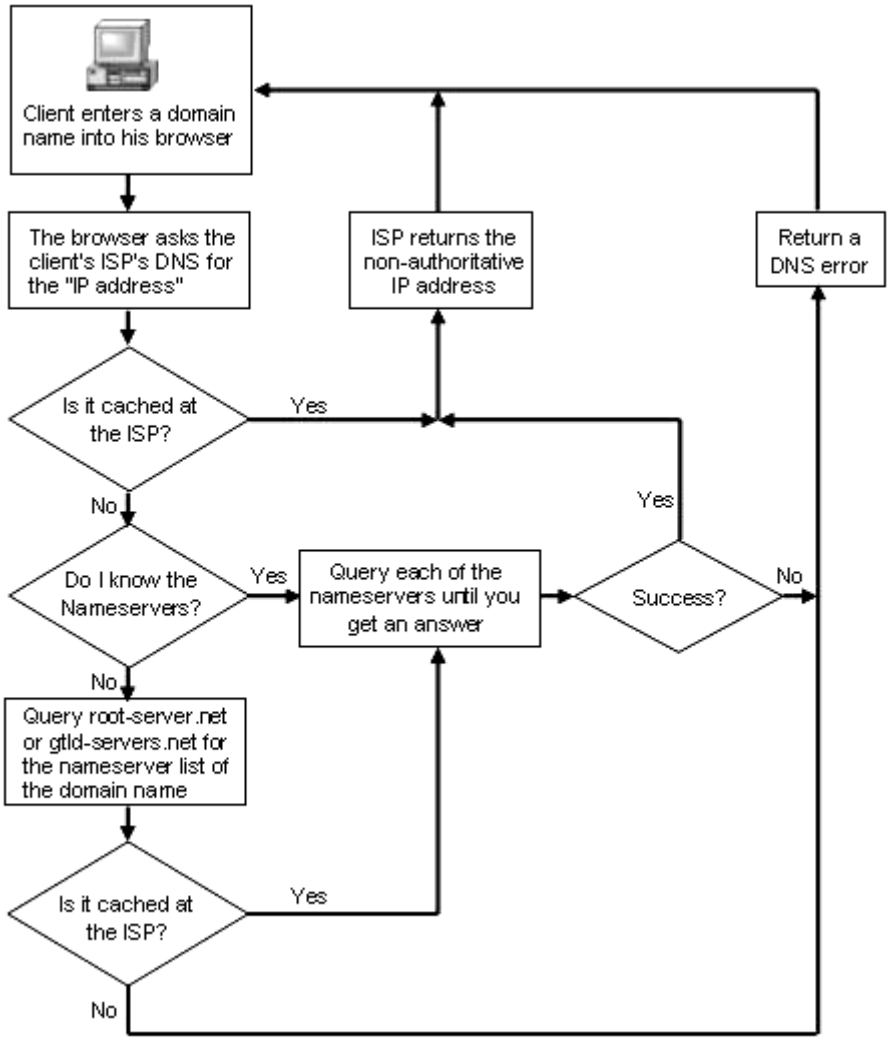


Figure 3-3: Simplified Example of how DNS Works

You can define up to two DNS servers. If a query to the primary address fails to be resolved after three attempts, the next gateway address is queried.

To use DNS, you must have a DNS server present on your network.

To set the SIP server DNS via Web, see SIP Server Configuration. To set the SIP server DNS via Telnet, see Settingthe SIP Server's Domain Name.

4 Initial Setup

To configure the Gateway, proceed as follows:

1. If a DHCP Server is not connected to the WAN interface, configure the IP Addresses on the WAN interface to use a Fixed IP. If the unit's LAN IP and WAN IP are not known use the Keypad configuration otherwise follow the configuration instructions in chapter 6 – Configuring the Gateway via Web.

2. Configure and save the VoIP protocol parameters appropriate to the protocol installed and to the Call server (H.323 - Gatekeeper; MGCP - Call agent; SIP - SIP Server).

3. Optionally configure and save other general parameters.

4. Reset the Gateway.

Once the Gateway is powered up, addressed, and configured, and the call management device (Gatekeeper, Call agent or SIP Server) is operating properly, you can place a call.

For flexible graphic configuration settings, use the WEB configuration. You can also configure, control and monitor the Gateway using Telnet. It is possible to disable either of the available management options (Web or Telnet).

4.1 Keypad Configuration

Basic configuration commands such as setting factory defaults and changing the IP mode from DHCP to fixed, or hearing the current IP address announced, can be done by entering configuration commands using the telephone keypad. Use this option if you have lost normal access to the Gateway via a PC. The following commands are activated on the telephone connected to Line 1 for ten minutes from the moment the Gateway is booted.

NOTE **The Keypad commands are active from boot for ten minutes on the telephone connected to Line 1.**

To set the factory defaults:

Dial ##3332858 (D,E,F,A,U,L,T).

Once the command is accepted, (a) you will hear "DOT" announced over the headset; (b) the Management LED on the front panel will glow a steady green; (c) after about 30 seconds the unit will power up with factory defaults.

To set the WAN IP mode:

To change the WAN IP mode from DHCP to fixed or vice-versa,

Dial ##3427937 (D,H,C,P,Y,E,S) for DHCP

OR

Dial ##342766 (D,H,C,P,N,O) for fixed WAN IP 10.1.0.54 Mask 255.255.0.0.

Once the mode is set, (a) you will hear "DOT" announced over the headset; (b) the Management LED on the front panel will glow a steady green for about 3 seconds; (c) the unit will boot with the required IP setting.

To hear the current LAN IP address announced over the headset:

Dial - ##472337 (I,P,A,D,D,R).

To hear the current WAN IP address announced over the headset:

Dial - ##47926 (I,P,W,A,N).

4.2 Keypad Configuration for MGCP

If the Keypad Configuration option is used before the Gateway is registered with the Call Agent, dial tone and other tones like "busy" will not be generated. To use the Keypad Configuration option, dial a valid Keypad Configuration sequence. If the "dot" confirmation is not heard after a short period, put the handset on the hook and repeat the dialed sequence.

5 Upgrading Firmware and Downloading Configuration Files

The Gateway is shipped from the factory, in a state of plug and play. (There is code in the Flash ROM). This section describes how to:

1. Download configuration files to the Gateway.
2. Upgrade the ROM image. (New ROM images can be obtained from your Gateway's vendor.)

A convenient way to configure the Gateway, is to download the configuration file. This can be done using one of the following optional methods:

Table 5-1: Methods for Downloading a Configuration File

Download Method	Description
Manual download	The configuration file and upgrade versions are downloaded directly via Web (see Manually Downloading the File using the Web) or Telnet (see Downloading the File Manually using Telnet.
DHCP AutoConfig (Bootp)	The configuration file and upgrade versions are downloaded automatically via DHCP server that is based on the provider's network. The "TFTP/HTTP server IP address" and the "file name" are provided by the DHCP server during the Bootp process and at half lease time. You can set DHCP server Automatic Configuration either via the Web (see Setting DHCP Automatic Configuration via the Web) or via Telnet (see Setting DHCP Automatic Configuration via Telnet).
Fixed (provisioned) TFTP/HTTP Auto Configuration	The configuration file and upgrade versions are downloaded automatically as needed during boot and at fixed polling intervals from the TFTP/HTTP server based on the provider's network. The "TFTP/HTTP server IP address" and the "file name" are provisioned into the gateway. You can set Fixed Automatic Configuration either via the Web (see Setting the TFTP/HTTP Server "Root" Configuration File via the Web) or via Telnet (see Setting the TFTP Server "Root" Configuration File via Telnet).

Two kinds of configuration files can be downloaded:

1. "Root" configuration file - the first file to be downloaded. This file can include any of the Gateway configuration parameters and three execution flags. Each execution flag can invoke one of the following possible actions:

   - Download a secondary General configuration file.
   - Upgrade the Gateway Application firmware.
   - Upgrade the Gateway Loader firmware.

   The Gateway is identified by its unique MAC address. The "root" configuration file, which typically includes specific configuration parameters, is downloaded to this address.

2. "General" configuration file - The second configuration file includes general parameters, common to a few or all the Gateway units in the network In addition, it includes the following execution flags.

   - Upgrading the Gateway Application firmware.
   - Upgrading the Gateway Loader firmware.

Both types of configuration files can also include:

- The TFTP/HTTP IP address.
- The Firmware file names.
- The Firmware file.

NOTE

1. If the Firmware file version (APP_VERSION, LDR_VERSION) parameters are used, a firmware upgrade will take place only if the Firmware file version differs from the current firmware version.

2. The name of the "root" configuration file must be of this format- *ipg_xxxx.cfg*.

3. Configuration files must include header "; Configuration Parameters. Don't edit this line !!! ". You can find an example of this file later in this guide and/or see file ipg_example.cfg.

4. To control the conditions for including new configuration parameters, use the 'Automatic Configuration ID' in the root file.

NOTE

The Gateway's configuration parameters are stored and valid for all firmware upgrades. Resetting to defaults is recommended only if the VoIP protocol was changed (e.g. from SIP to MGCP).

5.1 Manually Downloading the File using Telnet

```
IPG >
IPG >
IPG >
IPG >
```

```
IPG >commands
IPG.Commands >copy 192.168.1.16 sip_211_4_55_23.rom
```

Or:

```
IPG.Commands >copy 192.168.1.16 ipg_211_00a012112233.cfg
```

NOTE **Copy will work only if Auto Configuration flag is disabled.**

5.2 Manually Downloading the File using the Web

In order to manually download files (either upgrade files or configuration files):

1. In the vertical menu bar on the left, select **Download**.

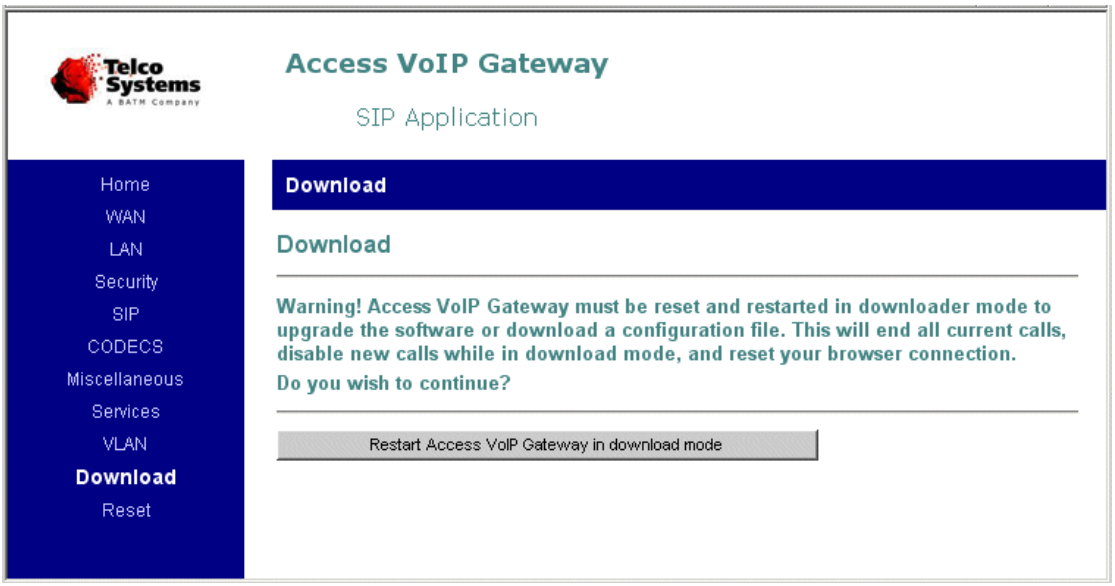


Figure 5-1: Download Page

2. Press the button labeled: **Restart access VoIP Gateway in download mode to boot the Gateway.** This may take several seconds. Notice that the name at the top of the screen indicates it is in Loader mode.

Warning! **Access VoIP Gateway must be reset and restarted in downloader mode to upgrade the software or download a configuration file. This will end all current calls, disable new calls while in download mode, and reset your browser connection.**

Figure 5-2: Download Page (TFTP/HTTP)

3. Choose the desired download method
   a. For **TFTP/HTTP Download**, enter the server address, enter the required filename and then click **Start Download**.
   b. For **HTTP ROM Download**, enter the required filename, verify that HTTP is selected in the **WAN**, **Auto Configuration** menu, and then click **Start HTTP Download**.
4. At the end of the process, exit Loader mode by clicking **Reset**. The Gateway Configuration will return to regular operation.

5.3 DHCP Automatic Configuration

In DHCP download (Bootp), the Gateway must be in DHCP mode. The names of the "root" configuration file and the IP of the TFTP/HTTP server are supplied to the Gateway when the Gateway queries the DHCP server for an IP address and a boot file, during boot and at half lease-time.

5.3.1 Setting DHCP Automatic Configuration via the Web

1. Open the **WAN Status** page (Figure 5-3).

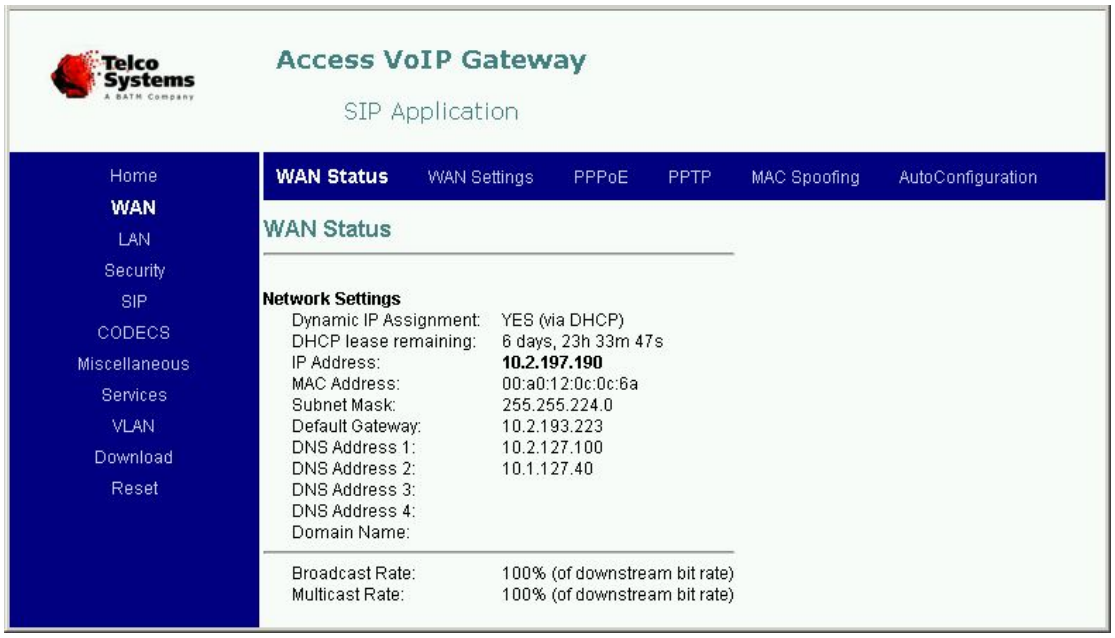


Figure 5-3: WAN Status Page

2. In the horizontal menu bar of the **WAN Status** page, select **WAN Settings** (Figure 5-4). Verify that the **Obtain WAN configuration dynamically** option is selected.

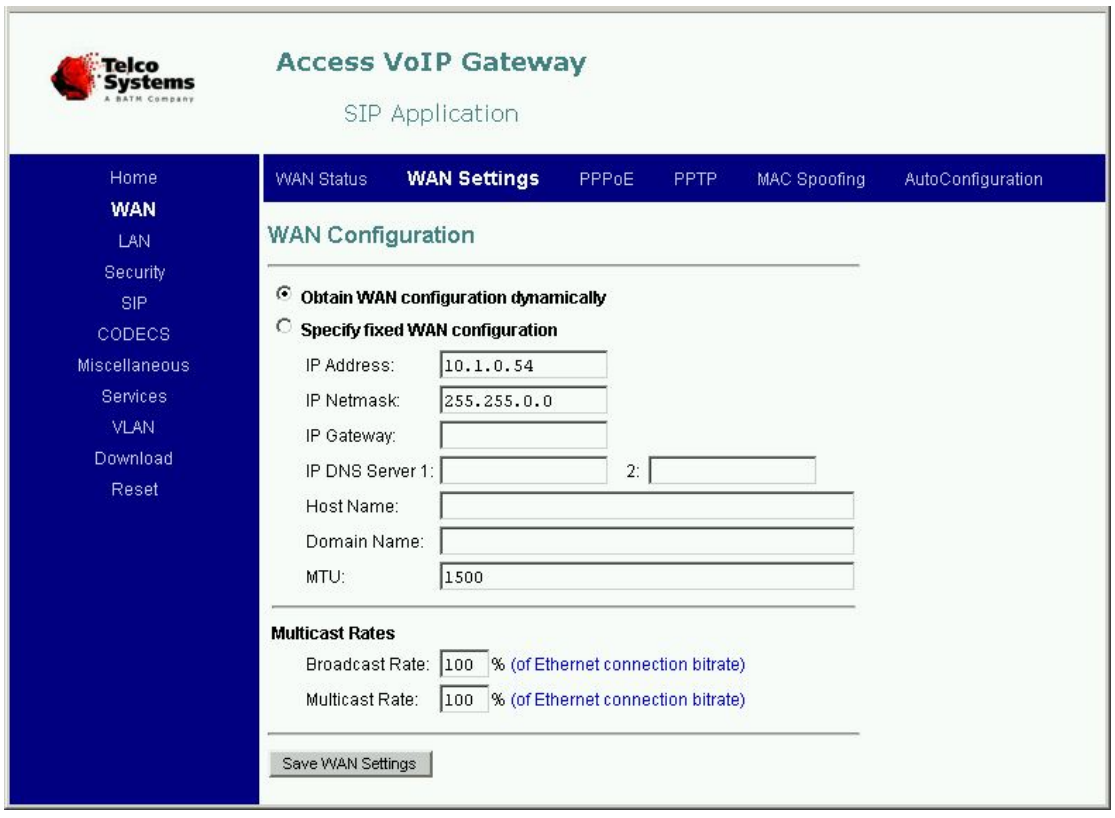


Figure 5-4: WAN Configuration Page

3. In the horizontal menu bar of the **WAN Configuration** page, select **AutoConfiguration** (Figure 5-5). Verify that the **Enable Automatic Configuration** option is selected.

Figure 5-5: Automatic Configuration Page

4. For Microsoft DHCP server:

   - Select **Use DHCP code options 66, 67** in the Gateway.

     In DHCP download (Bootp), the Gateway must be in DHCP mode. The name of the "root" configuration file and the IP address of the TFTP server are supplied to the Gateway when the Gateway queries the DHCP server for an IP address and a boot file, during boot and at half lease-time.

   - Reserve a station and define its MAC and IP.

   - Add options 66,67.

     - Option 66 (**TFTP Server Name Option**) - used to identify a TFTP server when the *name* (the "root" file) field in the DHCP header is being used for DHCP options.

     - Option 67 (**Bootfile Name Option**) - used to identify a boot-file (the "root" file) when the file field is the DHCP header that is being used for DHCP options.

   - Set the **Automatic configuration ID**.

     Set the Automatic configuration ID. Verify that it differs from the value on the DHCP Server. The Automatic configuration ID on the DHCP Server can be set to the value "always". This causes the configuration file to be executed on every boot without comparing to the ID stored in the Gateway.

5. Click on **Save Settings** to save the updated network settings.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

5.3.2 Setting DHCP Automatic Configuration via Telnet

1. Use the set **show dhcp** (**sh d**) command in WAN Configuration mode to verify that the WAN configuration is obtained dynamically.

```
IPG.Config.Network.Wan >show dhcp
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > dhcp|dh                    = y
```

   If the WAN configuration is not obtained dynamically, use the **set dhcp** (**se d**) command in WAN Configuration mode.

```
IPG.Config.Network.Wan >set dhcp y
```

2. Use the set **show autoconfig** (**sh a**) command in WAN Configuration mode to verify that the automatic configuration is enabled.

```
IPG.Config.Network.Wan >show autoconfig
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > autoconfig|a               = y
```

   If the automatic configuration is not enabled, use the **set autoconfig** (**se a**) command in WAN Configuration mode.

```
IPG.Config.Network.Wan >set autoconfig y
```

3. For Microsoft DHCP server:

   - Set the using of DHCP options 66, 67 by using the **set options6667** (**se o**) command in WAN Configuration mode. You can display the status of the DHCP options 66, 67 by using the **show options6667** (**sh o**) command in WAN Configuration mode.

```
IPG.Config.Network.Wan >set options6667 y
IPG.Config.Network.Wan >show options6667
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > options6667|o              = y
```

   - Set the Automatic configuration ID to a value different from the value on the DHCP server, by using the **set id** (**se id**) command in WAN Configuration mode. You can display the Automatic configuration ID by using the **show id** (**sh id**) command in WAN Configuration mode. To cause the configuration file to be executed on every boot and half lease time without comparing to the ID stored in the Gateway, set the DHCP server the ID to **always**.

```
IPG.Config.Network.Wan >set id 5
IPG.Config.Network.Wan >show id
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > id|id                      = 5
```

   - Reboot the Gateway for applying the changes by using the **reboot power** (**r p**) command is Commands mode.

```
IPG.Commands >reboot power
IPG.Commands > Warning! Reset system (y/n) ? y
```

5.4 Fixed (Provisioned) HTTP or TFTP Automatic Configuration

You can supply the IP address of the HTTP/TFTP server and the name of the "root" configuration file directly to the Gateway, instead of through the DHCP options. During boot, and at defined polling periods, the Gateway will poll the HTTP/TFTP server for a configuration file and will determine if an upgrade is needed.

NOTE **If Automatic Configuration is enabled, the IP address of the HTTP/TFTP server and the name of the "root" configuration file that are supplied by the user override the values obtained by the DHCP server.**

5.4.1 Setting the TFTP/HTTP Server "Root" Configuration File via the Web

1. Open the **WAN Status** page (Figure 5-3).
2. In the horizontal menu bar of the **WAN Status** page, select **WAN Settings**, You may select either of the following options: **Obtain WAN configuration dynamically** or **Specify fixed WAN configuration** (Figure 5-4).
3. In the horizontal menu bar of the **WAN Status** page, select **AutoConfiguration** (Figure 5-5). Verify that the **Enable Automatic Configuration** option is set.
4. Set the polling time (in hours) in the **Polling time (hours)** field. The polling time sets the time period for the file download.
5. Set the server protocol (HTTP or TFTP) in the **Server protocol** field.
6. Set the server IP address for the location of the configuration files in the **Server Address** field.
7. Set the name of the "root" configuration file in the **File name** field.

   The file name has the following syntax: *ipg_xxxx.cfg* where *xxxx* is free text, up to 90 characters in length.
8. Click on **Save Settings** to save the updated network settings.

NOTE **After entering and saving all configurations, you MUST Reset the Gateway.**

5.4.2 Setting the TFTP Server "Root" Configuration File via Telnet

1. The WAN configuration can be obtained dynamically or can be fixed. Use the **show dhcp** (**sh d**) command in WAN Configuration mode to verify the WAN DHCP configuration.

```
IPG.Config.Network.Wan >show dhcp
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > dhcp|dh                = y
```

If you wish to change the WAN DHCP configuration use the **set dhcp** (**se d**) command in WAN Configuration mode.

```
IPG.Config.Network.Wan >set dhcp y
```

2. Use the set **show autoconfig** (**sh a**) command in WAN Configuration mode to verify that the automatic configuration is enabled.

```
IPG.Config.Network.Wan >show autoconfig
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > autoconfig|a           = y
```

If the automatic configuration is not enabled, use the **set autoconfig** (**se a**) command in WAN Configuration mode.

```
IPG.Config.Network.Wan >set autoconfig y
```

3. Set the HTTP/TFTP server IP address for the location for the configuration files by using the **set tftpip** (**se t**) command in WAN Configuration mode. Use the **show tftpip** (**sh t**) command in WAN Configuration mode to verify the HTTP/TFTP server IP address.

```
IPG.Config.Network.Wan >set tftpip 10.2.197.9
IPG.Config.Network.Wan >show tftpip
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > tftpip|t               = 10.2.197.9
```

4. Set the "root" configuration file name by using the **set file** (**se f**) command in WAN Configuration mode. Use the **show file** (**sh f**) command in WAN Configuration mode to verify the name of the "root" configuration file.

   The file name has the following syntax: *ipg_xxxx.cfg* where *xxxx* is free text.

```
IPG.Config.Network.Wan >set file ipg_test.cfg
IPG.Config.Network.Wan >show file
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > file|f                 = ipg_test.cfg
```

5. Reboot the Gateway to effect the changes by using the **reboot power** (**r p**) command in Commands mode.

```
IPG.Commands >reboot power
IPG.Commands > Warning! Reset system (y/n) ? y
```

5.5 Creating and Encrypting Configuration Files

Use file **ipg_example.cfg**, as an example to create your own configuration file. Valid commands can be found in the file **config211_define.txt**. The "root" file name must be the following format: **ipg_*xxxx*.cfg**. For added security you can encrypt the "root" and General configuration files.

To encrypt a configuration file:

1. Install the encryption key(s) into the Gateway (see sections Setting the "Root" File Encryption Key and Installing a General Configuration File Encryption Key). The maximum size is 64 characters.

2. Encrypt the configuration file with the ***gwBin*** utility using the same encryption key that you entered into the Gateway. Make sure that the name given to the encrypted file is of format **ipg_*xxxx*.cfg**.

6 Configuring the Gateway via Web

You can configure the Gateway remotely via a PC Web browser. The Gateway can be configured to use a fixed WAN IP address or to acquire a WAN IP address from a DHCP server. The Gateway is factory set to acquire a WAN IP from a DHCP server.

1. Connect a PC to the LAN port.
2. Enter the default LAN IP address (192.168.100.1) of the Gateway into the Web browser to open the home page of the Gateway (Figure 6-1). If the page does not open, the default IP address may have been changed.
3. You can learn the subnet either by checking the PC's IP address (provided that the PC is configured as a DHCP client) or by using the Keypad option.

You can also configure the Gateway remotely with a Web browser via the WAN port, provided that a DHCP server is attached to the WAN port.

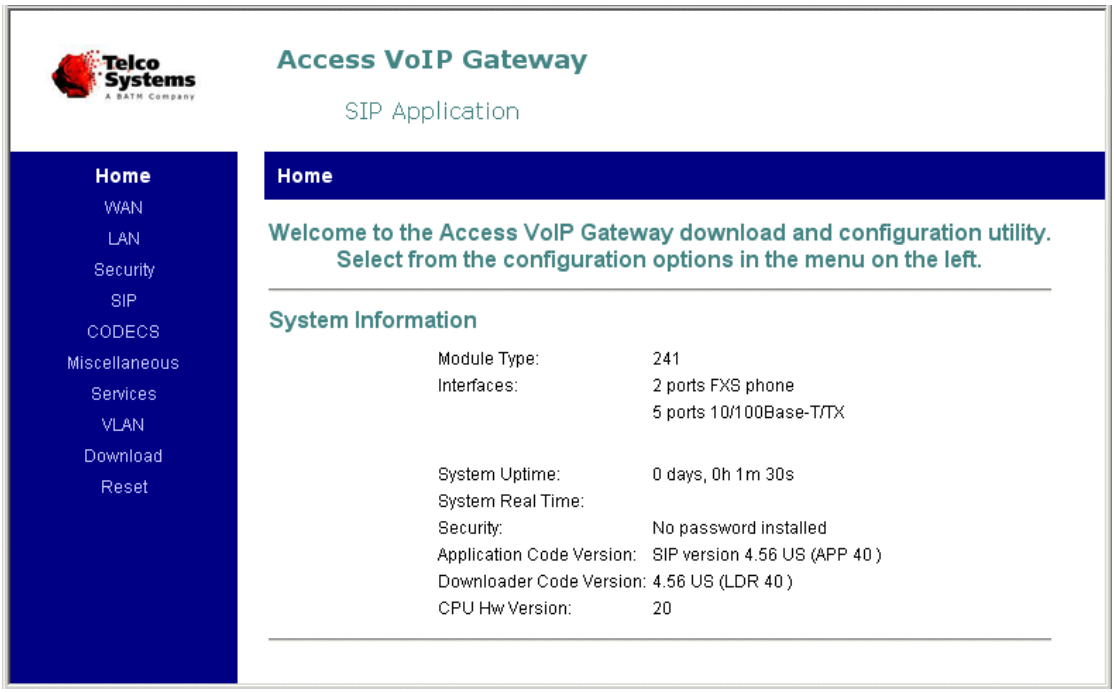


Figure 6-1: Example Gateway Home Page

To start a Web session with your Gateway:

1. Connect your PC to a LAN port on the rear of the Gateway or access remotely via the WAN port.

2. For local (LAN) connection, enter the default LAN IP address (192.168.100.1) of the Gateway into the PC Web browser. For remote (WAN) connection, enter the WAN IP address acquired from the DHCP server (see Figure 6-1).

To update a setting, enter the required settings on a web page and then save the changes by clicking on the **Save** button at the bottom of the page. Once all settings have been saved, select the **Reset** option on the left-hand side of the Web page to reset the Gateway and effectuate the new settings.

7 WAN Configuration via Web

The WAN Configuration Web pages allow you to configure the following WAN settings:

- WAN IP address, netmask and gateway address.
- IP DNS Server addresses, host and domain name.
- WAN broadcast and multicast traffic limitation.
- Point-to-Point Protocol over Ethernet (PPPoE) authentication and settings.
- Point-to-Point Tunneling Protocol authentication and settings.
- MAC spoofing (overriding the MAC address registered at the broadband provider).
- Automatic configuration at preset time intervals.

7.1 Default WAN Configuration

Table 7-1: Default WAN Configuration

Parameter	Default Value
Obtain IP address	Use DHCP Server
Broadcast limit	100%
Multicast limit	100%
Enable PPPoE	Disabled
Enable PPTP	Disabled
MAC Spoofing	Blank
DHCP automatic configuration ID	0
DHCP options 66, 67	Enabled
Auto Config mode	Enabled
Server Protocol	TFTP

7.2 WAN Status Page

To open the WAN Configuration pages:

In the vertical menu bar on the left of the Gateway Web page, select **WAN**.
The **WAN Status** page appears (Figure 7-1).

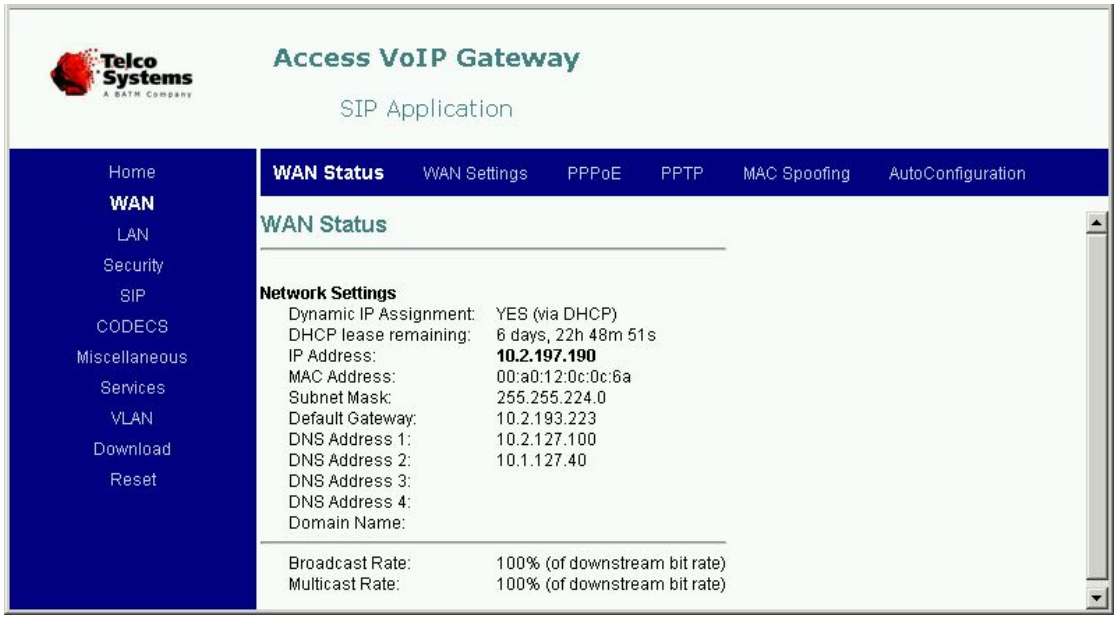


Figure 7-1: WAN Status Page

7.3 Assigning an IP Address to the Gateway

On the **WAN Setting** page, you can choose whether you want to obtain the IP address by a DHCP server or to set the IP address statically.

To change the mode from Using DHCP to Fixed IP, or to assign a different fixed IP address, configure the unit as follows:

- To change network settings, select **WAN Settings** on the horizontal menu bar. The **WAN Configuration** page appears (Figure 7-2).

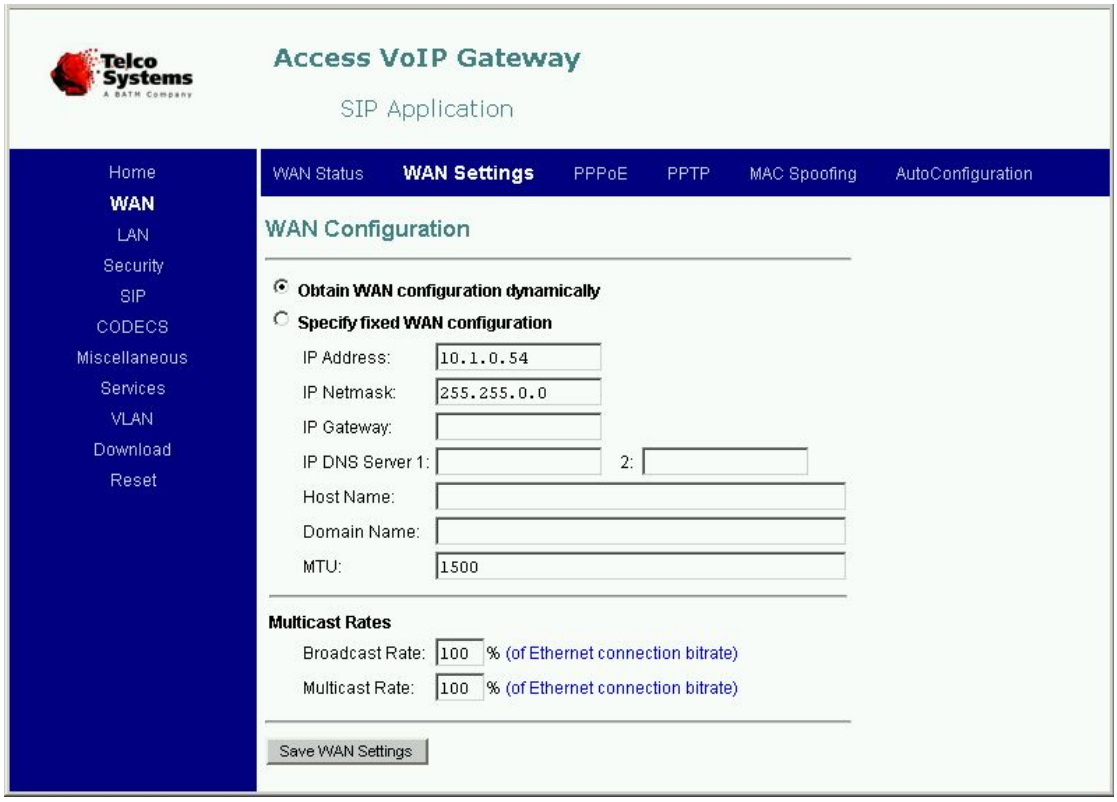


Figure 7-2: WAN Configuration Page

- **WAN Settings**

  Select either of the following options:

  - To use a DHCP server select **Obtain WAN configuration dynamically**. For more information regarding the DHCP protocol, refer to Understanding DHCP.

  - To specify fixed values for the WAN IP address, mask, gateway, DNS Server, etc select **Specify fixed WAN Configuration**.

    The fields associated with fixed IP addressing should be filled in or changed only if your broadband provider requires them. Use the values supplied by your broadband provider for the fields that are described in Table 7-2.

Table 7-2: The Available WAN Settings Configuration Fields

Field Name	Description
IP Address	The IP address of the WAN interface if **Specify fixed WAN Configuration** was selected.
IP Netmask	The subnet mask of the WAN interface if **Specify fixed WAN Configuration** was selected.
IP Gateway	The default gateway of the WAN interface if **Specify fixed WAN Configuration** was selected.
IP DNS Server 1	Statically assigned DNS server IP address, which will be provided to clients during the OFFER process.

Field Name	Description
IP DNS Server 2	Statically assigned DNS server IP address, which will be provided to clients during the OFFER process.
Host Name	The host name of the WAN.
Domain Name	The domain-name of the interface if **Specify fixed WAN Configuration** was selected.

NOTE **If you enabled PPPoE, the network IP parameters are acquired dynamically from the DSL provider if** Obtain WAN configuration dynamically **was selected.**

- **Multicast Rates**

  You can limit the broadcast and multicast traffic to your local network on the Gateway. Limiting this kind of traffic allows you to protect your local network from broadcast and multicast storms that can affect the voice and data traffic passing through the gateway.

  To limit broadcast and multicast traffic see the parameters described in Table 7-3.

Table 7-3: The Available Multicast Rates Configuration Fields

Field Name	Description
Broadcast Limit	Specifies the maximum limit on the percentage of multicast packets, which will be bridged to the LAN interface in Kbps (as a percentage of the WAN bandwidth).
Multicast Limit	Specifies the maximum limit on the percentage of broadcast packets which will be bridged to the LAN interface in Kbps (as a percentage of the WAN bandwidth).

- Scroll down to the bottom of the Web page, and click **Save WAN Settings**.
- Select **Reset** in the vertical menu bar, to reset the unit (see Completing the Gateway Configuration via Web). You can now use the new IP address.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

7.4 Enabling Point-to-Point Protocol over Ethernet (PPPoE)

The PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an LAN to a remote site through common CPE (Customer Premises Equipment). PPPoE can be used to have an office or building full of users share a common DSL (Digital Subscriber Line), cable modem, or wireless connection to the Internet. For more information regarding the theory of PPPoE see Understanding PPP over Ethernet (PPPoE).

If you have a DSL modem and are NOT using a router between the Gateway and the modem, configure PPPoE as follows:

- In the horizontal menu bar of the **WAN** page, select **PPPoE**. The **WAN PPPoE Configuration** page appears (Figure 7-3).

Figure 7-3: WAN PPPoE Configuration Page

- **Enable PPPoE**

  Select **Yes** in the **Enable PPPoE** drop-down list box to enable PPPoE (PPP-over-Ethernet).

- **Authentication**

  Fill in the username and password in the **Authentication** fields as supplied by your DSL provider. Optionally you can enter the service name for the requested service. To select a specific provider, enter his access name in the AC name field. Table 7-4 lists the available PPPoE fields.

- **PPPoE Settings**

  Optionally, you can set the PPPoE parameters (described in Table 7-4):

- Idle Timeout (in minutes)
- Service Name
- AC Name

- Click **Save PPPoE Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Table 7-4: The PPPoE Configuration Fields

Field Name	Description
User Name	PPP authentication user name supplied by your DSL provider.
Password	PPP authentication password supplied by your DSL provider.
Idle Timeout	Idle timeout in minutes before PPP connection is closed due to inactivity.
Service Name	PPPoE service name (supplied by your DSL provider).
AC Name	PPPoE Access name (supplied by your DSL provider).

7.5 Enabling the Point-to-Point Tunneling Protocol (PPTP)

The Point-to-Point-Tunneling Protocol (PPTP) is a networking technology that enables authenticating a user prior to granting access to a node. With PPTP, users can be authenticated prior to dialing in to their corporate network via the Internet.

If you need to setup a PPTP connection configure PPTP as follows:

- In the horizontal menu bar of the **WAN** page, select **PPTP**. The **PPTP Configuration** page appears (Figure 7-4).

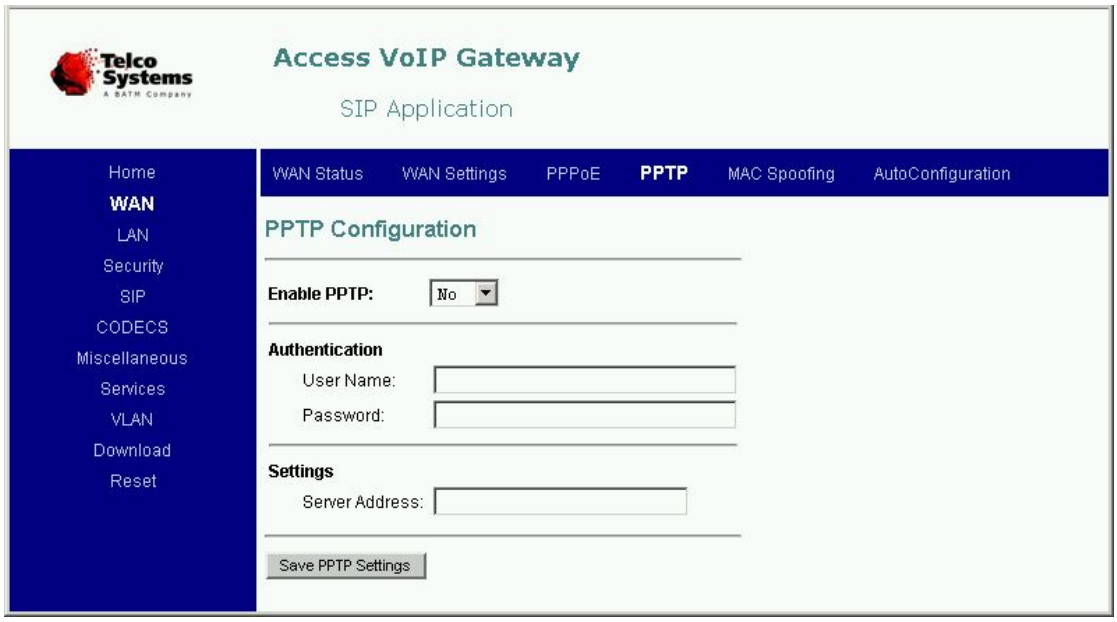


Figure 7-4: WAN PPTP Configuration Page

- **Enable PPTP**

  Select **Yes** in the **Enable PPTP** drop-down list box to enable PPTP (Point-to-Point-Tunneling).

- **Authentication**

  Fill in the username and password in the **Authentication** fields as supplied by your service provider.

- **PPTP Settings**

  Optionally, you can set the PPTP Server IP address or Domain name in the **Server Address** field.

- Click **Save PPTP Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Table 7-5: The PPTP Configuration Fields

Field Name	Description
User Name	PPTP authentication user name supplied by your service provider.
Password	PPTP authentication password supplied by your service provider.
Server Address	PPTP Server IP Address or domain name supplied by your service provider.

7.6 MAC Spoofing

MAC spoofing may be required in the case that your broadband provider associates a particular service to a specific device (e.g. your computer). The MAC address is a 12 digit hexadecimal number that is used by the Gateway's WAN interface.

To override the Gateway's MAC address that will be sent to your broadband provider

1. In the horizontal menu bar of the **WAN** page, select **MAC Spoofing**. The **MAC Spoofing Configuration** page appears (Figure 7-5).

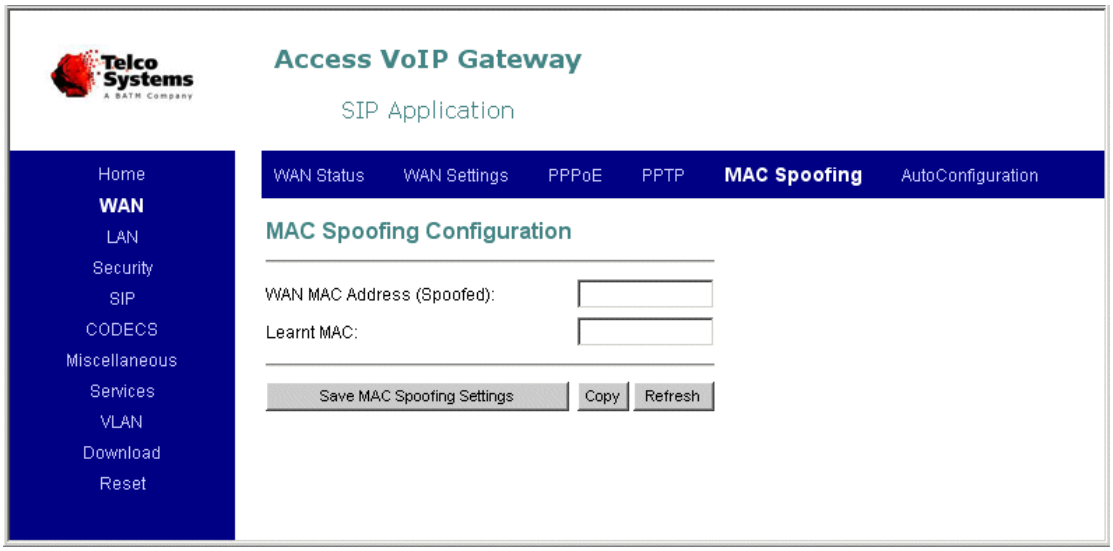


Figure 7-5: MAC Spoofing Configuration Page

2a. If you know the MAC address of your device, enter it into the WAN MAC Address (Spoofed) field.

2b. If you do not know the MAC address of your device, copy the value from the Learnt MAC's field to the WAN MAC Address field.

3. Click **Save MAC Spoofing Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

7.7 AutoConfiguration

To enable and set automatic configuration (see Upgrading Firmware and Downloading Configuration Files):

1. In the horizontal menu bar of the **WAN** page, select **AutoConfguration**. The **Automatic Configuration** page appears (Figure 7-6).

Figure 7-6: Automatic Configuration Page

2. Select the **Enable Automatic Configuration** check box for enabling automatic configuration.

3. Enter the **Automatic configuration ID**. The Gateway will run the configuration file only if the file name or ID is different from the ones currently stored in the Gateway.

   For DHCP Download you can set the ID also at the DHCP server along with the file name (e.g., ipg_12345.cfg, 8). For Fixed Auto Configuration the ID can be set also in the "root" Configuration file.

   The ID at the DHCP server or in the Configuration file can be set to the literal value "always", causing the configuration file to be executed on every boot without comparing to the ID stored in the Gateway.

4. In DHCP download (Bootp), the Gateway must be in DHCP mode. The name of the "root" configuration file and the IP of the TFTP server are supplied to the Gateway when the Gateway queries the DHCP server for an IP address and a boot file, during boot and at half lease-time.

   To enable using DHCP options 66, 67, select the **Use DHCP code options 66,67** check box. When this check box is selected:

   - Option 66 (**Boot Server Host Name**) is set as the IP of the TFTP server for the "root" configuration file.
   - Option 67 (**Bootfile Name**) is set as the name of the "root" configuration file.

5. For Fixed Auto Configuration set the **polling time** interval in hours.

6. To select Fixed (Provisioned) Auto Configuration, supply the IP address of the *HTTP/TFTP server* and the name of the "root" configuration file directly to the Gateway, instead of through the DHCP options. During boot, and at defined polling

periods, the Gateway will poll the HTTP/TFTP Server for a configuration file and will determine if an upgrade is needed.

7. Set the *Server IP* address.

8. Set the *file name* ("root" configuration file) to download.

9. Set the Server protocol (HTTP or TFTP).

10. Click **Save Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

---

8 LAN Configuration via Web

The LAN Configuration Web pages allow you to configure the following WAN settings:

- LAN IP address and subnet mask.
- LAN broadcast and multicast traffic limitation.
- Rate control – for insuring that even while running heavy bandwidth applications (data traffic) on the devices connected to LAN port the voice quality is preserved.
- DHCP Server settings.
- Port forwarding – to enable access to local ports from an external network using NPAT (Network Port Address Translator).

8.1 Default LAN Configuration

Table 8-1: Default LAN Configuration

Parameter	Default Value
Broadcast Rate	100%
Multicast Rate	100%
Rate Limit	Disabled
Rate Limit Method	Fixed
Fixed Rate Limit	32 Kbps
Dynamic rate limit	32 Kbps
IPSec NAT Traverse	Disabled
DHCP server default lease time	86400 seconds (24 hours)
Default IP address of the LAN interface	192.168.100.1
Default IP address of the DHCP client	192.168.100.100

8.2 Configuring LAN Settings

To open the LAN Configuration pages:

In the vertical menu bar on the left of the Gateway Web page, select **LAN**.
The **LAN Configuration** page appears (Figure 8-1).

Figure 8-1: LAN Settings Page

To configure LAN settings, broadcast and multicast traffic limits and/or rate control, proceed as follows:

- **Network Settings**

  In the **LAN Configuration** page, enter the following LAN parameters:

  - **IP Address** - The IP Address of the LAN interface.
  - **Subnet Mask** - The subnet mask of the LAN interface.

NOTE **LAN Subnet (combination of IP address and mask) must differ from the WAN Subnet. If they are identical, the portion of the LAN Subnet of the LAN IP is incremented until they differ. The new LAN value is saved and the unit will reboot with the new value.**

- **Multicast Rates**

  Optionally, set the broadcast and multicast limits in the appropriate fields:

  Broadcast Rate - specifies the maximum limit on the percentage of multicast packets, which will be bridged to the WAN interface in Kbps (as a percentage of the LAN side bandwidth).

  Multicast Rate - specifies the maximum limit on the percentage of broadcast packets, which will be bridged to the WAN interface in Kbps (as a percentage of the LAN

bandwidth).

- **Rate Control**

  With the Rate control feature you can limit the data bandwidth allocated to the device(s) connected to the LAN port. This is especially important for broadband users where the upload link to the ISP is considerably lower than the download link from the ISP. Setting the Rate control parameters will insure that even while running heavy bandwidth applications (data traffic) on the devices connected to LAN port the voice quality is preserved.

  You can choose one of the following rate control options:

  - **Disable Rate Limits** (default)
  - **Dynamic Rate Limits**
  - **Fixed Rate Limits**

  If you want to set rate limits, select **Fixed Rate Limits** or **Dynamic Rate Limits**:

  - Select **Fixed Rate Limits** and set the **LAN Rate Limit Rate** field to limit the bandwidth received from the LAN to the value of the LAN Rate Limit that is specified in the textbox (in Kbps). By default the **LAN Rate Limit** is set to 32 Kbps. The range of possible values is <32-131040> Kbps.

  - Select **Dynamic Rate Limits** option and set the **User Upload Rate** field to the value of the user's available upload bandwidth on the WAN connection. The Access gateway will dynamically reserve bandwidth for the active calls and limit the bandwidth for the LAN device to the remaining available bandwidth. By default the **User Upload Rate** is set to 32 Kbps. The range of possible values is <12-131040> Kbps.

    You can view the actual bandwidth allocated to the LAN device in the **Current LAN Rate Limit** parameter.

- Click Save LAN Settings.

NOTE **Rate Control changes are applied immediately after entering and saving. For all other configuration settings, you MUST reset the Gateway.**

8.3 DHCP Server Configuration

For background information regarding the DHCP protocol, refer to Understanding DHCP.

To use DHCP Server for assigning IP addresses and subnet masks automatically to devices connected to the LAN ports, proceed as follows:

In the horizontal menu bar of the **LAN** page, select **DHCP**. The **DHCP Server Configuration** page appears (Figure 8-2).

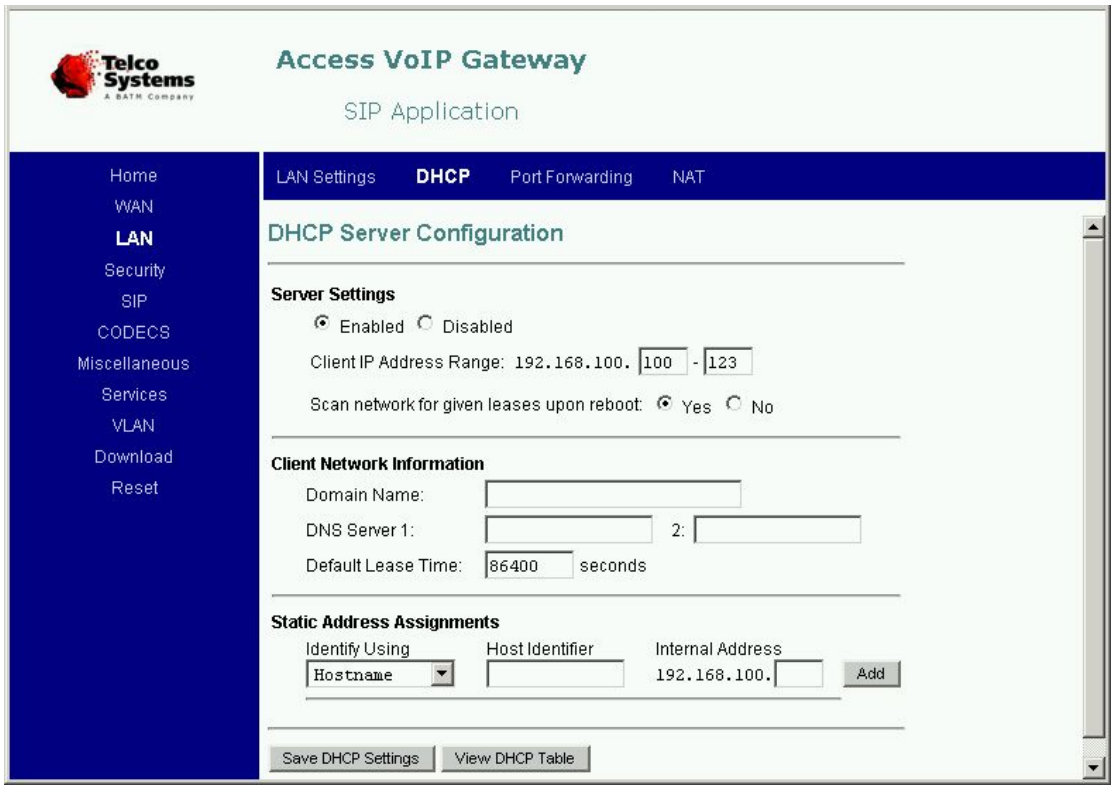


Figure 8-2: DHCP Server Configuration Page

- **DHCP Server Settings**

1. To enable the DHCP Server, select the **Server Settings Enabled** option.

2. Set the DHCP clients IP address range – up to 24 IP addresses are allowed. To change the LAN IP, see Configuring LAN Settings.

3. To enable scanning the LAN for existing DHCP clients on power up, select **Yes** in the **Scan network for given leases upon reboot**.

Client Network Information

- **Domain Name** – optionally enter the domain name for the local LAN.

- **DNS Server 1** and **DNS Server 2** – If the DNS parameters are left blank, the DNS Server IP addresses will be acquired from the WAN. If you want to use additional DNS Server addresses, enter their IP addresses.

- **Default Lease Time** - The duration of the lease for an IP address that is assigned from the DHCP server to a DHCP client. By default, the **Default Lease Time** is set to 86400 seconds (24 hours). The range of possible values is <30-2592000> seconds.

- **DHCP Server Static IP Settings**

  You can define LAN devices statically. The devices can be defined by Host name or by MAC address:

  - **Identity Using** – Select the type of identifier, Host name or MAC, you wish to

use in the next field.

- **Host Identifier** – Enter the appropriate value (Host name or MAC).
- **Internal address** – static IP address of the local host.

Click **Add,** and repeat for additional static IP addresses as required. The configured hosts appear at the bottom of the window and can each be removed by clicking the **Remove** button (Figure 8-3). Up to 8 static hosts can be defined.

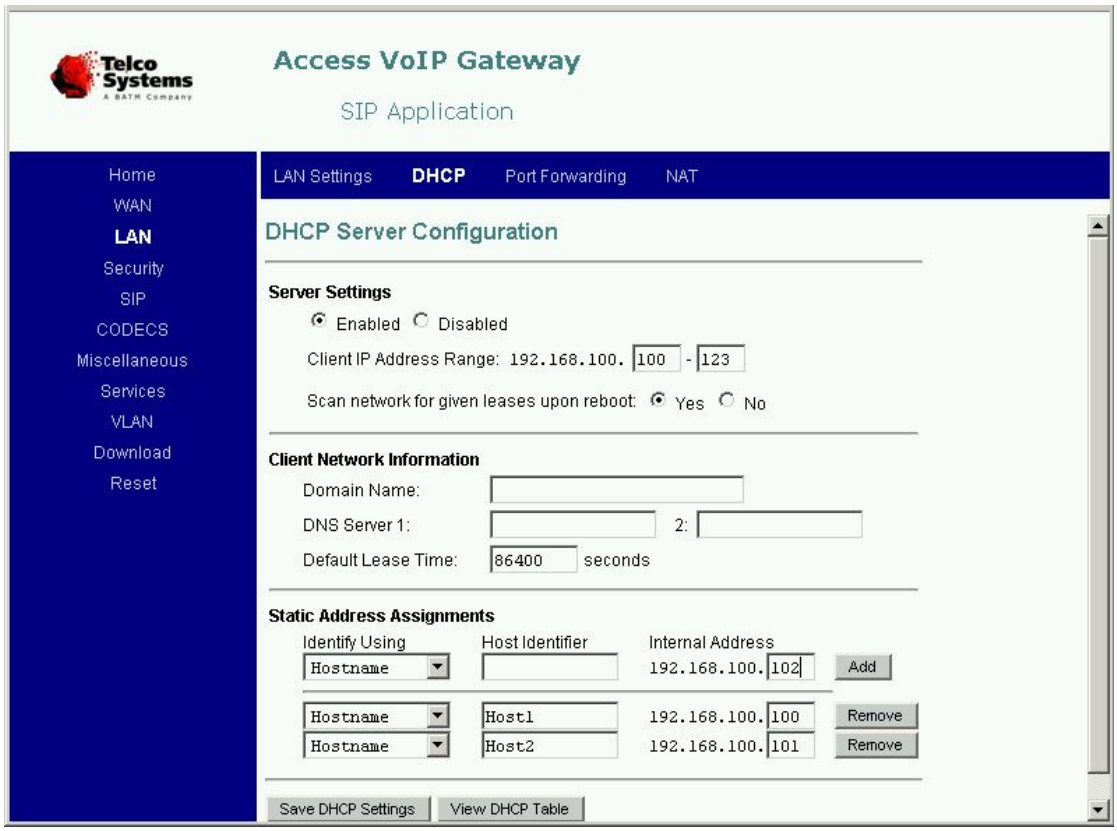


Figure 8-3: DHCP Server Configuration Page Example

- To view the DHCP Client table (Figure 8-4), click on **View DHCP Table**.
- Click **Save DHCP Settings** to save the DHCP server configuration.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

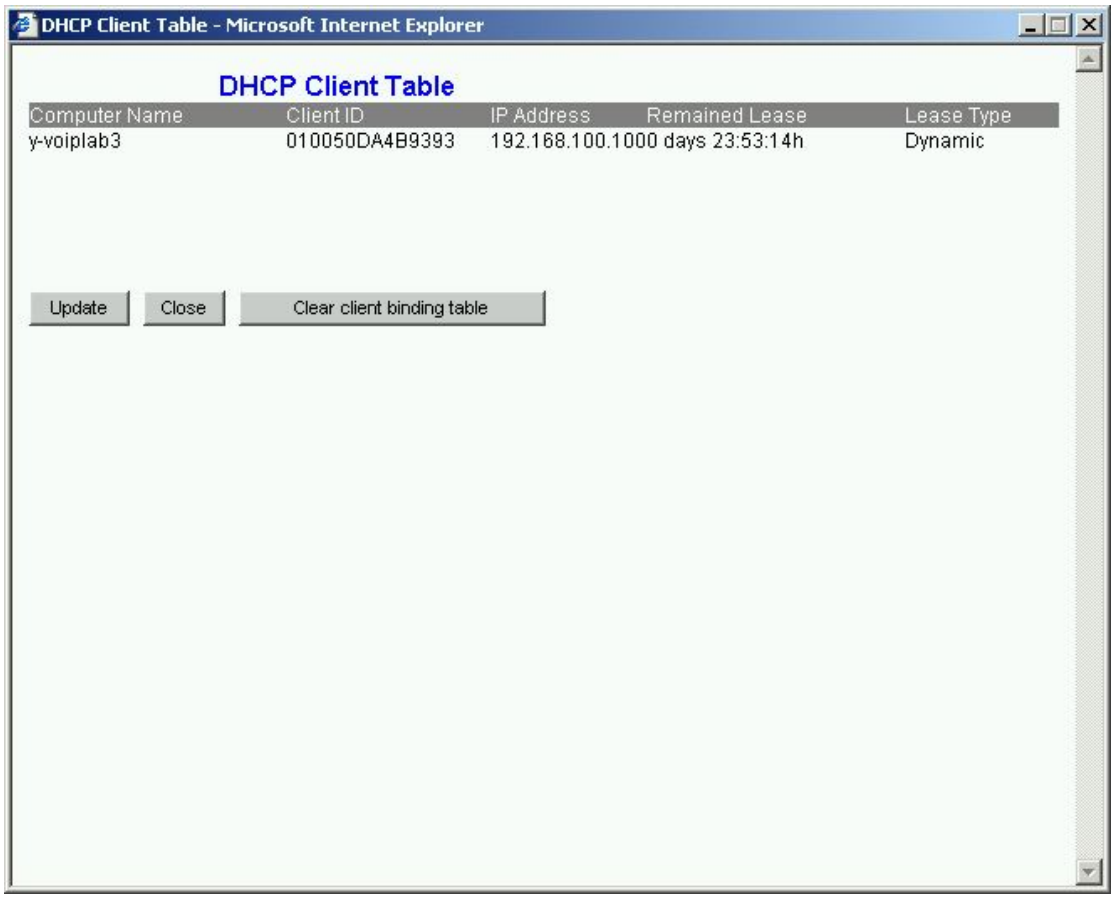


Figure 8-4: DHCP Client Table Page

8.4 Port Forwarding

Port forwarding associates local port ranges to local IP addresses, using NPAT (Network Port Address Translator), in order to enable external network users to access local devices, without the need for the local servers to first access the global network. For more information regarding the NAT protocol see Understanding NAT and NAPT.

To configure port forwarding:

1. In the horizontal menu bar of the **LAN** page, select **Port Forwarding**.
   The **Port Forwarding Configuration** page appears (Figure 8-5).

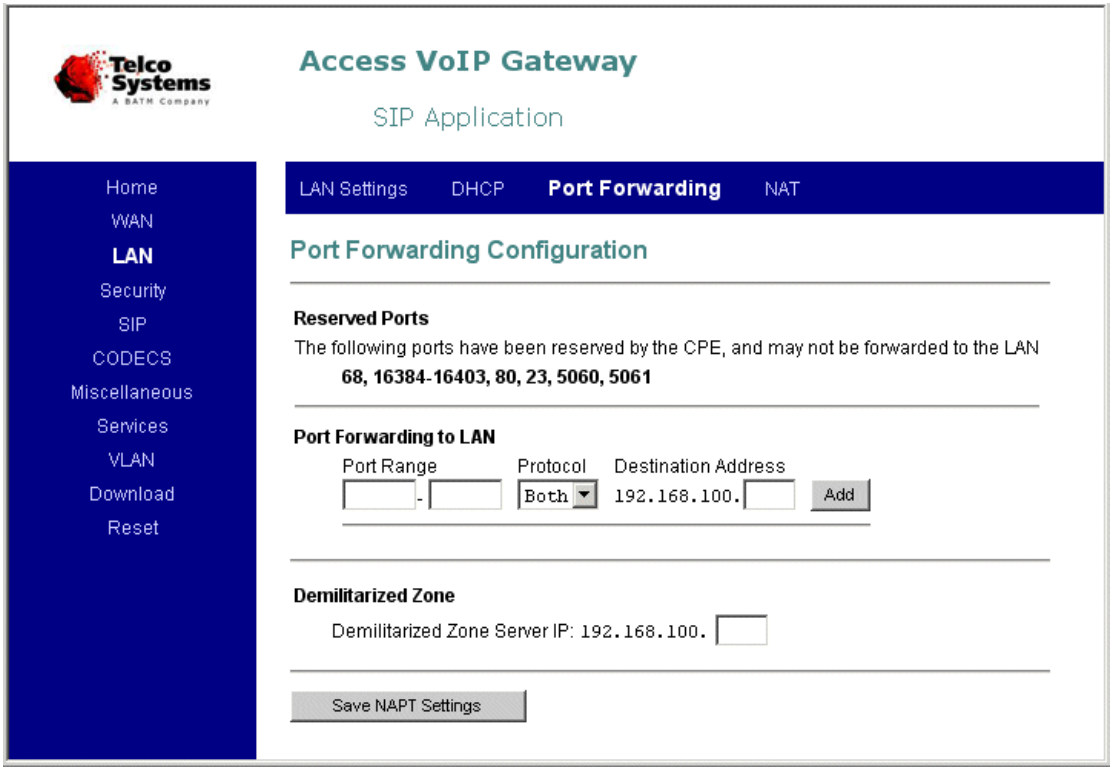


Figure 8-5: Port Forwarding Configuration Page

2. Enter an allowed *port range* (in range <0-65535>, do not use any of the port numbers that are specified in the **Reserved Ports** list).

   - Specify the *transport protocols* to forward for port range.
   - Specify the *low byte number* of the destination address in decimal notation (in the range <1-255>).

3. Click on **Add**.

4. Repeat for additional port forwarding associations as required. The configured associations appear at the bottom of the window and can each be removed by clicking the **Remove** button. Up to 8 devices can be defined.

5. Enter the IP address of your Demilitarized Zone (DMZ) device. (All WAN traffic with unknown TCP/UDP ports will be forwarded to this device.)

6. Click **Save NAPT Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

8.5 IPSec NAT Traverse

The IPSec NAT Traverse feature supports IPSec VPN passing through NAT. Users with NAT-T (UDP tunnel for VPN traffic) should not enable this feature. By default, the option is disabled.

To configure IPSec NAT Traverse:

1. In the horizontal menu bar of the **LAN** page, select **NAT**.
   The **NAT IPSec traverse configuration** page appears (Figure 8-6).

Figure 8-6: NAT IPSec Traverse Configuration Page

2. Check in the **Enable NAT IPSec traverse** dialog box.
3. Click **Save Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

9 Security Configuration via Web

In today's networks security is very important for protecting the Gateway and your local network from hackers. The Getaway's Web management interface offers the following security features:

- Password – enables preventing unauthorized access to the Gateway's configuration.
- Advanced security – enables specify a list of IP addresses that are allowed to manage the Gateway (up to eight IP addresses). You can set management permissions to subnets rather than set them for single stations, by specifying a subnet mask for each IP address.
- DHCP security – enables to receive an IP address and other configuration parameters from a DHCP server that is listed in the IP address list (up to eight IP addresses).
- Access – enables blocking Gateway management via HTTP and/or Telnet on the LAN/WAN interfaces.
- Encryption Key – enables installing an Encryption Key to encrypt the configuration file.
- EncGeneral – enables setting a "General" configuration file encryption key.

9.1 Default Security Configuration

Table 9-1: Default Security Configuration

Parameter	Default Value
Password	None
Advanced security	Disabled
DHCP security	Disabled
HTTP access on the LAN interface	Enabled
HTTP access on the WAN interface	Enabled
Telnet access on the LAN interface	Enabled
Telnet access on the WAN interface	Enabled

9.2 Setting the Password

You can use a security password to prevent access to the configuration of the Gateway by unauthorized users via the Console or the Web Configuration pages.

To set a password:

1. In the vertical menu bar of the current Gateway Web page, select **Security**. The **Set Security Password** page appears (Figure 9-1).

Figure 9-1: Set Security Password Page

2. Enter the *new password* and confirm it.

3. Click on **Save Password** to effect the change.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

9.3 Configuring Advanced and DHCP Security

To configure Advanced Security:

1. In the horizontal menu bar of the **Security** page, select **Advanced Security**. The **Advanced Security Configuration** page appears (Figure 9-2).

Figure 9-2: Advanced Security Configuration Page

Table 9-2 lists the options and entries in the advanced security configuration page:

Table 9-2: The Available Advanced Security Configuration Fields

Field Name	Description
Advanced Security Enable	Select this option to enable Advanced Security.
DHCP Security enable	Select this option to enable the Gateway, when in DHCP mode, to receive an IP address and other configuration parameters from a DHCP server only if it is listed in the IP address list.
IP Address	Optionally, list the IP addresses of stations that are permitted to manage the Gateway. Up to eight IP addresses can be set.
Subnet mask	Extends the Gateway's management permissions to up to eight IP subnets.

NOTE **To permit management of the Gateway only to specified stations or specified subnets, you must enter the IP address with or without subnet masks for each station or subnet allowed.**

If no stations are specified, all stations are permitted to manage the Gateway.

2. After selecting the desired options and entering the desired values, click on **Save Settings** to effect the configuration.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

9.4 Enabling/disabling Configuration via Telnet or HTTP

To enable/disable Telnet and HTTP per LAN/WAN port:

1. In the horizontal menu bar of the **Security** page, select **Access**. The **Service Access Configuration** page appears (Figure 9-3).

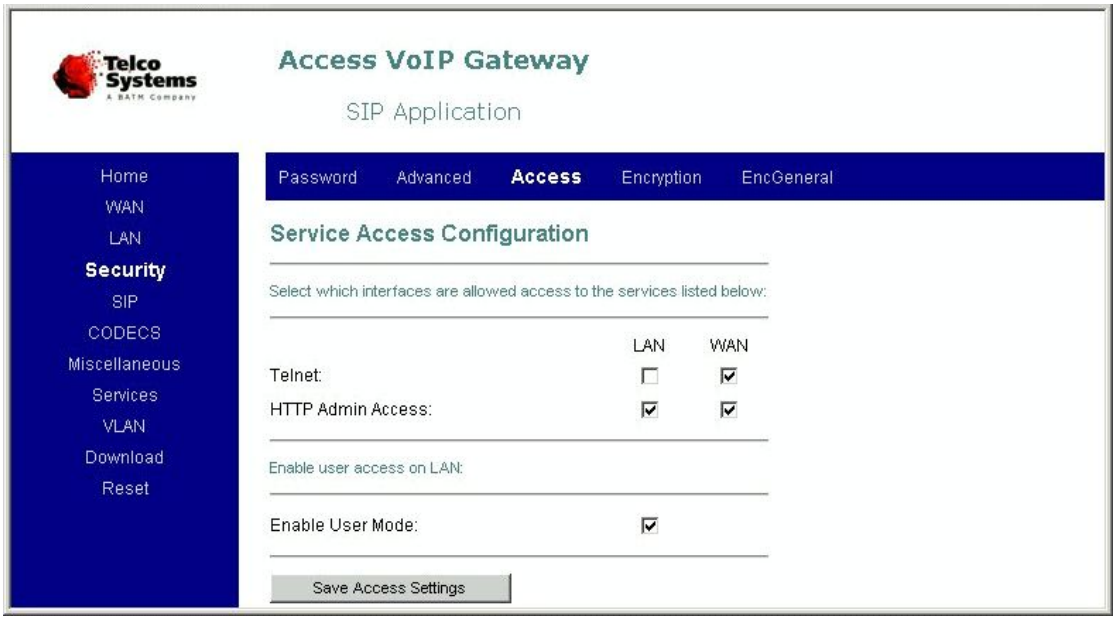


Figure 9-3: Service Access Configuration Page

2. If required, select or clear the **Telnet** and/or **HTTP** check box.

3. If required, enable the User Mode by selecting the **Enable User Mode** check box. In this mode two users are defined – Admin and User. Once User Mode is enabled and Admin password is defined the Admin will have full access and the User will have limited access to the Web screens.

   In addition, in this mode Telnet access is via Admin password only. When the User Mode is enabled, User Web access is always enabled on the LAN and disabled on the WAN. On the **Service Access Configuration** screen the **HTTP** parameter can disable Admin access for the WAN and/or for the LAN. By default, User Mode is disabled and Admin access is enabled on the WAN and LAN

4. Click on **Save Service Access Settings** to effect the change.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

WARNING **Do not disable all managing interfaces, to avoid losing management control over the unit.**

9.5 Setting the "Root" File Encryption Key

In order to use encryption with the "Root" configuration file (see Creating and Encrypting Configuration Files), the user needs to define an encryption key. By default the field is empty and configuration files are assumed to be not encrypted.

To install a new encryption key:

1. In the horizontal menu bar of the **Security** page, select **Encryption**. The **Set Encryption Key** page appears (Figure 9-4).

Figure 9-4: Set Encryption Key Page

2. Enter and confirm the new key in the appropriate fields.

3. Click on **Save Key** to effect the change.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

9.6 Setting the "General" Configuration File Encryption Key

In order to use encryption with the general configuration file, the user must define an encryption key of up to 64 characters (see Creating and Encrypting Configuration Files). By default the field is empty and configuration files are assumed to be not encrypted.

To install a new general configuration file encryption key:

1. In the horizontal menu bar of the **Security** page, select **EncGeneral**. The **Set General Configuration File Encryption Key** page appears (Figure 9-5).

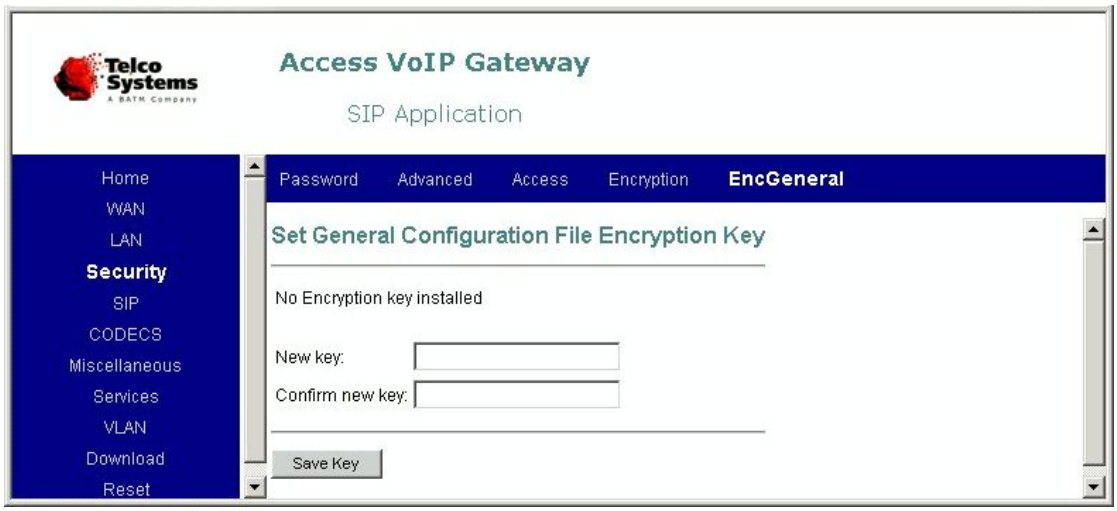


Figure 9-5: Set General Configuration File Encryption Key Page

2. Enter and confirm the new key in the appropriate fields.

3. Click on **Save Key** to effect the change.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

10 Miscellaneous Configuration via Web

In the **Miscellaneous** Web configuration page you can set the following:

- The NTP (Network Time Protocol) IP address for obtaining the correct time.
- The local time zone, relative to GMT.
- Automatically adjust the internal clock to daylight saving time according to the local time zone.
- Local country caller ID.
- Syslog server IP address and the log messages severity level.
- Assign server ports for the various types of servers.
- Assign advanced calling features.
- Configure Ring Tone names and cadences.
- Configure Wait Tones.
- Configure Call Progress Tones (for both FXS and FXO calls).

10.1 Default Miscellaneous Configuration

Table 10-1: Default Miscellaneous Configuration

Parameter	Default Value
Time Zone	GMT – 08:00 Pacific Time
Adjust clock for daylight savings	Disabled
Country CID	United States
Ring Format	Trapezoid 20 Hz Balanced
HTTP Server Port	80
Telnet Server Port	23
Syslog Client Port	514
TFTP client port	69

Parameter	Default Value
HTTP client port	80
Call Waiting	Enabled (configurable only in SIP)
Caller ID display	Enabled (configurable only in SIP)
3-way calling	Enabled (configurable only in SIP)
Last call redial	Enabled (available only in SIP)
Distinctive ring tones	Enabled (available only in SIP)
Call transfer	Enabled (configurable only in SIP)
Do Not Disturb (DND)	Enabled (available only in SIP)
Call forwarding	Enabled (configurable only in SIP)
Block/accept last call	Enabled (available only in SIP)
Auto redial	Enabled (available only in SIP)
Block caller ID	Enabled (available only in SIP)
Anonymous Call Rejection	Enabled (available only in SIP)
Show Caller Identity on Call Waiting	Enabled (configurable only in SIP)
Auto redial Expire Timer value	1800 seconds
Conditional forward key pattern	*1 (available only in SIP)
Unconditional forward key pattern	*2 (configurable only SIP)
Disable forward key pattern	*3 (configurable only SIP)
Enable DND key pattern	*4 (available only in SIP)
Disable DND key pattern	*5 (available only in SIP)
Blind Transfer key pattern	*98 (available only in SIP)
Redial last call key pattern	*69 (available only in SIP)
Block last call key pattern	*60 (available only in SIP)
Accept last call key pattern	*80 (available only in SIP)
Auto redial	*66 (available only in SIP)
Disable auto redial	*86 (available only in SIP)

Parameter	Default Value
Block Caller ID per call	*70(available only in SIP)
Enable Anonymous Call Rejection (ACR)	*77(available only in SIP)
Disable Anonymous Call Rejection (ACR)	*87(available only in SIP)
Dead-air period configuration	0 seconds
Ring Cadences	See The Default Ring Cadences with Associated Names table (available only in SIP)
Call Waiting Tone Cadences	All default values for the Ring Cadences and their Ring Names are based on the 5 Bellcore GR-506-CORE ring patterns.
Call Progress Tones	For both FXS and FXO. See the Call Progress Tones Descriptions table.

Table 10-2: The Default Ring Cadences with Associated Names

Ring Number	Ring Cadence	Alert-Info Ring Name
1	ON 2000 ms OFF 4000 ms	Bellcore-dr1
2	ON 800 ms OFF 400 ms ON 800 ms OFF 4000 ms	Bellcore-dr2
3	ON 400 ms OFF 200 ms ON 400 ms OFF 200 ms ON 800 ms OFF 4000 ms	Bellcore-dr3
4	ON 300 ms OFF 200 ms ON 1000 ms OFF 200 ms ON 300 ms OFF 4000 ms	Bellcore-dr4

Ring Number	Ring Cadence	Alert-Info Ring Name
5	ON 500 ms OFF 20 ms	Bellcore-dr5
6	ON 2000 ms OFF 4000 ms	Bellcore-dr6
7	ON 2000 ms OFF 4000 ms	Bellcore-dr7
8	ON 2000 ms OFF 4000 ms	Bellcore-dr8

10.2 Clock Localization

To configure the clock to local time:

1. In the vertical menu bar of the current Gateway Web page, select **Miscellaneous**. The **Clock** page appears.

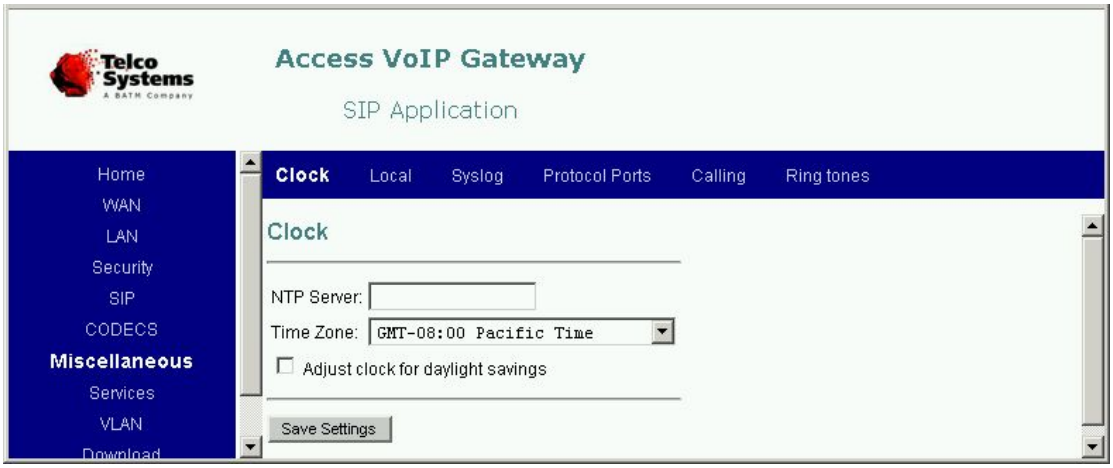


Figure 10-1 Clock Localization Page

Table 10-3 lists the options and entries in the clock localization page.

Table 10-3: The Available Clock Localization Configuration Fields

Field Name	Description
NTP Server	The IP address of the NTP server. For more information regarding the NTP protocol, see Understanding NTP.
Time Zone	Local time zone, relative to GMT. The default is 480 minutes.
Adjust clock for daylight savings	Automatically adjusts the internal clock to daylight saving time according to the local time zone. For more information regarding the NTP protocol, see Daylight Saving Time

	(Summer Time).

2. Click **Save Settings** to save the configuration changes.

NOTE **After entering and saving all configurations, you MUST RESET the Gateway.**

10.3 Local Settings

Local settings include the local country and the ring format (Trapezoidal 20 Hz Balanced or Sinusoidal 25 Hz Unbalanced). Note that the trapezoidal signal may not activate ringing on some phones.

To select the Country for local Caller ID support:

1. In the vertical menu bar of the current Gateway Web page, select **Miscellaneous**.
2. In the horizontal menu bar, select **Local**. The **Local settings** page appears (Caller ID Configuration Page).
3. Select the *local country* in the drop-down list-box.
4. Select either **Trapezoid 20 Hz Balanced** (the default) or **Sinusoid 25 Hz Unbalanced**.
5. Click **Save Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

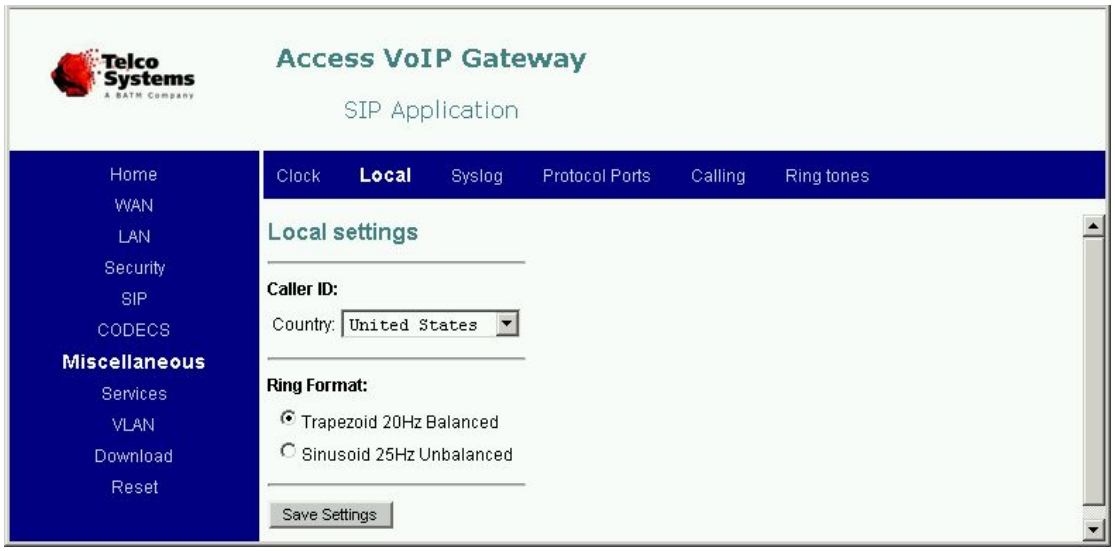


Figure 10-2: Caller ID Configuration Page

10.4 Syslog Server Configuration

For more detailed information on the logging facility, see Understanding Syslog.

To set the Syslog server IP address and the log message severity level:

1. In the vertical menu bar of the current Gateway Web page, select **Miscellaneous**.
2. In the horizontal menu bar, select **Syslog**. The **Syslog Daemon Address Configuration** page appears (Figure 10-3).

Figure 10-3: Syslog Daemon Address Configuration Page

3. Set the IP address of the Syslog server in the **Syslog Server IP Address** field (in the *A.B.C.D* format).

4. Set the log messages severity level in the **Message severity level** drop-down list-box.

   The severity is inversely related to the specified level (0 represents highest severity, 7 represents lowest severity). When you specify a severity level, logging output of the specified level and all lower levels (higher severities) are enabled. The severity levels of the log message types are listed in Table 3-4.

5. Click **Save Settings**.

10.5 Sending Device Information to the Syslog Server

You can upload the system configuration and SIP RTP statistics of active calls from NVRAM to the Syslog server.

To upload the system configuration to the Syslog server:

1. In the lower part of the **Syslog** page (Figure 10-3), in the **Send device information to syslog daemon** field, press the **Upload Config** button.

   The NVRAM entries will be received at the Syslog. The entries will be numbered. The last entry will be marked Total: #*xxx*, where *xxx* is the number of NVRAM entries.

2. If not all entries were received, you can repeat the request starting at any entry, by entering the starting entry number in the **Start Upload Entry** field and pressing the **Upload Config** button again.

To send SIP RTP statistics of active calls to the Syslog server:

1. In the lower part of the **Syslog** page in the **Send device information to syslog daemon** field, select the line number for which you want statistics to be sent (Figure 10-4).

   You can select Line 1, Line 2 or both ("all").

2. Press on **Send Line info**.

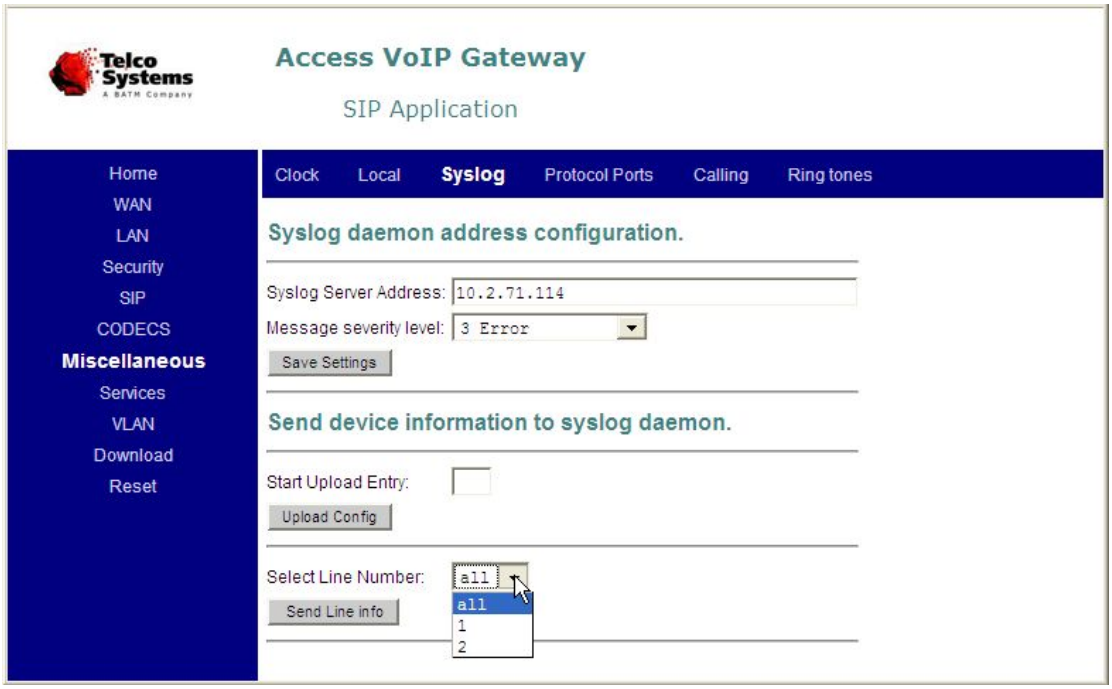


Figure 10-4: Selecting the Line Number in the Syslog Web Page

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

10.6 Port Protocol Configuration

The user can configure the TCP\UDP ports used by the management protocols for the Web HTTP Server, Telnet Server, Syslog Client and HTTP/TFTP client. Following is an example demonstrating the configuration of the TCP port used by the Web management.

Default TCP port 80 is used by HTTP for Web management. If an HTTP server using TCP port 80 is placed in the LAN, users will need to change the management TCP port. To enable access to the LAN server from the WAN, the user will also need to setup a port forwarding entry on port 80 in the Web **Port-Forwarding** screen.

To change the protocols' ports:

1. In the vertical menu bar of the current Gateway Web page, select **Miscellaneous**.
2. In the horizontal menu bar, select **Protocol Ports**. The **Ports configuration** page appears (Figure 10-5).

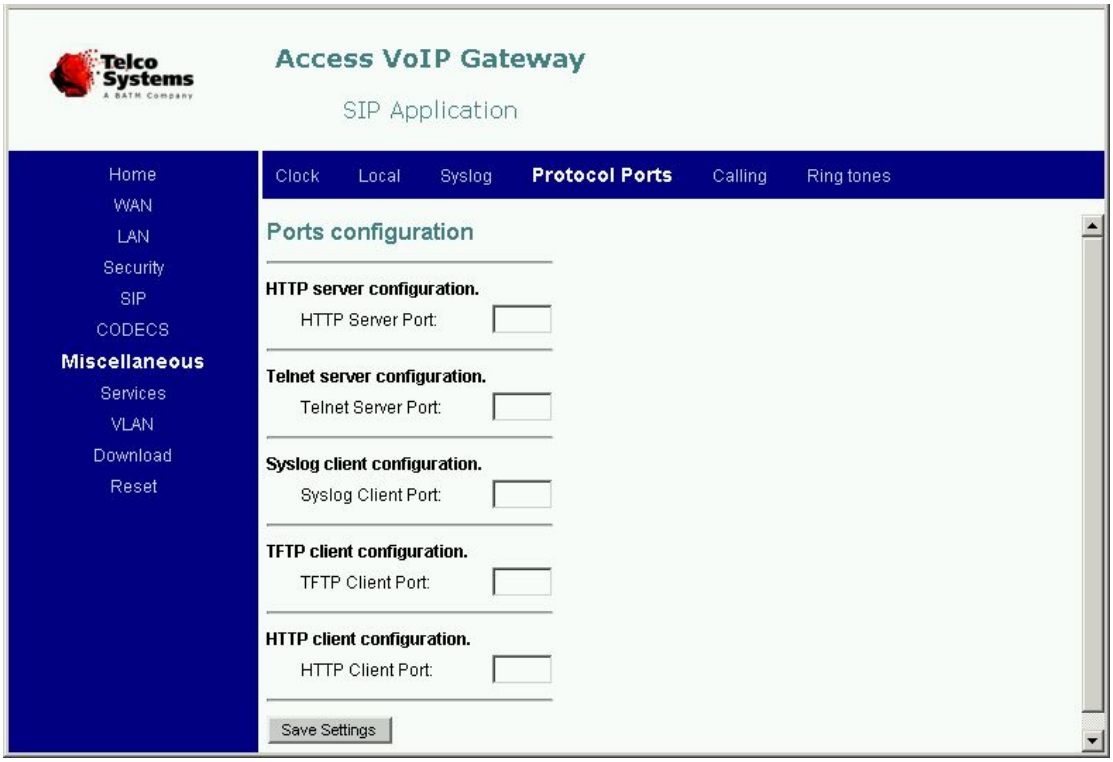


Figure 10-5: The Port Protocol Configuration Page

3. Set the HTTP server port in the range <1-65535> in the **HTTP Server Port** field.
4. Set the Telnet server port in the range <1-65535> in the **Telnet Server Port** field.
5. Set the Syslog client port in the range <1-65535> in the **Syslog Client Port** field.
6. Set the TFTP client port in the range <1-65535> in the **TFTP Client Port** field.
7. Set the HTTP client port in the range <1-65535> in the **HTTP Client Port** field.
8. Click **Save Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

10.7 SIP Advanced Calling Features and Key Sequence Configuration

In SIP, all Advanced Calling features can be either enabled or disabled. By default, all Advanced Calling features are enabled. The assigned key sequences for using the Asterisk (*) calling features can be configured also from the Miscellaneous-Calling web screen.

To set the Advanced Calling Features and Key Sequence Configuration:

1. In the vertical menu bar of the current Gateway Web page, select **Miscellaneous**.
2. In the horizontal menu bar, select **Calling**. The top part of the **Advanced Calling Features** page appears (Figure 10-6).
3. Table 10-4 lists the available fields for Enabling/Disabling Advanced Calling features.

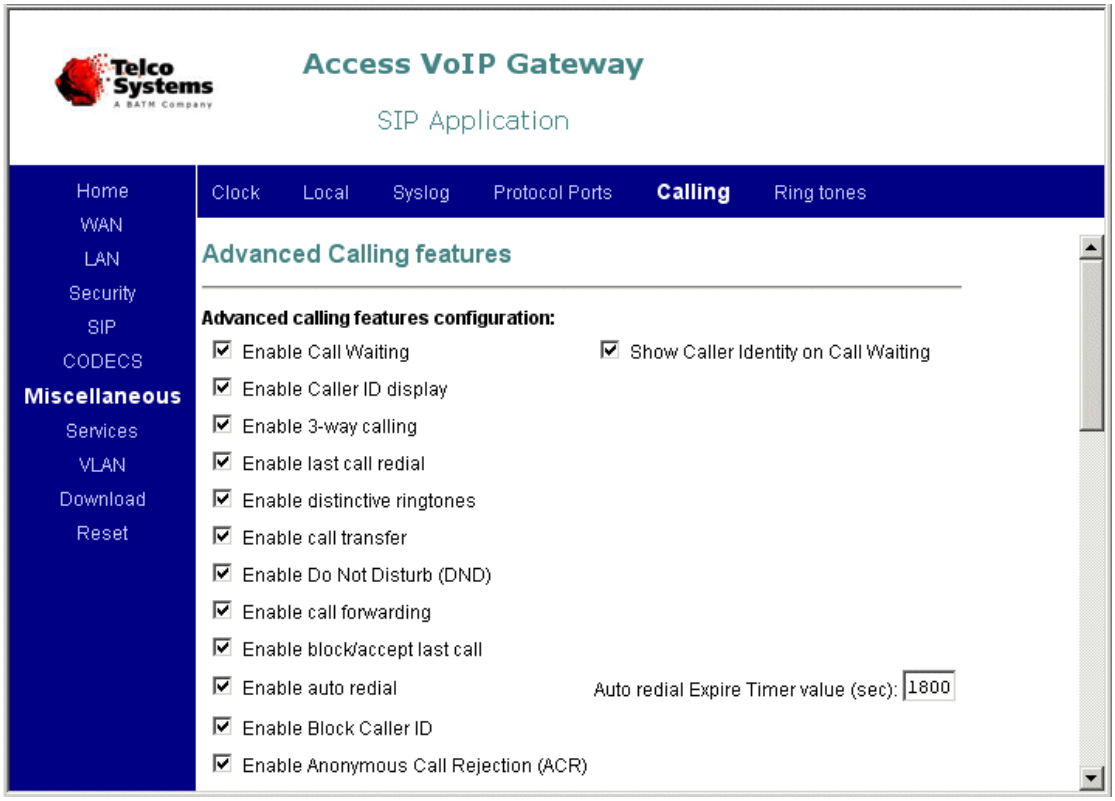


Figure 10-6: The Advanced Calling Features Page

Table 10-4: The Available Advanced Calling Features Configuration Fields

Field Name	Description
Enable Call Waiting	Enables / Disables Call Waiting feature. See Call Waiting for usage.
Enable Caller ID display	Enables /Disables the feature to view the CID of received Calls.

Field Name	Description
Enable 3-way calling	Enables /Disables Conference Call feature. See Conference Call for usage.
Enable last call redial	Enables /Disables Redialing Last Call feature. See Redialing of Last Received Call for usage.
Enable distinctive ringtones	Enables / Disables Distinctive Ringtones feature. See Ring Tones Configuration.
Enable call transfer	Enables / Disables Blind Transfer Call. See Blind Transfer Call).
Enable Do Not Disturb (DND)	Enables / Disables DND feature. See Do Not Disturb (DND) for usage.
Enable call forwarding	Enables / Disables Call Forwarding feature. See Forward a call and Conditional Call Forwarding for usage.
Enable block/accept last call	Enables / Disables Block/Accept Last Call feature. See Block Last Received Call for usage.
Enable auto redial	Enables / Disables Auto Redial. See Auto Redial for usage
Enable Block Call ID	Enables / Disables per-call to block sending Caller ID. See Block Sending CID per Call for usage.
Enable Anonymous Call Rejection (ACR)	Enables / Disables to reject calls from an anonymous source. See Anonymous Caller Rejection (ACR) for usage.
Show Caller identity on Call Waiting	Enables seeing the name of the Caller on the call waiting.
Auto redial Expire Timer value	The time period in seconds for dialing a busy number. The default is 1800 seconds.

4. After making your Advanced Calling Feature selections, scroll down to the **Handset Advanced Configuration** part (Figure 10-7) for setting the key-sequences used to Activate / Deactivate Advanced Calling features. Table 10-5 lists the available fields in this part of the page.

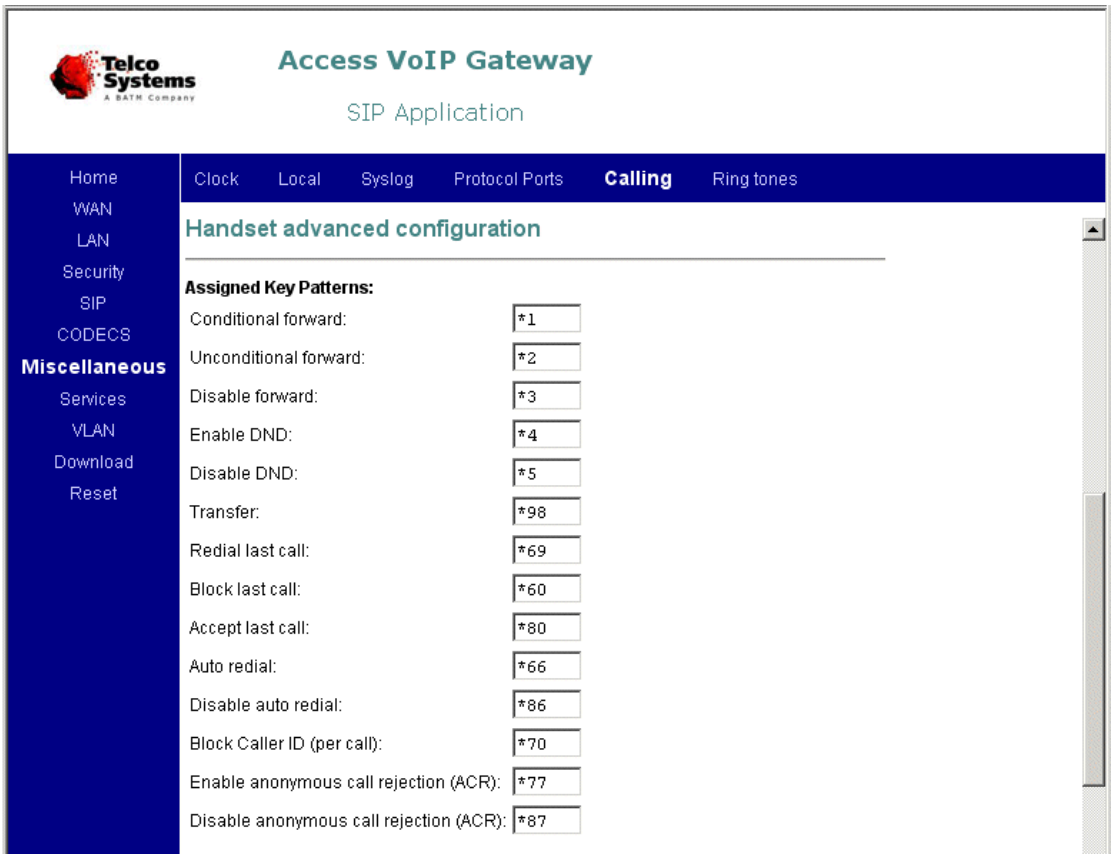


Figure 10-7: The Assigned Key Sequences Fields

Table 10-5: The Available Key Sequences Fields

Field Name	Description
Conditional forward	Activate Conditional call forward key sequence. See Conditional Call Forwarding for usage. Default key sequence is *1.
Unconditional forward	Activate Unconditional call forward key sequence. See Conditional Call Forwarding for usage. Default key sequence is *2.
Disable forward	Deactivate Call forward key sequence. . Default key sequence is *3
Enable DND	Activate DND key sequence. See Do Not Disturb (DND) for usage. Default key sequence is *4
Disable DND	Deactivate DND key sequence. See Do Not Disturb (DND). Default key sequence is *5.
Transfer	Activate Blind Transfer Call key sequence. See Blind Transfer Call for usage. Default key sequence is *98
Redial last call	Redial last received caller key sequence. See Redialing of Last Received Call for usage. Default key sequence is *69

Field Name	Description
Block last call	Block last received caller key sequence. See Block Last Received Call for usage. Default key sequence is *60
Accept last call	Re-accept last blocked number key sequence. See Block Last Received Call for usage. Default key sequence is *80
Auto redial	Activate Auto Redial by hanging up key sequence. See Auto Redial for usage. Default key sequence is *66
Disable auto redial	To cancel the periodic Auto Redialing before the timeout has been reached key sequence. See Auto Redial for usage. Default key sequence is *86
Block Caller ID (per call)	Disables your caller ID from appearing on the callee's phone screen key sequence. See Block Sending CID per Call for usage Default key sequence is *70.
Enable Anonymous Call Rejection (ACR)	Reject all calls from an anonymous caller's key sequence. The default keypad value to activate rejecting anonymous calls is *77.
Disable Anonymous Call Rejection (ACR)	Cancels ACR key sequence. The default keypad value to re-accept anonymous calls is *78.

6. After making your Handset Advanced selections, scroll down to the **Dead-air Configuration** part (Figure 10-8) for setting the dead-air period in seconds if required.

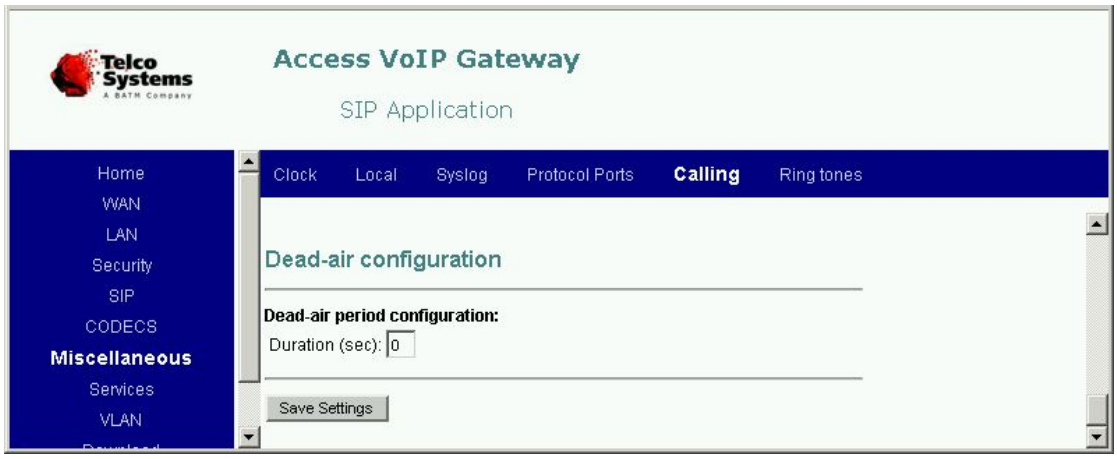


Figure 10-8: Dead-air Period Configuration Field

Table 10-6: Dead-Air Period

Field Name	Description
Dead-Air period	The Dead-Air period is a period of silence at the end of a call, prior to the busy tone. This period is needed by some Voice Mails to identify the end of the call. By default the value is zero and there is no Dead-Air period.

7. If required, set the Dead-air period.

8. Complete your desired settings and click **Save Settings**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

10.8 Ring Tones Configuration

Ring Tones Configuration is used to identify the caller based on a distinct ring. Ring Names are used for Distinctive Rings and Call Waiting tones. The names are sent in the Alert-Info header of the INVITE message to indicate the ring that should be played.

The SIP Alert-Info Header

The feature is dependent on the remote caller or the SIP server for including the Alert-Info header with the appropriate Ring Name in the INVITE message for the Distinctive Ring or Call Waiting Tone.

10.8.1 Ring Names and Cadences

Eight Ring Names associated with eight Ring Cadences (patterns) used by both telephone lines can be configured for the Distinctive Rings. Six Ring Cadences (with the same Ring Names as for the Distinctive Rings) are used for the Call Waiting Tones. The default values for the Ring Cadences and their Ring Names are based on the 5 Bellcore GR-506-CORE ring patterns. If the Ring Name in **Alert-Info header** is not recognized or is not supplied, the standard Bellcore Ring pattern 1 is used and cannot be changed to another pattern. The default Alert-Info Ring names can be configured to different names but the default names will also be recognized.

Table 10-2 lists the default Ring Names and associated Cadences. Eight defaults are used by the Distinctive Rings and six defaults are used by the Call Waiting Tones. The default values are used when the tables are left blank.

To set the Ring Tones:

1. In the vertical menu bar of the current Gateway Web page, select **Miscellaneous**.
2. In the horizontal menu bar, select **Ring Tones**. The **Ringing Configuration** page, comprising four sets of fields, appears.
3. Set the SIP Alert-Info header ring names to be recognized in the fields **Ring Name 1** to **Ring Name 8**.
4. Click **Save Ring Names**

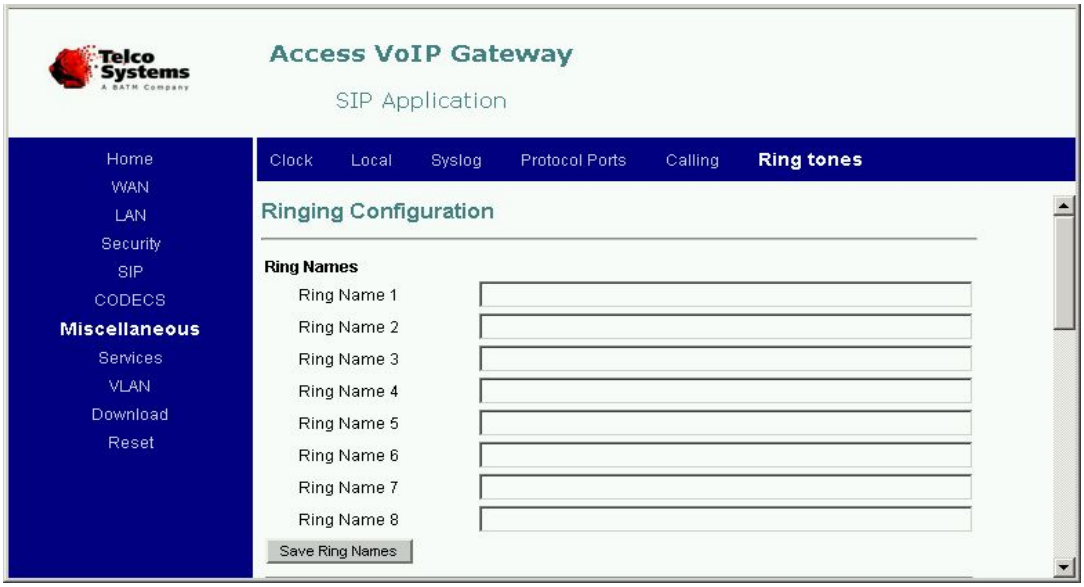


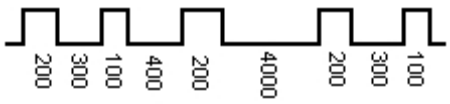
Figure 10-9: The Ring Name Fields in the Ringing Configuration Page

4. Scroll down to Ring Cadences. Set the Distinctive Ring cadences in the fields **Ring Cadence 1** to **Ring Cadence 8**.

   Distinctive Rings Cadences (patterns) are associated with the Ring Names. The Distinctive Rings Cadence parameter can be: **ON**, **OFF**, **IDLE**, **R**-repeat, time in milliseconds.

   Example:

   RING_2=ON(200),OFF(300),ON(100),OFF(400),ON(200),IDLE(4000),R

   Click **Save Ring Cadences**.

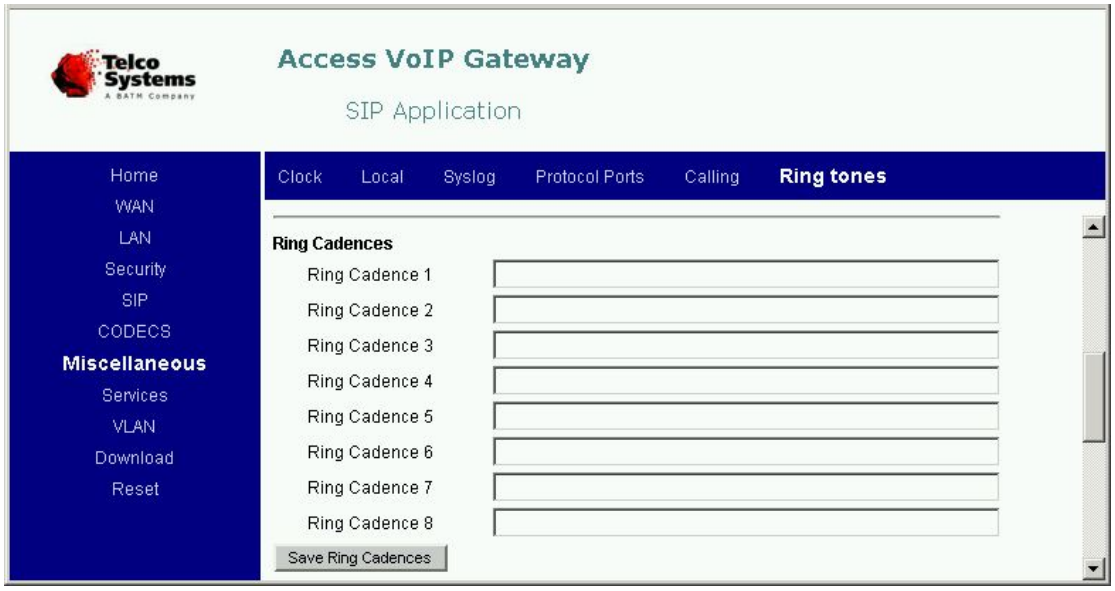


Figure 10-10: The Ring Cadence Fields in the Ringing Configuration Page

10.8.2 Call Waiting Tone Cadence Patterns

The **Call Waiting Tone Cadences** are tone patterns associated with the above Ring Names.The Call Waiting Tone Cadences table includes six entries. The five entries after the first entry are used when the remote caller or SIP server include the **Alert-Info** header with an appropriate Ring Name for the required Distinctive Call Waiting tone. If the Ring Name is not recognized or not supplied, a default tone is used. The first entry is used to configure the default Call Waiting tone.

1. Set the Call Waiting Ring Tones in the **CWTCadence 1** to **CWTCadence 6** fields.

   See CWT Detailed Configuration Description below.

2. Click **Save Call Waiting Tone Cadences**.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

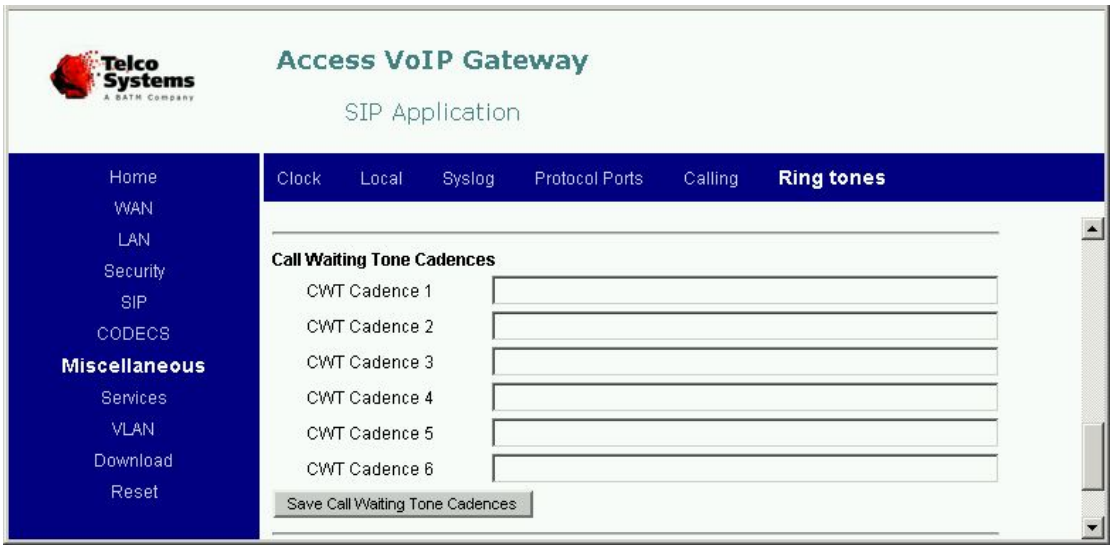


Figure 10-11: The Call Waiting Tone Cadence Fields in the Ringing Configuration Page

The default Call Waiting tone is heard 5 times and has the Format:

440@-13#[on(300),IDLE(3700)]5

To change the tone to be heard 4 times use the format:

440@-13#[on(300),IDLE(3700)]4

Following is a detailed description for configuring the **Call Waiting Tone Cadences table.**

10.8.2.1 CWT Detailed Configuration Description

An entry in the table must have the following form: **Frequency@Power#Cadence**

Frequency – Frequency of the tone in Hz;

Power- Power of the tone in dBm, i.e. it is relative to 1mW and may take negative values meaning that the power of the tone volume is less than 1mW;

You can also use:

Frequency@Power+ Frequency@Power+ … which means that a compound tone, comprising of different harmonic signals (with different frequencies and levels) is used.

Cadence – Ring pattern

Cadence includes Sequences.

Sequence: **ON(**Timeval**)** or **ON(**Timeval**), OFF(**Timeval**),** …,

where *Timeval* is the duration in milliseconds that the tone is active (ON) or non-active (OFF).

Example: ON(100), OFF(200), ON(300)

A Sequence can be repeated a number of times: **[***sequence***]***number*,

where *number* is the number of times the sequence is repeated

Example: [ON(100), OFF(200), ON(300), OFF(400)]3

A Sequence can be inactive for a specified time period or it can be repeated indefinitely:

[Sequence**]**number**,R** or **[**Sequence**]**number**,IDLE(**Timeval**),R**

R - means the given Sequence is repeated indefinitely.

IDLE(*Timeval***) -** means the Sequence is inactive for *Timeval* milliseconds.

Example: [ON(100), OFF(200), ON(300), OFF(400)]3, IDLE(2000),R

Examples:

Example 1 - European dial tone

425@-5#ON(1000),R

The tone is frequency 425Hz at level -5dbm and is repeated indefinitely.

Example 2

1800@100#[ON(500),OFF(100),ON(100)]4,ON(100),OFF(100),IDLE(2000),R

The Sequence ON, OFF, ON is repeated 4 times. After that the Sequence ON(100), OFF(100) and then Idle for 2 seconds is repeated indefinitely.

10.8.3 Call Progress Tones

Call Progress Tones are audible signals that are used to inform the caller or callee of the progress of a call (e.g. ring tone, busy tone, etc.).

By default the **Call Progress Tones** parameters are null. The system uses the default Bellcore definitions. The progress tones can be reconfigured in order to adapt to local country tones.

1. Fill in the Call Progress Tones fields if you want to change their defaults. The following tones are available: **Dial Tone, Busy Tone, Reorder Tone, Off Hook Warning, Ringback Tone, Confirm Tone, Stutter Tone (MWI), Ring, FXO Dial Tone, FXO Busy Tone**.

   Refer to Call Progress Tones Descriptions table for tone definitions.

2. Click **Save Call Progress Tones**.

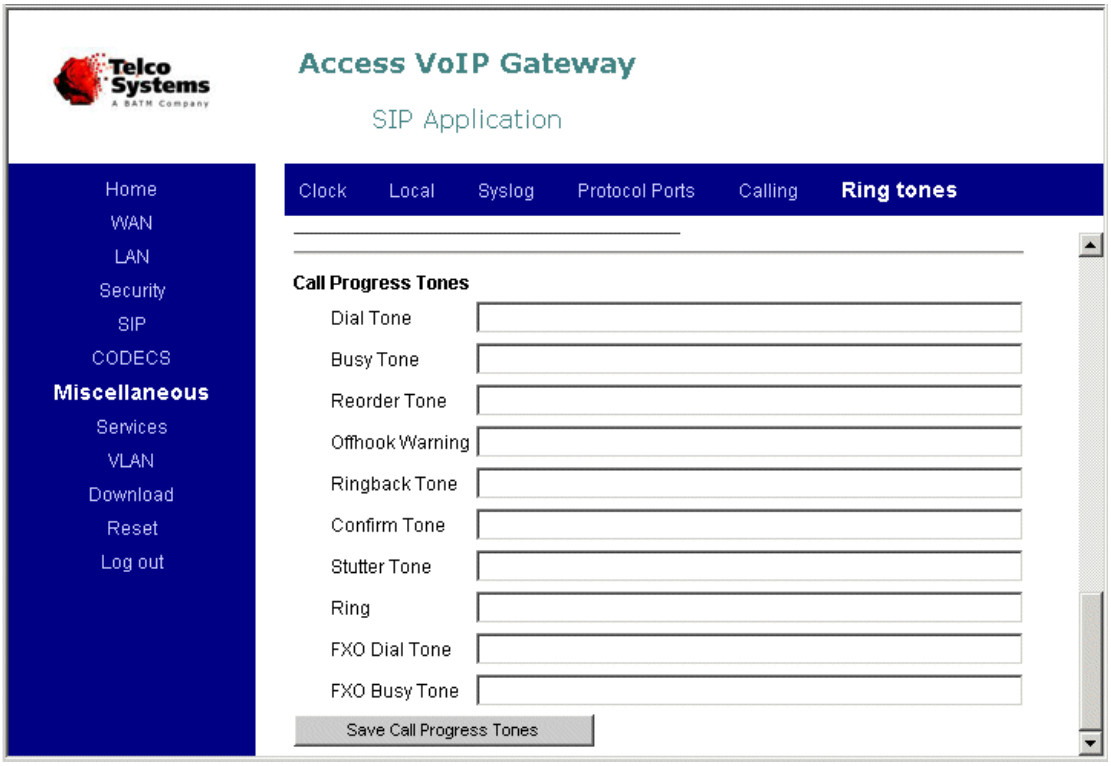


Figure 10-12: The Call Progress Tones Fields in the Ringing Configuration Page

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Table 10-7: Call Progress Tones Descriptions

Field Name	Description and Default Configuration
Dial Tone	The FXS Dial Tone indicates that the network is ready to accept a phone number. Default: **350@-12+440@-12#ON(100),R**
Busy Tone	This tone is played in the headset when the destination number is engaged or when a call is ended. Default: **480@-12+620@-12#ON(500),OFF(500),R**
Reorder Tone	The Reorder Tone, also known as, Network Busy or Fast busy and sounds like a fast busy signal, is played in the headset if a call can not be completed due to a network error other than destination busy (line is engaged). Default: **480@-12+620@-12#ON(250),OFF(250),R**
Off Hook Warning	Warning tones are heard when the receiver is left off hook. When the receiver is picked up a dial tone is heard for the first 10 seconds. After 10 seconds a Busy tone is heard for 20 seconds, and then followed by a Receiver off-hook (ROH) warning tone for another

Field Name	Description and Default Configuration
	60 seconds. To change the periods or to disable the feature consult the Auto Configuration manual. The default ROH tone used is: **1400@-6+2060@-6+2450@-6+2600@-6#[ON(100),OFF(100)]200**
Ringback Tone	Indicates that the destination number is being alerted (called). Default: **440@-12+480@-12#ON(2000),OFF(4000),R**
Confirm Tone	Indicates that the network has processed a request received by the caller, e.g. activation/deactivation of call forwarding. Default: **350@-12+440@-12#ON(100),OFF(100),R**
Stutter Tone (MWI)	Indicates that there is a message waiting. Default: **440@-13#[on(300),IDLE(3700)]5**
Ring	Indicates to the callee that his number is being called. This tone is audible by the callee Default: **ON(2000),OFF(4000),ON(2000),R**
FXO Dial Tone	(Supported by **Access 241-FXO only**.) After the caller dials a PSTN number, the gateway "listens" for a valid FXO Dial Tone in order to route the call to the PSTN. If a valid Dial Tone is not detected the Reorder Tone (Fast Busy) will be heard in the headset indicating that the call can not be executed. Default: **350@-12+440@-12#ON(100),R**
FXO Busy Tone	(Supported by **Access 241-FXO only**.) Indicates the termination of the PSTN phone call. By default the USA Bellcore Busy Tone is detected. Default: **480@-12+6200@-12#ON(500),OFF(500),R**

11 Voice and Management Services Configuration via Web

For setting VLANs dedicated for the voice and management traffic open the **Voice & Management Services Configuration** screen (Figure 11-1). The user can assign VLAN and priority tags to outgoing packets. This will help devices such as switches and routers in the LAN to serve the VoIP packets with higher priority queues and with lower delays. Service VLANs can be defined also for security reasons.

The following Services can be set with a VLAN and priority:

- Management packets, including Ping and Voice.
- RTP (Real-time Transport Protocol) frames, you can also assign a priority using the ToS (Type of Service) field in the IP header of the RTP.

  The RTP is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services. Originally specified in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1889, RTP was designed by the IETF's Audio-Video Transport Working Group to support video conferences with multiple, geographically dispersed participants. RTP is commonly used in Internet telephony applications. RTP does not in itself guarantee real-time delivery of multimedia data (since this is dependent on network characteristics); it does, however, provide the wherewithal to manage the data as it arrives to best effect.
- Server registration and start packets of the VoIP call session.

11.1 Default Voice and Management Services Configuration

Table 11-1: Default Voice and Management Services Configuration

Parameter	Default Value
TOS for RTP packets	160

11.2 Configuring Voice and Management Services

To configure the Voice and Service management:

1. In the vertical menu bar of the current Gateway Web page, select **Services**. The **Voice & Management Services Configuration** page appears (Figure 11-1).

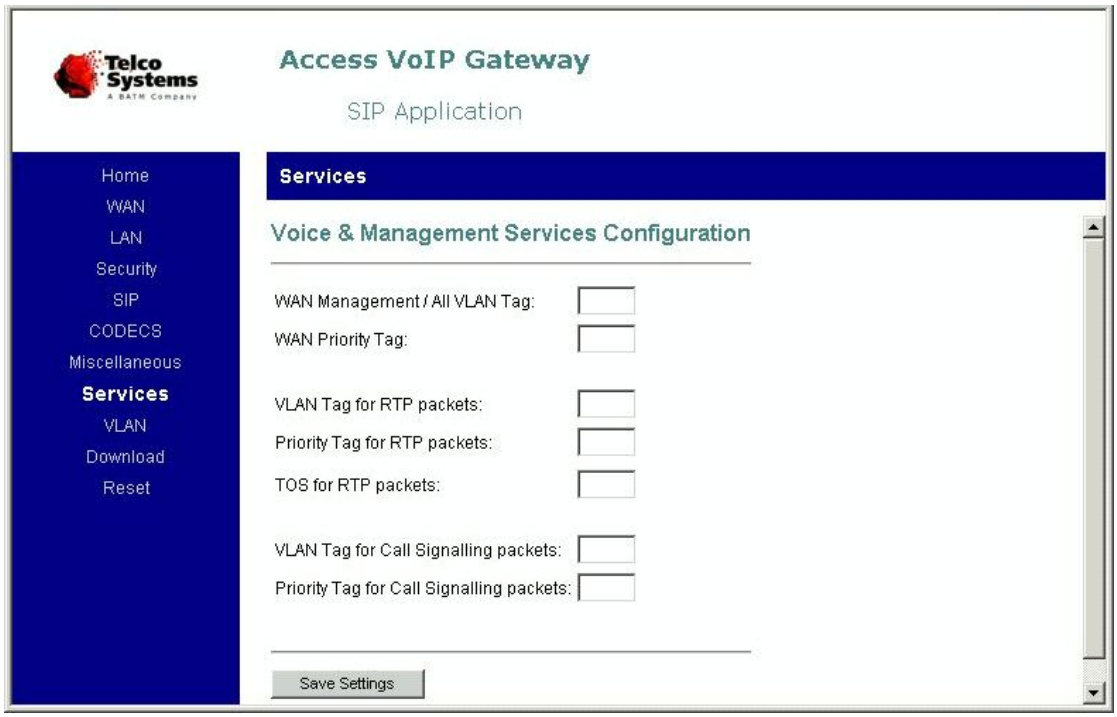


Figure 11-1: Voice and Management Services Configuration Page

Table 11-2 lists the available fields in this window:

NOTE VLAN tags are simply VLAN IDs. Priority tags are simply priority values.

Table 11-2: The Available Voice and Management Services Configuration Fields

Field Name	Description
WAN Management / All VLAN Tag	To assign a unique VLAN tag to all management including ping and voice, enter a VLAN value in the range <1 – 4095>.
WAN Priority Tag	To assign a priority tag to all management including ping and voice, enter a value in the range 0 (lowest priority) to 7 (highest priority).
VLAN Tag for RTP packets	To assign a unique VLAN tag to the outgoing RTP (Real-time Transport Protocol) frames, enter a VLAN value in the range <1 – 4095>. Overrides the **VLAN Tag** field.
Priority Tag for RTP	To assign a priority tag to the outgoing RTP (Real-time

Field Name	Description
packets	Transport Protocol) frames, enter a value in the range 0 (lowest priority) to 7 (highest priority). Overrides the **Priority Tag** field.
TOS for RTP packets	To assign a priority using the TOS (Type of Service) field in the IP header of the RTP frames, Insert a TOS value in the range 0-255. For example, enter a TOS value of 16 for minimum delay. The default value is 160.
VLAN Tag for Call Signaling packets	To assign a unique VLAN tag to the start frames of the VoIP call session, enter a VLAN value in the range 1 – 4095. Overrides the **VLAN Tag** field.
Priority Tag for Call Signaling packets	To assign a priority tag to the start frames of the VoIP call session, enter a value in the range 0 (lowest priority) to 7 (highest priority). Overrides the **Priority Tag** field.

2. Click **Save Settings** to save the configuration changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

12 Configuring VLANs via Web

NOTE VLANs temporarily cannot be activated in the current version.

VLAN (Virtual Local Area Network) logically group a set of stations to communicate as if they were on the same LAN segment. Traffic between VLANs is restricted. Unicast and broadcast traffic is forwarded only to LAN segments of the same VLAN. The Gateway enables you to configure up to eight 802.1Q-compatible VLANs. A VLAN is identified by a unique number from 1 to 4095 (VLAN ID). By default, the VLAN configuration is disabled and traffic is free to travel between all EdgeGate ports.

VLAN tagging is required to identify traffic from more than one VLAN on the same port. A "tag" is simply the VLAN identification number (VLAN ID), as specified in the 802.1Q standard. The tag is included in the packets forwarded across the LAN. You can allow the Gateway to connect to non 802.1Q-compliant devices by adding/removing the tag from packets according to tag definitions in the VLAN configuration table.

12.1 Default VLAN Configuration

Table 12-1: Default VLAN Configuration

Parameter	Default Value
Using VLANs	Disabled
Default ports' VLAN ID	1, untagged

12.2 Configuring VLAN

To set VLAN configuration on a Gateway:

In the vertical menu bar of the current Gateway Web page, select **VLAN**.
The **VLAN** Configuration page appears (Figure 12-1).

NOTE The WAN port on Access 211, is Port 2.

The WAN port on Access 241, is Port 5.

Figure 12-1: VLAN Configuration Page

Use the TAB key or click to move around the table in the VLAN configuration page. The Gateway is factory set with VLAN ID – 1 assigned by default to all the ports of the unit. Each port must have a default ID. All packets received on the Gateway ports without a VLAN tag will inherit the default VLAN ID of the receiving port as their VLAN ID.

You can use the VLAN configuration page to define new VLANs.

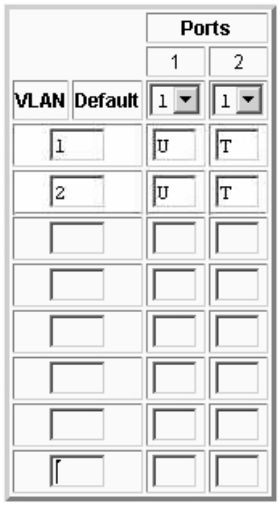
To define a new VLAN, proceed as follows:

1. In the **VLAN** column, enter the new VLAN ID.

2. In the Ports table, in the row corresponding to the new VLAN ID and in the column under the number of each port that is permitted to be a member of the new VLAN:

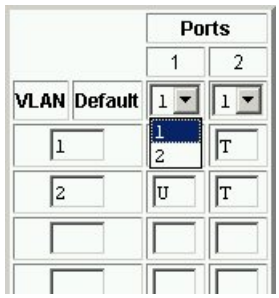
   - Enter **T** if packets of the VLAN are to be transmitted from the port with a VLAN tag in the packet (Tagged).

   - Enter **U** if packets of the VLAN are to be transmitted from the port without a VLAN tag in the packet (Untagged).



3. You can use the **Del** key to remove a port, if it is not a member of the new VLAN.

4. Once the port members of a VLAN have been entered, you can assign the VLAN as the default VLAN for one or more ports that belong to that VLAN. Select the proper VLAN ID on the **Default** VLAN row in all the required ports.



5. If you wish to remove a VLAN from the **VLAN** column, first make sure it is not a default VLAN for any port. If it is, assign another VLAN as default for the port(s) and then delete the original VLAN.

6. Click **Save** to save the VLAN configuration (you will probably need to scroll down to reach the **Save** button).

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Once the VLAN configuration table is set and **VLAN Enable** is selected, packets received at an EdgeGate port will be forwarded only to ports of the same VLAN (ports that have their port member field set to "T" or "U" for that VLAN).

Traffic addressed to the EdgeGate unit (Web management or VoIP protocol frames) will be received and transmitted on any of the defined VLANs.

13 Protocol H.323 Configuration via Web

H.323 is a standard approved by the International Telecommunication Union (ITU) to promote compatibility in videoconference transmissions over IP networks. H.323 was originally promoted as a way to provide consistency in audio, video and data packet transmissions in the event that a Local Area Network (LAN) did not provide Guaranteed Service Quality (QoS).

If the Gateway has H.323 installed you need to configure the Gatekeeper IP address and other H.323 parameters with the Web Configuration. To run the Web Configuration see Configuring the Gateway via the Web.

13.1 Default H.323 Configuration

Table 13-1: Default H.323 Configuration

Parameter	Default Value
Dial plan	>#|[2-9]xxxxxxxx|1[2-9]xxxxxxxxx|x.T
Caller ID	FSK
RRQ for KeepAlive RRQ	Disabled
T38 fax support	Disabled
Send In-band DTMF	Enabled
Send Out-of-band DTMF	Enabled
Audio/CODEC standard	G711 u-law and a-law
Packetization period	30 ms
Silence Suppression	Enabled
Fixed Jitter Buffer	100ms

13.2 Setting the H.323 Configuration

To configure the Gatekeeper IP address and other H.323 parameters:

- In the vertical menu bar of the current Gateway Web page, select **H323**. The **H323 Configuration** page (Figure 13-1) appears.

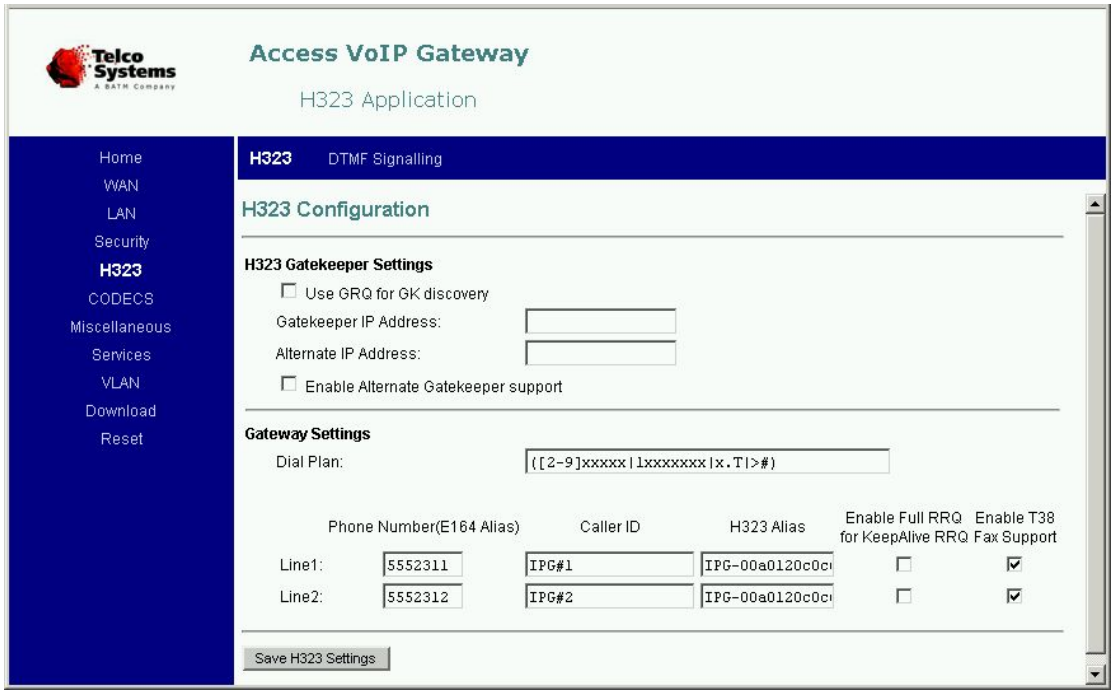


Figure 13-1: H.323 Configuration Page

- **H323 Gatekeeper Settings**
  - Choose whether or not to use GRQ (Gatekeeper Request) for gatekeeper (GK) address.

    The GRQ is a Registration, Admission, and Status (RAS) message sent as a gatekeeper request.
  - Enter the *IP address* of your gatekeeper in the first field and the phone numbers for **Line1** and **Line2** at the bottom of the page. All other fields on this page have default values and need not to be filled in.

    At this point, you can click on **Save H323 Settings** at the bottom of the page and use the default Dial Plan. Alternatively, you may enter a user-defined dial plan in the **Dial Plan** field.
  - Set the *alternate* IP address of H.323 gatekeeper. If you want the *alternate* IP address of H.323 gatekeeper to be used, select the **Enable Alternate Gatekeeper support** check box.
- **Gateway Settings**
  - Setting the Dial Plan

    Use the default dial plan (>#[2-9]xxxxxxxxx|1[2-9]xxxxxxxxx|x.T) or set your own dial plan. For more information regarding the dial plan format see Using the Dial Plan.
  - For each phone *line* set the following:
    - ∇ Set the *phone number* (with E164 alias).

The E164 is the format of global switched telephone numbers are defined by the ITU-T (International Telecommunications Union - Telecommunications Standardization Sector). The 16-digit number is split into international, national and user number portions.

- ∇ Set the *caller ID*.

  Enter the "Name" you want to show on the called party's Caller ID display. When you make a call from a line of the Gateway with the Caller ID inserted, the remote called party will receive this string. Gateway US version is factory set to FSK (Bellcore) CID.

- ∇ Set the *H.323 alias*.

  The H.323 Alias is usually descriptive of the particular client terminal and usually contains alphanumeric characters.

- ∇ Select the **Enable Full RRQ for KeepAlive RRQ** check box to enable the RRQ.

  The RRQ is a RAS (Registration, Admission, and Status protocol) message sent as a registration request.

- ∇ Select the **Enable T38 Fax Support** check box to enable T38 fax support.

  The T38 is a Real time IP Fax Relay protocol.

- Click on the **Save H323 Settings** button to save the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

13.3 DTMF Signaling

Dual Tone Multi-Frequency (DTMF) identifies telephone buttons by a combination of two tones. When you press a button, two standard tones are sent. One tone uniquely indicates the row number and the other tone uniquely indicates the column number of the button that you press.

To configure DTMF Signaling:

In the horizontal menu bar of the H323 Configuration Web page, select **DTMF Signaling**. The **DTMF Configuration** page appears (Figure 13-2).

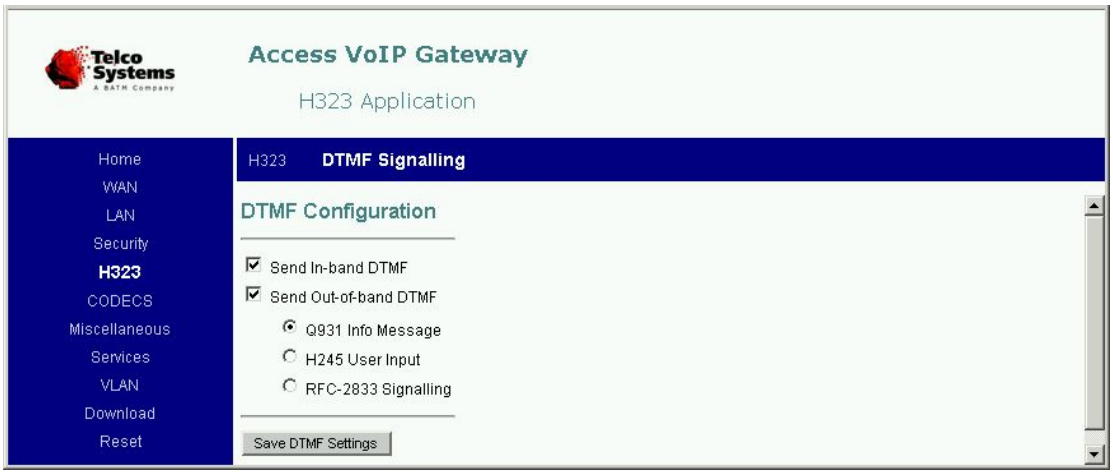


Figure 13-2: DTMF Configuration Page

Table 13-2 lists the available fields in the DTMF configuration page:

Table 13-2: The Available Voice and Management Services Configuration Fields

Field Name	Description
Send In-band DTMF	Supports signaling tones within the audio channel.
Send Out-of-band DTMF	Supports signaling tones outside the audio channel. This requires choosing one of the following options: **Q931 Info Message** The Q.931 protocol contains control information that is exchanged with telephone networks. The information includes digital code for the following messages: ALERTING, CALL PROCEEDING, CONNECT, CONNECT ACKNOWLEDGE, SETUP, SETUP ACKNOWLEDGE, SUSPEND, SUSPEND ACKNOWLEDGE, SUSPEND REJECT, RESUME, RESUME ACKNOWLEDGE, RESUME REJECT, DISCONNECT, RELEASE, RELEASE COMPLETE, STATUS ENQUIRY and STATUS. • **H245 User Input** Enables forwarding H.245 user input indication messages. • **RFC-2833 Signaling** Enables the RFC2833 protocol for transmission of Telephony event packets.

Click **Save DTMF Settings** at the bottom of the Web page to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

13.4 Audio/CODEC Configuration

The Gateway supports G711 u-law and a-law standards by default. The user can set the Gateway to also support one of the three voice coding standards: G723, G726 or G729. Both

ports will be allowed to use the selected option. For every supported voice coding standard the user can enable/disable **Silence Suppression** and, except for G723, select the default **Packetization** period (as a multiple of 10ms in the range 10ms-100ms).

To set Audio/CODEC parameters:

1. In the vertical menu bar of the current Gateway Web page, select **CODECS**. The **Audio/CODEC Configuration** page appears (Figure 13-3).

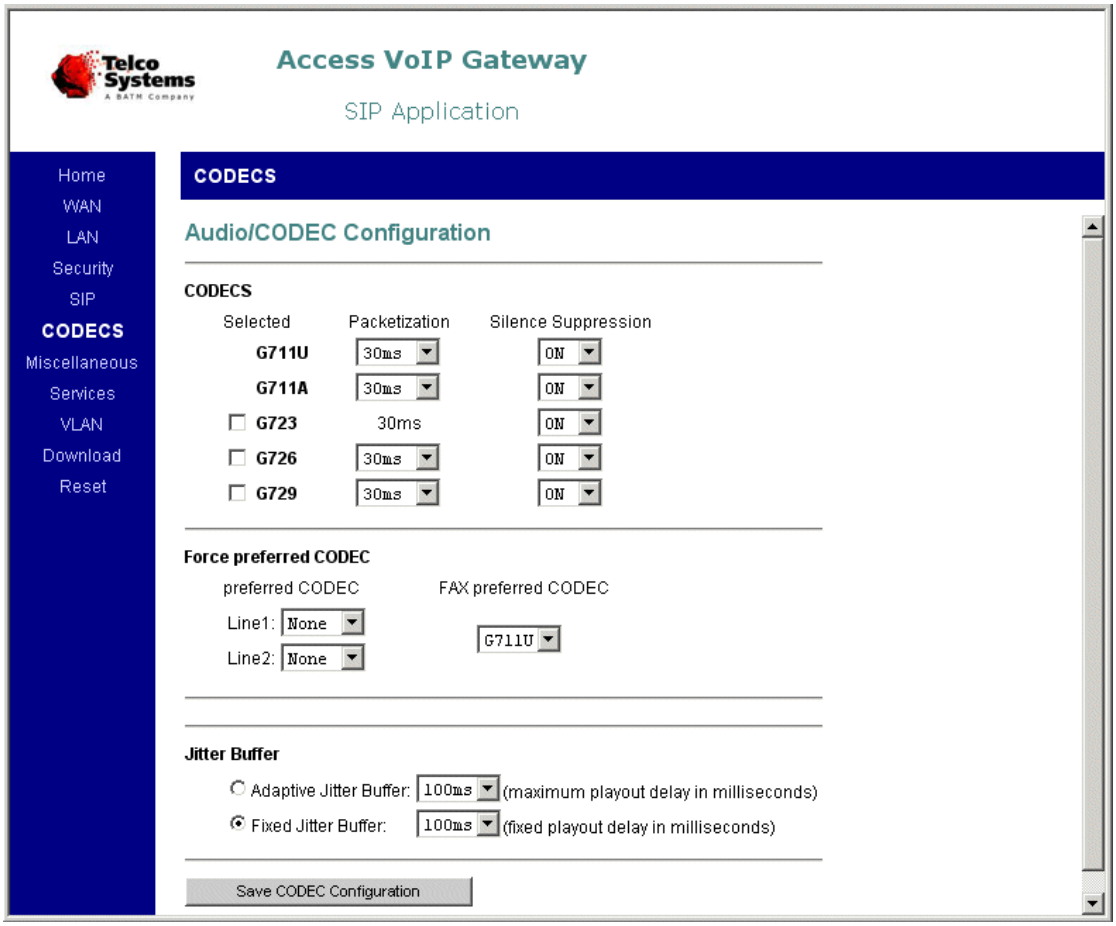


Figure 13-3: Audio/CODEC Configuration Page

2. Select the Audio/CODEC *standard.*

NOTE Only one complex code (G723, G726, G729) can be selected.

3. Set the *Packetization* period.

4. Set the *Silence Suppression*.

5. Select the Preferred Codecs for Line 1, Line 2 and Fax.

5. Select Fixed Jitter Buffer, and set the fixed playout delay in milliseconds.

   You may select Adaptive Jitter Buffer, and set the maximum playout delay in milliseconds.

6. Click **Save CODEC Configuration** at the bottom of the Web page to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

14 Protocol MGCP Configuration via Web

The MGCP (Media Gateway Control Protocols) is designed to control Telephony Gateways from external call control elements called media gateway controllers or call agents. A telephony gateway is a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks

If the Gateway has MGCP installed you need to configure the Call Agent IP address and other MGCP parameters with the Web Configuration. To run the Web Configuration, see Configuring the Gateway via the Web.

14.1 Default MGCP Configuration

Table 14-1: Default MGCP Configuration

Parameter	Default Value
Call Agent Address	Obtained from a DNS server
Call Agent port	2427
Endpoint domain name	Gateway's IP address
Max. delay before RSIP	600 seconds
Max. disconnect delay before RSIP	0, the feature is disabled
Allocated Endpoints	Number of telephone connectors (2)
Support Packet Cable NCS 1.0	Enabled
Support IETF MGCP 1.0 (RFC 2705)	Disabled
Support Message Piggybacking	Enabled
Send Telephone Events via RFC2833 signaling	Disabled
Enable Keypad Events (0-9, *, #)	Disabled
Payload value	96
Suppress voice packets during RFC2833 Telephone Event packet transmission	Disabled
Squelch inband DTMF audio	Disabled
ABCD event signaling mode	Transition

Parameter	Default Value
Audio/CODEC standard	G711 u-law and a-law

14.2 Setting the MGCP Configuration

To configure MGCP parameters:

In the vertical menu bar of the current Gateway Web page, select **MGCP**. The **MGCP Configuration** page (Figure 14-1) appears.

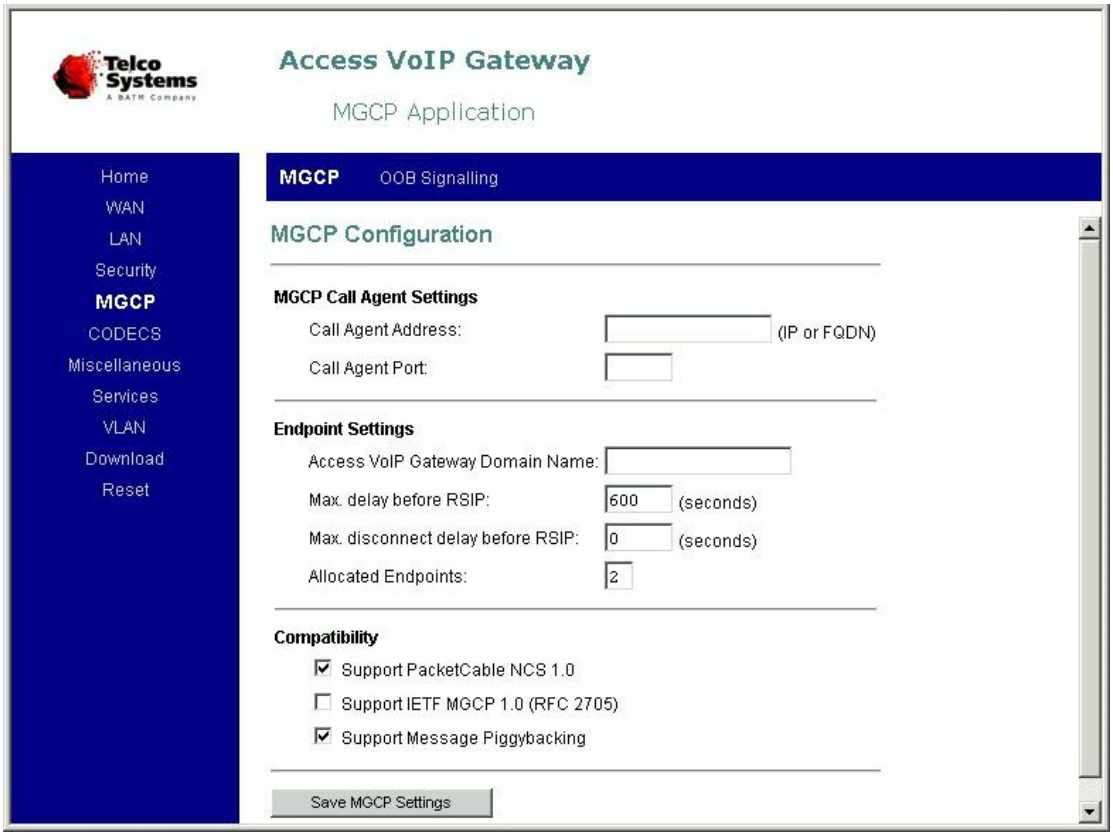


Figure 14-1: MGCP Configuration Page

Table 14-2 lists the available fields in the MGCP configuration page.

Table 14-2: The Available MGCP Configuration Fields

Field Name	Description
Call Agent Address	Fill in the address of the Call Agent in this field Or Leave this field blank if you wish to obtain the Call Agent address from a DNS server. The address of the call agent can be IP address or FQDN address.

Field Name	Description
	FQDN (Fully-Qualified Domain Name) is a portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program that an Internet request is addressed to. The FQDN includes the second-level domain name and any other levels.
Call Agent port	Enter the Call Agent port number in this field Or Leave this field blank if you wish to use the default MGCP Call Agent port 2427.
Access VoIP Gateway Domain Name	Enter the Endpoint Domain name in this field Or Leave this field blank if Gateway's IP address is to be used for the Domain Name.
Max. delay before RSIP	Maximum time in seconds allowed for the Restart In Progress message to be sent to the Call agent. The default value is 600 seconds.
Allocated Endpoints	Number of allocated Endpoints. Number of phone lines permitted to register with Call Agent. Minimum=1. Maximum=Number of telephone connectors.
Max. disconnect delay before RSIP	If this parameter is not zero, MGCP RSIP will be sent when the link on the Uplink port goes up after being down for a period longer than **Max. disconnect delay before RSIP**. By default the parameter is zero and the feature is disabled.
Support Packet Cable NCS 1.0	Enable/disable Packet Cable NCS 1.0 support.
Support IETF MGCP 1.0 (RFC 2705)	Enable/disable MGCP 1.0 support.
Support Message Piggybacking	When this option is enabled, the Gateway is permitted to send Piggyback messages (several MGCP messages sent in one UDP frame) to the Call agent.

Enter your settings and click **Save MGCP Settings** to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

14.3 RTP Telephone Event (RFC2833) Configuration

RFC2833 describes a protocol for sending Telephony events (Receiver ON/OFF Hook, Ring ON/OFF) and DTMF digits in RTP packets. This method is used as an alternative method for

the MGCP protocol signaling frames to solve a variety of signaling delays. The Payload value is Payload Type field of the RTP frame. Payloads 0-95 are well defined and reserved values by IANA. Payloads values of 96-127 are free (dynamic) and are not reserved by the standards.

If the RFC2833 protocol for Telephony events is enabled, voice packets can be suppressed during the transmission of the RFC2833 Telephone Event packets.

To configure RTP Telephone Event (RFC2833) parameters:

In the horizontal menu bar of the MGCP Configuration page, select **OOB Signaling**. The **RTP Telephone Event (RFC2833) Configuration** page (Figure 14-2) appears.

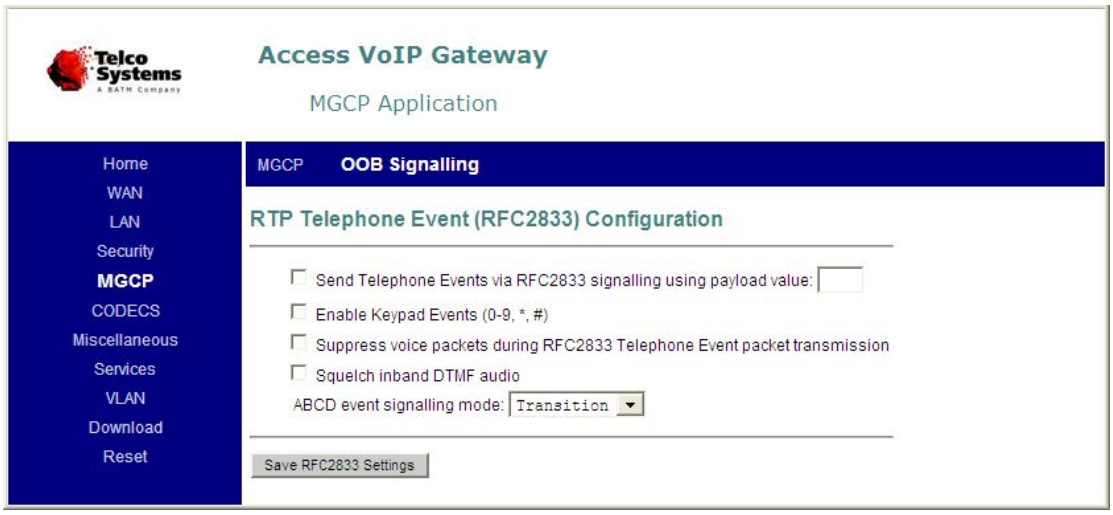


Figure 14-2: RTP Telephone Event (RFC2833) Configuration Page

Table 14-3 lists the available fields in **the RTP Telephone Event (RFC2833) Configuration** page.

Table 14-3: The Available RTP Telephone Event (RFC2833) Configuration Fields

Field Name	Description
Send Telephone Events via RFC2833 signaling using payload value	When enabled, the Gateway will send RFC2833 frames for the Telephony events (see also **Enable Keypad Events)**. Consult your Call server documentation to know if this RFC2833 option is supported and what Payload value is required. The default payload value is 96.
Enable Keypad Events (0-9, *, #)	This option enables sending the DTMF digits 0-9,*,#. By default, DTMF sending is disabled.
Suppress voice packets during RFC2833 Telephone Event packet transmission	Enabling this option preserves the original voice bandwidth and prevents the need for more bandwidth for the RFC2833 packets. Consult your Call server documentation for the preferred mode of operation.
Squelch inband DTMF audio	When selected inband DTMF audio is not transmitted

Field Name	Description
	in the audio stream.
ABCD event signaling mode	Two possible modes for RFC2833 Telephony events signaling (ABCD signaling packets) are available: • **Transition** mode: In this mode, the event packet is sent only at the moment of the event. • **Continuous** mode: In this mode, the event packet is sent continuously at the rate of the voice, as long as the event exists. The Continuous mode behaves better in situations of packet loss, preventing cases such as stuck ringers. Consult your Call server documentation for the preferred mode of operation.

Enter your settings and click **Save RFC2833 Settings** to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

14.4 Audio/CODEC Configuration

The Gateway supports G711 u-law and a-law standards by default. The user can set the Gateway to also support one of the three voice coding standards: G723, G726 or G729.

To set Audio/CODEC parameters:

1. In the vertical menu bar of the current Gateway Web page, select **CODECS**. The **Audio/CODEC Configuration** page appears (Figure 14-3).

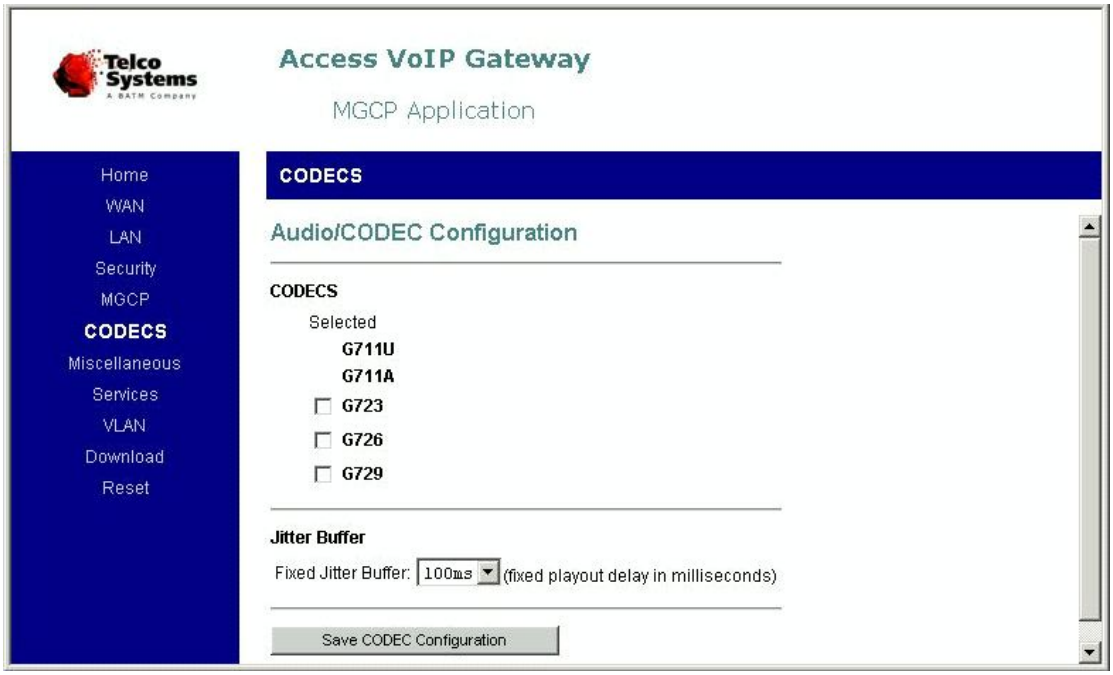


Figure 14-3: Audio/CODEC Configuration Page

2. Select the Audio/CODEC *standard.*

3. Set the *Fixed Jitter Buffer,* which is the fixed playout delay in milliseconds.

4. Click **Save CODEC Configuration** at the bottom of the Web page to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

15 Protocol SIP Configuration via Web

The SIP (Session Initiation Protocol) is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality.

If the Gateway has SIP (Session Initiation Protocol) installed you must configure the SIP Server IP address and other SIP parameters with the Web Configuration. To run the Web Configuration, see Configuring the Gateway via the Web.

NOTE **This chapter includes configuration instructions for SIP parameters supported by all Access gateways, as well as, PSTN parameters supported by the Access 241-FXO alone.**

15.1 Default SIP Configuration

Table 15-1: Default SIP Configuration

Parameter	Default Value
SIP server IP address	Empty
SIP server port number	5060
Domain Name	10.2.80.206 (This field must be filled in.)
FXS Dial plan	>#|[2-9]xxxxxxxxx|1[2-9]xxxxxxxxx|x.T
FXO Dial plan (For **Access 241-FXO** only.)	Null
RTP/RTPC NAT port base	16384
INVITE Expires Timer value	Disabled
SIP Session Timer value	Disabled
Support PRACK method with provisional response reliability	Disabled
SIP Registration Timer Value	1800 seconds
Send RTP on 183 Session Progress	Disabled
Send Telephone Events via RFC2833 signaling using payload value	96

Parameter	Default Value
Suppress voice packets during RFC2833 Telephone Event packet transmission	Disabled
Call Forward	Disabled
Audio/CODEC standard	G711 u-law and a-law
SIP call control transport protocol	UDP
Jitter Buffer	100 ms

15.2 SIP Server Configuration

To configure the SIP Protocol parameters:

In the vertical menu bar of the current Gateway Web page, select **SIP**.
The **SIP Configuration** page (Figure 15-1) appears. You may need to scroll down in order to display the fields at the bottom of this page (Figure 15-2).

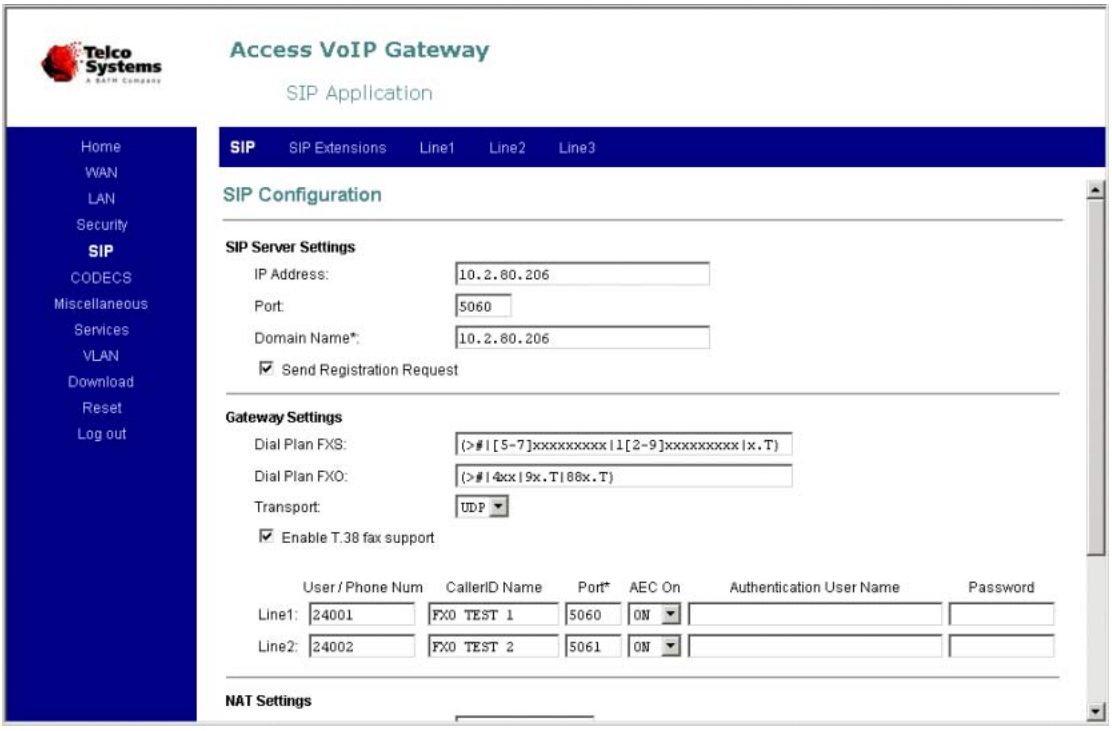


Figure 15-1: SIP Configuration Page (SIP Server and Gateway Settings)

15.2.1 SIP Server Settings

- SIP server **IP address** or Domain Name.

  If this field is set to a Domain name and the SIP Server port is empty, the SIP server information will be obtained by a **DNS SRV query**. If the DNS SRV query fails the DNS A queries and the default SIP port 5060 will be used.

If this field is set to a Domain name and the SIP Server port is not empty DNS A queries with Server port will be used.

If the field is set to the Server's IP and Server port is configured, Server's IP and configured port will be used. If the port is not configured the default port 5060 will be used.

- Set SIP server **Port** number (5060 by default).
- SIP Server's **Domain Name**, which is used in registration. For more information regarding the DNS (Domain Name Server) of the SIP server, see DNS Resolver.

  For example: LINExNUMBER@DOMAINNAME
- Select the **Send Registration Request** check box if you want the Gateway to send REGISTER request.

15.2.1.1 DNS SRV Support for SIP

SRV (abbreviated from SERVICE) is the Gateway's request from the DNS server to receive the IP addresses of servers that distribute some kind of service. The type of DNS queries used depends on the way the SIP Server IP and port are configured. The following describes the possible options:

- A Domain name is set for the SIP Server's IP address.
  - ∇ If the Port is set, the Access Gateway will use DNS A type queries.
  - ∇ If the Port is not set, the Access Gateway will use DNS SRV queries. If the query is unsuccessful, DNS A type queries will be performed and the default SIP port 5060 is used.
- An IP address is set for the SIP Server's IP.
  - ∇ If the port is set the configured Server IP address and the configured port are used.
  - ∇ If the port is not set the Configured IP address and the default SIP port 5060 are used.

15.2.2 Gateway Settings

- Setting the **FXS Dial Plan**

  Use the default FXS Dial Plan (>#|[2-9]xxxxxxxx|1[2-9]xxxxxxxx|x.T) or set your own dial plan in the **Dial Plan** field. For more information regarding the dial plan format refer to Using the Dial Plan for SIP, H.323 and PSTN.
- Setting the **FXO Dial Plan (for AC-241-FXO only)**

  The default FXO Dial Plan is Null. Set your own dial plan in the FXO **Dial Plan** field. For more information regarding the dial plan format refer to Using the Dial Plan for SIP, H.323 and PSTN.

NOTE **For AC-241-FXO - it is up to the user to configure the two Dial plans correctly so that a match for a dialed number occurs only in one of the Dial plans and not in both.**

The FXO Dial Plan enables the gateway to ascertain whether the outgoing call should be routed to the FXO port (PSTN) or to the FXS port (VoIP). The FXO Dial plan implements the same dialing rules as the FXS Dial plan.

Upon making an outgoing call, the gateway compares between the dialed number and the FXO Dial Plan. If they do not match then it compares the dialed number to the FXS Dial Plan.

- Set the SIP call control **Transport** protocol.
- For each phone *line* set the following:
  - ∇ Set the *phone number* (E164 number).

    The E164 is the format of global switched telephone numbers are defined by the ITU-T (International Telecommunications Union - Telecommunications Standardization Sector). The 16-digit number is split into international, national and user number portions.

  - ∇ Set the *caller ID*.

    Enter the "Name" you want to show on the called party's Caller ID display. When you make a call from a line of the Gateway with the Caller ID inserted, the remote called party will receive this string. Gateway US version is factory set to FSK (Bellcore) CID.

  - ∇ Set the SIP call-signaling *port*.

  - ∇ Choose whether or not *AEC* is on.

    The AEC (Automatic Echo Cancellation) reduces the amount of feedback the called party hears when the calling party is using a speakerphone.

  - ∇ Set the Authentication *user name* and *password*.

15.2.3 NAT Settings

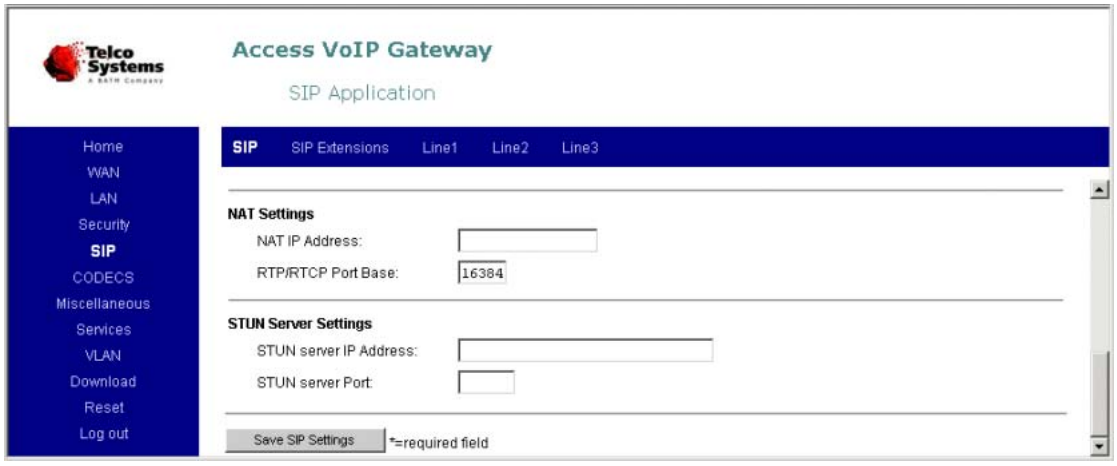


Figure 15-2: SIP Configuration Page (NAT and STUN Server Settings)

- Set the *NAT IP Address* to be used for SIP.

  If the IP address is not set, the NAT option is disabled. For more information regarding the NAT protocol refer to Understanding NAT and NAPT.

- Set the RTP (Real-time Transport Protocol)/RTPC *port base*.

15.2.4 STUN Server Settings

The STUN (Simple Traversal of UDP through NATs) server is an implementation of the STUN protocol that enables STUN functionality in SIP-based systems. STUN is an application-layer protocol that can determine the public IP and nature of a NAT device that sits between the STUN client and STUN server.

- Set the STUN server *IP address*.
- Set the STUN server port.

Set the values for **SIP Server Settings, Nat Settings** and **STUN Server Settings** according to the way the Gateway is connected to the network:

- If the Gateway does not reside behind a NAT server and has an outbound (global) IP address, you only need to set the SIP Server's **IP address**, **Port** and **Domain Name** fields.
- If the Gateway resides behind a NAT server and wishes to communicate with the SIP server via a **Proxy** server:
  - Set the **SIP server IP address** and **Port** fields to the values of the Proxy server's IP address and port.
  - Set the **Domain Name** to the SIP Server's Domain name.
- If the Gateway resides behind a NAT server and wishes to communicate with the SIP server using **STUN** support:
  - Set the SIP server's **IP address, Port** and **Domain Name** fields to the values of the

SIP server's IP address, port and Domain Name.

- Set the **STUN** Server's **IP address** and **Port** fields to the IP and port of the STUN server.

- If the Gateway resides behind a NAT server and the outbound (global) IP is **Static**, the Gateway could be configured to use the outbound (global) IP also for the SIP protocol.
  - Set the SIP server's **IP address, Port** and **Domain Name** fields to the values of the SIP server's IP address, port and Domain Name.
  - Set the **NAT IP address** field to the value of the Gateway's outbound IP address.
- Click the **Save SIP Settings** to save the SIP configuration.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

15.3 SIP Extensions

To configure SIP Extensions:

- In the horizontal menu bar of the **SIP** page, select **SIP Extensions**. The **SIP Extensions** configuration page (Figure 15-3) appears.

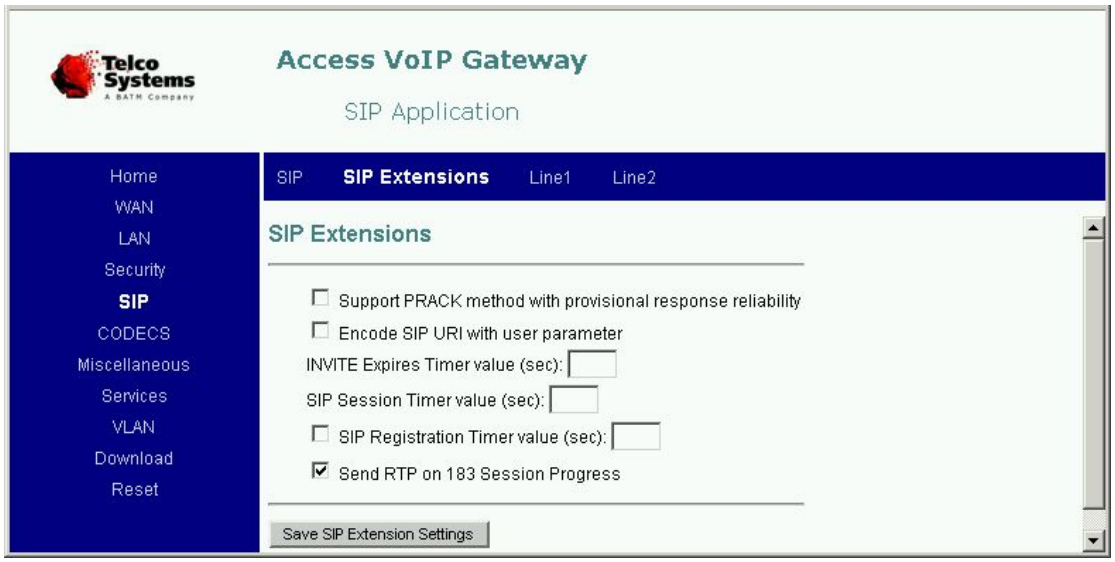


Figure 15-3: Example SIP Extensions Page

Table 15-2 lists the available fields in the SIP Configuration page.

Table 15-2: The Available SIP Extension Configuration Fields

Field Name	Description
Support PRACK method with provisional response reliability	Provides a standard reliability mechanism for provisional responses, which means that the Gateway is sending ACKs for provisional responses (180, 183, etc). Reference: RFC3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP).
Encode SIP URI with user parameter	The set of valid telephone-subscriber strings is a subset of valid user strings. The user URI parameter exists to distinguish telephone numbers from user names that happen to look like telephone numbers. If the user string contains a telephone number formatted as a telephone-subscriber, the user parameter value "phone" SHOULD be present. Even without this parameter, recipients of SIP and SIPS URIs may interpret the pre-@ part as a telephone number if local restrictions on the name space for user name allow it. Reference: RFC3261, Section 19.1.1: *SIP and SIPS URI Components*. Example: from: <77540@192.168.0.40;user=phone>
INVITE Expires Timer value	Defines the length of time we allow for an OK response to an INVITE. If the time elapses – we transmit a CANCEL to invalidate the INVITE. There is no default value - this option is not used if no value is specified. Reference: RFC3261, Section 13.2.1 Creating the Initial INVITE. "The User Agent Client (UAC) MAY add an Expires header field (Section 20.19) to limit the validity of the invitation. If the time indicated in the Expires header field is reached and no final answer for the INVITE has been received, the UAC core SHOULD generate a CANCEL request for the INVITE, as per Section 9".
SIP Session Timer value	Specifies the Session-Expires header in an INVITE request. Used as the SIP session's keep-alive mechanism. There is no default value - this option is not used if no value is specified. Draft-ietf-sip-session-timer-10.txt of the Internet Engineering Task Force is currently supported: "This document defines an extension to the Session Initiation Protocol (SIP). This extension allows for a periodic refresh of SIP sessions through a re-INVITE or UPDATE request. The refresh allows both user agents and proxies to determine if the SIP session is still active". The extension defines two new header fields, Session-Expires, which conveys the lifetime of the session, and Min-SE, which conveys the minimum allowed value for the session timer.

Field Name	Description
SIP Registration Timer Value	Specifies a suggested value that the server should take into consideration when it returns the Expires timer for registration in the OK response. The value is inserted in the Expires header. The server may choose another value, and the device will obey that value (re-register using the server's value). The default value (if no value is specified) is 1800 seconds. Reference: RFC3161, Section 10.2.1.1: Setting the Expiration Interval of Contact Addresses.
Send RTP on 183 Session Progress	By default a caller receiving a "183 Session Progress" response with SDP (Session Description Protocol) should only receive RTP at this stage. For devices that pass through Proxies for NAT (like pulver.com) sending RTP at this stage should be enabled.

- Click **Save SIP Extension Settings** for saving the SIP Extension configuration.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

15.4 Line 1 and Line 2 Status and Configuration

To display the registration status and configure settings for Line 1:

- In the horizontal menu bar of the **SIP** page, select **Line1**. The **Line Status** and **Line Configuration** page for Line 1 (Figure 15-4) appears.

To display the registration status and configure settings for Line 2:

- In the horizontal menu bar of the **SIP** page, select **Line2**. The **Line Status** and **Line Configuration** page for line 2 appears. The page is equivalent to the page for line 1.

15.4.1 Line1 and Line2 Status

The line status displays the registration status on the screen. The following statuses are available:

- **Registered** – This means that the gateway has been registered in the SIP server, and the VoIP service is active.
- **Not registered** – This means the gateway has not been registered in the SIP server.

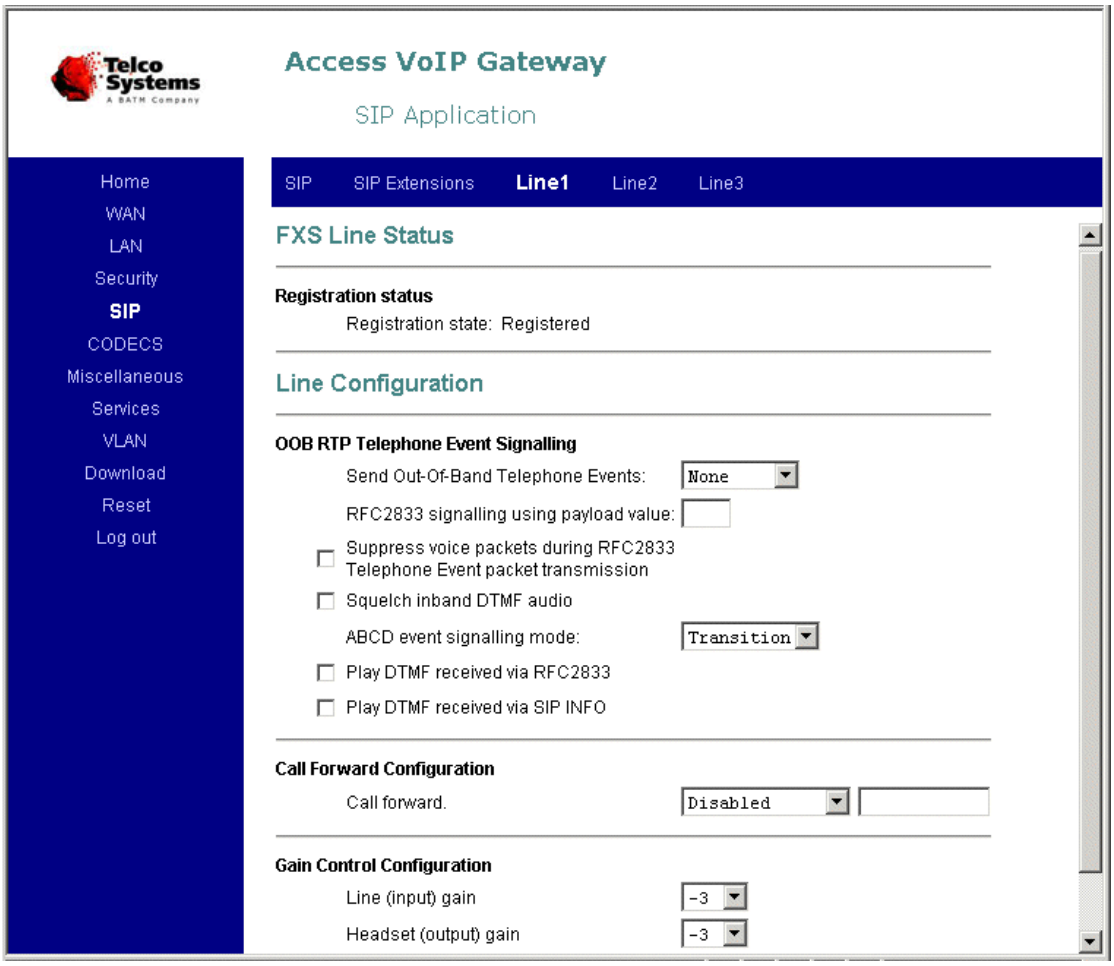


Figure 15-4: Example Line 1 Status and Configuration Page

15.4.2 Line1 and Line2 Configuration

RFC2833 describes a protocol for sending Telephony events (Receiver ON/OFF Hook, Ring ON/OFF) and DTMF digits in RTP packets. This method is used as an alternative method for the SIP protocol signaling frames to solve a variety of signaling delays. The Payload value is Payload Type field of the RTP frame. Payloads 0-95 are well defined and reserved values by IANA. Payload values of 96-127 are free (dynamic) and are not reserved by the standards.

If the RFC2833 protocol for Telephony events is enabled, voice packets can be suppressed during the transmission of the RFC2833 Telephone Event packets.

The SIP RTP Telephone Event Signaling (RFC2833) configuration parameters are configured per line. Figure 15-4 shows the configuration fields for Line1. The configuration page for Line2 is equivalent to this page.

Another alternative method is to send the DTMF via the SIP INFO method.

To configure RTP Telephone Event (RFC2833) parameters or SIP INFO DTMF:

- In the horizontal menu bar of the SIP configuration page, select **Line 1** for line 1 configuration (Figure 15-4) or **Line 2** for line 2 configuration. The Line Configuration page for the selected line will appear.

Table 15-3 lists the available fields in the SIP RTP Telephone Event (RFC2833) and SIP INFO DTMF method configuration page for both line 1 and line 2. Note that each parameter needs to be set for each line separately.

Table 15-3: The Available SIP RTP Telephone Event (RFC2833) Configuration Fields

Field Name	Description
Send Out-Of-Band Telephone Events	When this field is selected, the Gateway can send DTMF via SIP INFO method, or it can send the Telephony events and DTMF via RFC2833 frames. For RFC2833 the payload field value must be set. The default payload value is 96. Consult your Call server documentation to know if the SIP INFO method or RFC2833 option is supported and what Payload value is required.
Suppress voice packets during RFC2833 Telephone Event packet transmission	Enabling this option preserves the original voice bandwidth and prevents the need for more bandwidth for the RFC2833 packets. Consult your Call server documentation for the preferred mode of operation.
Squelch inband DTMF audio	When selected inband DTMF audio is not transmitted in the audio stream.
ABCD event signaling mode	Two possible modes for RFC2833 Telephony events signaling (ABCD signaling packets) are available: **Transition** mode: In this mode, the event packet is sent only at the moment of the event. **Continuous** mode: In this mode, the event packet is sent continuously at the rate of the voice, as long as the event exists. The Continuous mode behaves better in situations of packet loss, preventing cases such as stuck ringers. Consult your Call server documentation for the preferred mode of operation.
Play DTMF received via RFC 2833	Option to generate DTMF tones for received OOB RFC 2833 DTMF events.
Play DTMF received via SIP INFO	Option to generate DTMF tones received via the SIP INFO method.

To set the Call Forward Configuration:

- Select the setting of the Call Forwarding feature. The Call Forwarding applies during call establishment by providing a diversion of an incoming call to another destination alias address. Call forwarding can also be activated by dialing *1 or *2 and deactivted by dialing *3 (See link 4.4.3). The following stetting are available:
    - Disabled
    - Conditional

Callees frequently wish to redirect incoming calls to an alternative destination if the primary destination fails to answer within 20 seconds. The reasons for failure are multifold. They may include busy callee, disconnected callee's phone, user who currently does not answer, or user denying the incoming call. The alternative destination is typically a voicemail system but it may be also another human or some other SIP device.

- Unconditional

  The call is always diverted to another destination.

Both types of Forwarding, Conditional and Unconditional can be selected.

To set the Gain Control Configuration (headset volume) for VoIP calls:

- In the SIP page horizontal menu bar, select **Line1** or **Line2**.
  - Select a **Line (input) Gain** value in the range of <-12 to +3>. This is the volume at which the callee will hear the caller.
  - Select a **Headset (output) Gain** value in the range of <-12 to +3>. This sets the volume at which the caller will hear through the headset. If this volume is too loud, an echo will occur in the headset.
- Click **Save Line Settings** to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

15.5 Line3 Configuration (AC-241-FXO only)

This **Line3 (FXO)** page enables to set up **Gain Control Configuration** settings and **PSTN Detection** for PSTN communication.

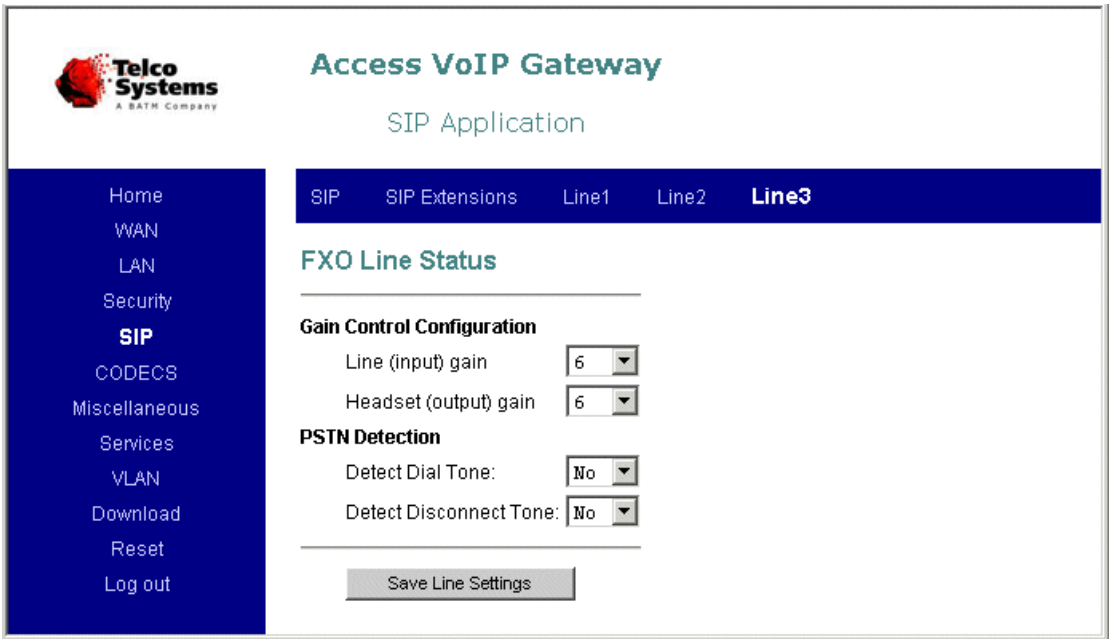


Figure 15-5: Line 3 Configuration Page

To set the Gain Control Configuration (headset volume) for PSTN calls:

- In the SIP page horizontal menu bar, select **Line3**.
  - Select a **Line (input) Gain** value in the range of <+12 to -12>. This is the volume at which the callee will hear the caller.
  - Select a **Headset (output) Gain** value in the range of <+12 to -12>. This sets the volume at which the caller will hear through the headset. If this volume is too loud, an echo will occur in the headset.

To set the PSTN Detection settings for PSTN calls (FXO):

- **Detect Dial Tone** – to enable the option, select **Yes**. By default the option is enabled.

  If the option is enabled, after the caller dials a PSTN number, the gateway "listens" for a valid FXO Dial Tone in order to route the call to the PSTN. If a valid FXO Dial Tone is not detected the Reorder Tone (Fast Busy) will be heard in the headset indicating that the call can not be executed.

  If the option is disabled, the unit will not check for a valid FXO Dial Tone and the caller will not be alerted if the PSTN call can not to be executed. Refer to Call Progress Tones to configure the FXO Dial Tone to be configured.

- **Detect Disconnect Tone** – to enable the option, select **Yes**. By default the option is enabled.

  If the option is enabled the gateway "listens" for the Disconnect tone indicating the termination of the PSTN phone call by the PSTN. If the option is disabled the caller will need to go on hook to complete the call termination. Refer to Call Progress Tones to configure the FXO Disconnect Tone to be detected can be configured.

- Click **Save Line Settings** to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

15.6 Audio/CODEC Configuration

The Gateway supports G711 u-law and a-law standards by default. The user can set the Gateway to also support one of the three voice coding standards: G723, G726 or G729. Both ports will be allowed to use the selected option. For every supported voice coding standard the user can enable/disable **Silence Suppression** and, except for G723, select the default **Packetization** period (as a multiple of 10ms in the range 10ms-100ms).

To set Audio/CODEC parameters:

1. In the vertical menu bar of the current Gateway Web page, select **CODECS**. The **Audio/CODEC Configuration** page appears (Figure 15-6).

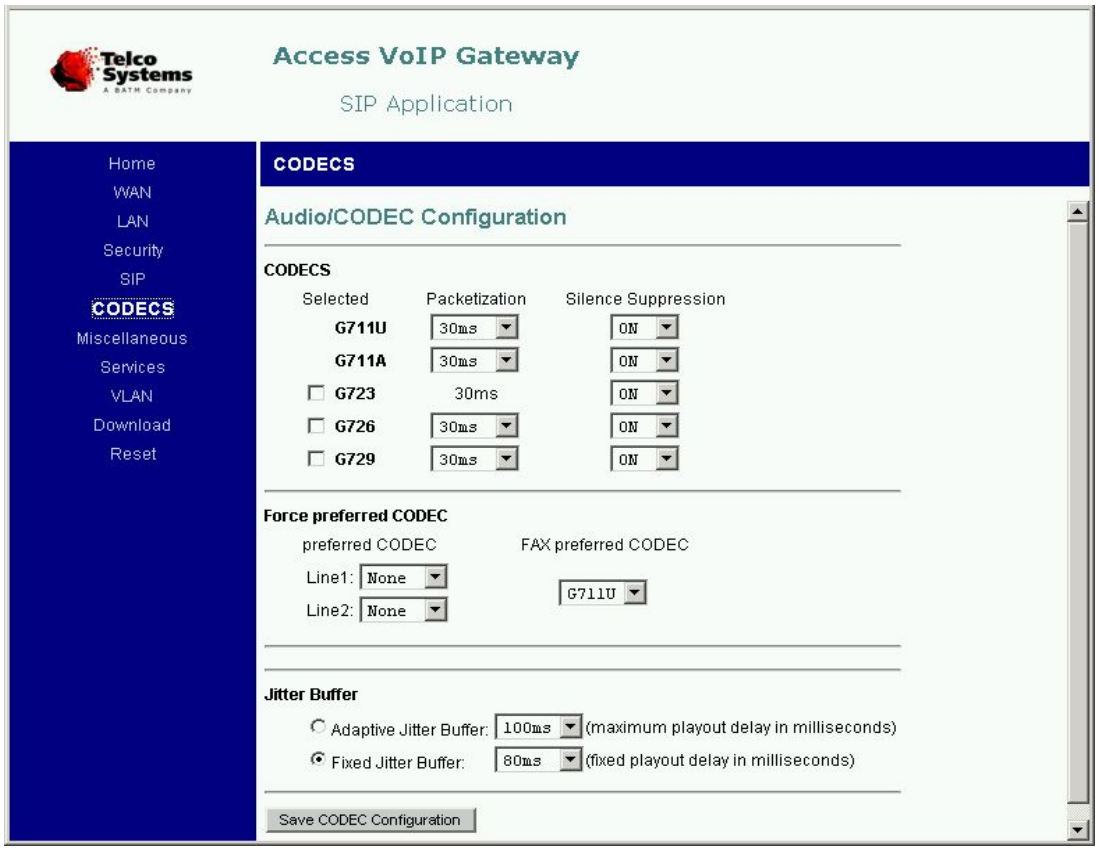


Figure 15-6: The Audio/CODEC Configuration Page

2. Select the Audio/CODEC *standard*.
3. Set the *Packetization* period.
4. Set the *Silence Suppression*.
5. Set the *Fixed Jitter Buffer*, which is the fixed playout delay in milliseconds.

   You may select Adaptive Jitter Buffer, and set the maximum playout delay in milliseconds.
6. Click **Save CODEC Configuration** at the bottom of the Web page to effect the changes.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

15.7 Selecting a Preferred CODEC for SIP

During the CODEC negotiation process you can select preferred CODEC regardless of its position in the SDP packet. By default, no preferred CODEC is set and the first common CODEC in SDP CODEC list is selected.

NOTE **A complex CODEC (G723, G726, G729) can be used as a preferred CODEC only if it is selected in the CODECS screen.**

15.7.1.1 Selecting Preferred CODEC for Fax Transmissions for SIP

You can select preferred CODEC for fax transmissions. The Preferred CODEC parameter is displayed on the CODEC Web Screen. Possible values for the parameter are G711U, G711A and NONE. For NONE the Fax CODEC is the same as assigned for the regular voice calls. The preferred CODEC for fax insures that G711 CODEC is used for all fax transmissions even if a complex CODEC like G729 is selected for voice.

16 Completing the Gateway Configuration via Web

After entering and saving all configurations, you MUST reset the Gateway.

To reset the Gateway with the new configuration settings:

1. In the vertical menu bar, select **Reset**. The **Reset** page appears (Figure 16-1).

2. Click the **Reset** button. The Gateway reboots and the application home page opens with the new configuration settings.

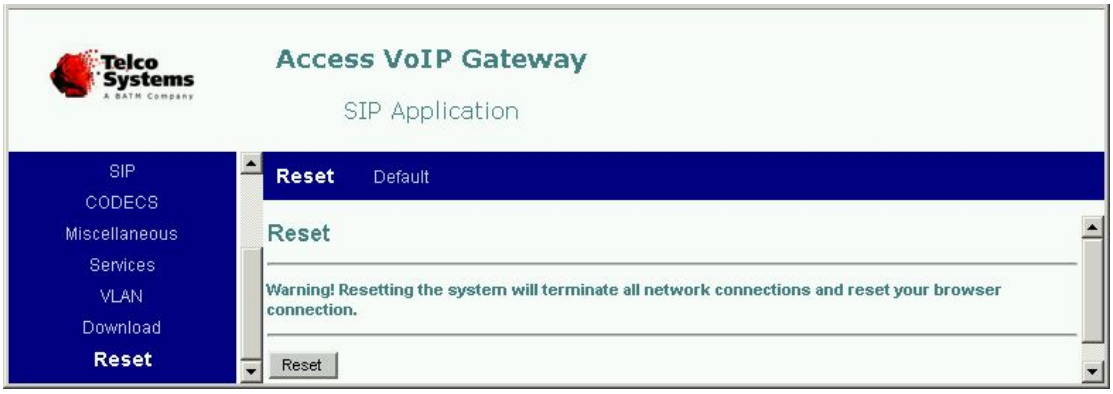


Figure 16-1: Reset Page

To reset the Gateway to factory default configuration:

1. In the horizontal menu bar of the Reset page, select **Default**. The **Set Default Configuration** page (Figure 16-2) appears.

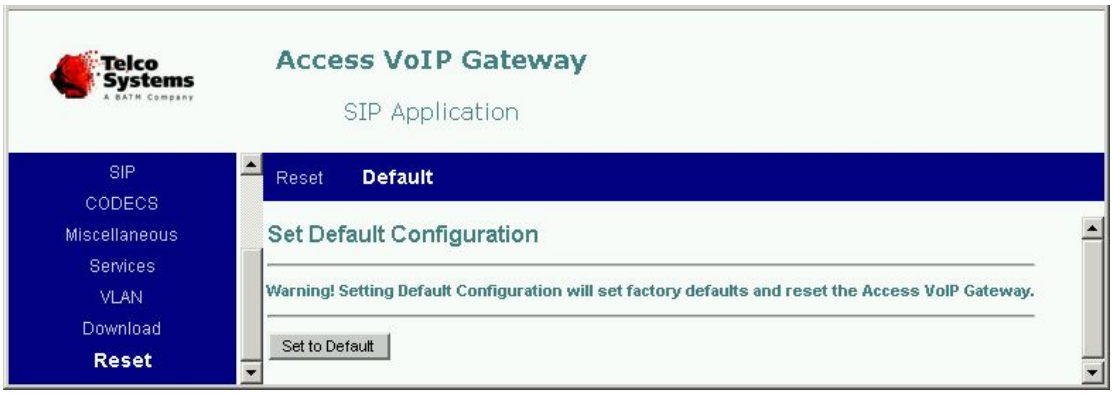


Figure 16-2: Set Default Configuration Page

2. Click the **Set to Default** button. The Gateway reboots and the application home page opens with the factory default settings. If you apply the default configuration, all changes except network parameters (IP, DHCP mode, etc.) are cancelled.

17 Configuring the Gateway via Telnet

You can use the terminal CLI (Command Line Interface) commands via Telnet to configure and control the Gateway.

Any workstation with a Telnet facility should be able to communicate with the Gateway over the network. Two Telnet sessions can be opened concurrently with the Console. The Telnet session will be disconnected after a specified time of inactivity.

Before you can start a Telnet session, you must know the IP address of the Gateway. To open the Telnet session, you must specify the IP address of the Gateway that you want to manage. Check the user manual supplied with your Telnet facility if you are unsure of how to do this.

Once the connection is established, you will be prompted to log in. VT100 emulation and V100 keys must be used.

To apply a CLI command:

1. Type the command in lowercase characters. You may abbreviate any or all of the keywords.

   Examples of abbreviations: l or ? for list, en for end (as a rule, you may abbreviate keywords down to the shortest unique abbreviation – any length between the full and the shortest unique presentation is valid).

2. Press <Enter>.

3. You may use the UP or DOWN arrows to scroll through the last eight commands.

17.1 Command Modes

The CLI user interface is divided into several modes. The mode you are currently in determines the available commands. Enter a question mark (?) at the mode prompt to obtain a list of commands available for each command mode.

17.1.1 Enable Mode

When you start a session, you begin in Enable mode. The Enable mode prompt is an angle bracket (>):

```
IGP>
```

Enable mode can be password protected. By default, no password is set. You can set a password using the Web management (for more information, see Setting the Password).

17.1.2 Commands Mode

The Commands mode allows you to perform general operations on the Gateway such as rebooting, restoring the Gateway to the factory defaults and downloading a configuration file or software image. The Commands mode is indicated by the following prompt:

```
IGP.Commands >
```

To access the Commands mode:

Type the **commands** command (or the **c** shortcut) in Enable mode:

```
IGP >commands
IGP >c
```

The system responds with the Commands prompt:

```
IGP.Commands >
```

Table 17-1 shows the commands that are available in Commands mode.

Table 17-1: Command Mode Commands

Command	Description
reboot,r	Resets the system.
default,d	Sets the default configuration.
copy,c	Downloads a software image or configuration file from a TFTP\HTTP server.
send,s	Sends information to the Syslog server
ping <host> [<1-100>]	'host' is the IP of the host to ping followed by the number of pings to send. The unit will ping the host and display a status of the received ping replies.

The Commands mode commands are described in the Completing the Gateway Configuration via Telnet chapter.

17.1.3 Report Mode

The Report mode allows you to display the interfaces statistics and download configuration information. The Report mode is indicated by the following prompt:

```
IGP.Report >
```

To access the Report mode:

Type the **report** command (or the **r** shortcut) in Enable mode:

```
IGP >report
```

```
IGP >r
```

The system responds with the Report prompt:

```
IGP.Report >
```

17.1.4 Statistics Mode

The Statistics mode allows you to display and clear the interfaces statistics. The Statistics mode is indicated by the following prompt:

```
IGP.Report.Statistics >
```

To access the Statistics mode:

Step 1: Type the **report** command (or the **r** shortcut) in Enable mode:

```
IGP >report
IGP >r
```

The system responds with the Report prompt:

```
IGP.Report >
```

Step 2: Type the **statistics** command (or the **s** shortcut) in Report mode:

```
IGP.Report >statistics
IGP.Report >s
```

The system responds with the Statistics prompt:

```
IGP.Report.Statistics >
```

17.1.5 Download Mode

The Download mode allows you to display the configuration download status. The Download mode is indicated by the following prompt:

```
IGP.Report.Download >
```

To access the Download mode:

Step 1: Type the **report** command (or the **r** shortcut) in Enable mode:

```
IGP >report
IGP >r
```

The system responds with the Report prompt:

```
IGP.Report >
```

Step 2: Type the **download** command (or the **d** shortcut) in Report mode:

```
IGP.Report >download

IGP.Report >d
```

The system responds with the Download prompt:

```
IGP.Report.Download >
```

17.1.6 Configuration Modes

Using the configuration modes (Global, Interface, etc.), you can make changes to the Gateway's configuration. If you save the configuration, these commands are stored and used after rebooting. To access the various configuration modes, you must start at Global Configuration mode.

The Global Configuration mode allows configuration capabilities. It is indicated by the following prompt:

```
IGP.Config >
```

The following example indicates that the CLI is in Interface Configuration mode:

```
IGP.Config.Interface >
```

To access the Global Configuration mode:

Type the **config** command (or the **con** shortcut) in Enable mode:

```
IGP >config

IGP >con
```

The system responds with the Global Configuration prompt:

```
IGP.Config.Interface >
```

Table 17-2 shows the configuration modes available in the Gateway.

Table 17-2: Configuration Modes Summary

Configuration Mode	For configuring	Command Syntax

Interface	The Gateway physical interfaces settings.	`IPG.Config >interface`
		`IPG.Config.Interface >`
		
		`IPG.Config >in`
		`IPG.Config.Interface >`

Security	The security settings.	`IPG.Config >security`
		`IPG.Config.Security >`
		
		`IPG.Config >se`
		`IPG.Config.Security >`

Configuration Mode	For configuring	Command Syntax
Network	The network settings (LAN and WAN).	IPG.Config >**netconfig** IPG.Config.Network > IPG.Config >**n** IPG.Config. Network >
LAN	The LAN (Local Area Network) settings.	IPG.Config.Network >**lan** IPG.Config.Network.Lan > IPG.Config.Network >**la** IPG.Config.Network.Lan >
WAN	The WAN (Wide Area Network) settings.	IPG.Config.Network >**wan** IPG.Config.Network.Wan > IPG.Config.Network >**w** IPG.Config.Network.Wan >
VLAN	Virtual LANs (VLANs) settings.	IPG.Config >**vlan** IPG.Config.VLAN > IPG.Config >**v** IPG.Config.VLAN >
HTTP	The HTTP (Hypertext Transfer Protocol) settings.	IPG.Config >**http** IPG.Config.HTTP > IPG.Config >**ht** IPG.Config.HTTP >
SIP	The SIP (Session Initiation Protocol) settings.	IPG.Config >**sip** IPG.Config.SIP > IPG.Config >**si** IPG.Config.SIP >
H.323	The H.323 protocol settings.	IPG.Config **>h323** IPG.Config.H323 > IPG.Config >**h3** IPG.Config.H323 >
MGCP	The MGCP (Media Gateway Control Protocols) settings.	IPG.Config >**mgcp** IPG.Config.Mgcp > IPG.Config >**m** IPG.Config.Mgcp >

17.2 General Commands

Table 17-3 lists the commands you can use at all times, regardless of the type of the prompt that is displayed.

Table 17-3: General Commands

Command	Description
`exit`	Escape current mode and go to previous mode.
`help`	Display the format of available commands in the current mode. You

Command	Description
	can also use the question mark (?) for displaying the list of commands.
quit	Disconnect and log out.
end	Escape current mode and go to Privileged (Enable) mode.
list (or ?)	Display list of the command available in the current mode.

17.3 Using the CLI Commands

The CLI commands can be used in two forms:

1. Typing the full form of the command that is specified in the command help:

```
IPG.Config >?
IPG.Config > interface,in  - Interface Configuration
IPG.Config > security,se   - Advanced Security Configuration
IPG.Config > netconfig,n   - Network Configuration
IPG.Config > vlan,v        - VLAN Configuration
IPG.Config > http,ht       - HTTP Configuration
IPG.Config > sip,si        - SIP Configuration
IPG.Config > help,h   - Display commands format
IPG.Config > list,l,? - Display command list
IPG.Config > end,en   - current mode and go to main mode
IPG.Config > exit,ex  - current mode and go to previous mode
IPG.Config > quit,q   - Quit console
IPG.Config >interface
```

2. Using the abbreviated form (shortest unique form) of the command, that is specified in the command help.

```
IPG.Config >?
IPG.Config > interface,in  - Interface Configuration
IPG.Config > security,se   - Advanced Security Configuration
IPG.Config > netconfig,n   - Network Configuration
IPG.Config > vlan,v        - VLAN Configuration
IPG.Config > http,ht       - HTTP Configuration
IPG.Config > sip,si        - SIP Configuration
IPG.Config > help,h   - Display commands format
IPG.Config > list,l,? - Display command list
IPG.Config > end,en   - current mode and go to main mode
IPG.Config > exit,ex  - current mode and go to previous mode
IPG.Config > quit,q   - Quit console
IPG.Config >in
```

3. Using any combination longer than the abbreviated form and shorter than the full form of the command which is specified in the command help:

```
IPG.Config >inter
```

NOTE **Command abbreviations that are shorter than the specified abbreviated forms are not accepted.**

18 WAN Configuration via Telnet

The WAN CLI allows you to configure the following WAN settings:

- WAN IP address, netmask and gateway address;
- IP DNS Server addresses, host and domain name;
- VoIP IP address, netmask and gateway address;
- WAN broadcast and multicast traffic limitation;
- Point-to-Point Protocol over Ethernet (PPPoE) authentication and settings;
- MAC spoofing (overriding the MAC address registered at the broadband provider);
- Automatic configuration at preset time intervals.

18.1 Default WAN Configuration

Table 18-1: Default WAN Configuration

Parameter	Default Value
Obtain IP address	Use DHCP Server
DHCP automatic configuration ID	0
DHCP options 66, 67	Enabled
Auto Config mode	Enabled

18.2 WAN Configuration Commands

Table 18-2 lists the WAN configuration commands.

NOTE After setting and saving all configurations, you MUST reset the Gateway.

Table 18-2: The Available WAN Configuration Commands

Command	Description
`wan`	Enters into WAN Configuration mode.
`set dhcp`	Enables the use of DHCP server for obtaining the network IP parameters.

Command	Description
`set ipaddress`	Sets the IP address of the WAN interface if fixed IP address was selected.
`set ipnetmask`	Sets the subnet mask of the WAN interface if fixed IP address was selected.
`set ipgateway`	Sets the default gateway of the WAN interface if fixed IP address was selected.
`set ipdns`	Sets the IP address of the DNS if fixed IP address was selected.
`set dnshostname`	Sets the unit's host-name
`set dnsdomainname`	Sets the domain-name of the DNS if fixed IP address was selected.
`set id`	Sets the Automatic Configuration ID. The **no** form of the command removes the DHCP Automatic Configuration ID
`set options6667`	Enables the use of DHCP options 66, 67.
`set autoconfig`	Enables the Auto Config mode.
`set tftpip`	Sets the TFTP/HTTP server IP address.
`set file`	Sets the file name.

18.2.1 Entering into WAN Configuration Mode

The **wan** command, in Network Configuration mode, enters into WAN Configuration mode.

The prompt-line that is displayed in response to the command indicates that WAN Configuration mode has been entered.

Command Syntax

```
IPG.Config.Network >wan
IPG.Config.Network.Wan >

IPG.Config.Network >w
IPG.Config.Network.Wan >
```

18.2.2 Enabling DHCP

The **set dhcp** command, in WAN Configuration mode, enables the use of DHCP server for obtaining the network IP parameters. The **no** form of the command restores the DHCP server option to the default value.

For more information regarding the DHCP protocol, refer to Understanding DHCP.

By default, the DHCP option is enabled.

Command Syntax

```
IPG.Config.Network.Wan >set dhcp {y | n}
IPG.Config.Network.Wan >no set dhcp

IPG.Config.Network.Wan >se dh {y | n}
IPG.Config.Network.Wan >no set dhcp
```

Argument Description

y	Use DHCP.
n	Use a fixed IP address.

18.2.3 Setting the IP Address of the WAN Interface

The **set ipaddress** command, in WAN Configuration mode, sets the IP address of the WAN interface if fixed IP address was selected (by disabling DHCP). The **no** form of the command removes the IP address.

You should set or change the IP address only if your broadband provider requires it.

Command Syntax

```
IPG.Config.Network.Wan >set ipaddress A.B.C.D
IPG.Config.Network.Wan >no set ipaddress

IPG.Config.Network.Wan >se pie A.B.C.D
IPG.Config.Network.Wan >no se ipa
```

Argument Description

A.B.C.D	IP address.

18.2.4 Setting the Subnet Mask of the WAN Interface

The **set ipnetmask** command, in WAN Configuration mode, sets the subnet mask of the WAN interface if fixed IP address was selected (by disabling DHCP). The **no** form of the command removes the subnet mask.

You should set or change the IP subnet netmask only if your broadband provider requires it.

Command Syntax

```
IPG.Config.Network.Wan >set ipnetmask A.B.C.D
IPG.Config.Network.Wan >no set ipnetmask

IPG.Config.Network.Wan >se ipn A.B.C.D
IPG.Config.Network.Wan >no se ipn
```

Argument Description

A.B.C.D	IP network mask.

18.2.5 Setting the Default Gateway of the WAN Interface

The **set ipgateway** command, in WAN Configuration mode, sets the IP address of the default gateway of the WAN interface if fixed IP address was selected (by disabling DHCP). The **no** form of the command removes the default gateway.

You should set or change the default gateway's IP address only if your broadband provider requires it.

Command Syntax

```
IPG.Config.Network.Wan >set ipgateway A.B.C.D
IPG.Config.Network.Wan >no set ipgateway

IPG.Config.Network.Wan >se ipg A.B.C.D
IPG.Config.Network.Wan >no se ipg
```

Argument Description

A.B.C.D	IP address of the default gateway.

18.2.6 Setting the IP Address of the DNS Server

The **set ipdns** command, in WAN Configuration mode, sets the IP address of the DNS Server if fixed IP address was selected (by disabling DHCP). The **no** form of the command removes the IP address.

Command Syntax

```
IPG.Config.Network.Wan >set ipdns A.B.C.D
IPG.Config.Network.Wan >no set ipdns

IPG.Config.Network.Wan >se ipd A.B.C.D
IPG.Config.Network.Wan >no se ipd
```

Argument Description

A.B.C.D	IP address of the DNS server.

18.2.7 Setting the Host Name

The **set dnshostname** command, in WAN Configuration mode, sets the host name of the unit. The **no** form of the command removes the host name.

Command Syntax

```
IPG.Config.Network.Wan >set dnshostname STRING
IPG.Config.Network.Wan >no set dnshostname

IPG.Config.Network.Wan >se dnsh STRING
IPG.Config.Network.Wan >no se dnsh
```

Argument	Description
STRING	Host-name of the DNS server.

18.2.8 Setting the Domain Name

The **set dnsdomainname** command, in WAN Configuration mode, sets the domain name of the unit if fixed IP address was selected (by disabling DHCP). The **no** form of the command removes the domain name.

Command Syntax

```
IPG.Config.Network.Wan >set dnsdomainname STRING
IPG.Config.Network.Wan >no set dnsdomainname

IPG.Config.Network.Wan >se dnsd A.B.C.D
IPG.Config.Network.Wan >no se dnsd
```

Argument	Description
STRING	Domain-name of the DNS server.

18.2.9 Setting the Automatic Configuration ID

The **set id** command, in WAN Configuration mode, sets the Automatic Configuration ID. The **no** form of the command removes the DHCP Automatic Configuration ID.

The Gateway will run the configuration file only if the file name or ID is different from the ones currently stored in the Gateway.

If the ID in the Config file or on the DHCP server is set to the literal value "always", the configuration file is executed on every boot without comparing to the ID stored in the Gateway.

By default, the configuration ID is set to zero (0).

Command Syntax

```
IPG.Config.Network.Wan >set id STRING
IPG.Config.Network.Wan >no set id

IPG.Config.Network.Wan >se id STRING
IPG.Config.Network.Wan >no se id
```

Argument	Description
STRING	The Automatic Configuration ID.

18.2.10 Enabling the Use of DHCP Options 66, 67

The **set options 66, 67** command, in WAN Configuration mode, enables the use of DHCP options 66, 67. The **no** form of the command restores the DHCP server options to the default value.

In DHCP download (Bootp), the Gateway must be in DHCP mode. The name of the "root" configuration file and the IP of the TFTP server are supplied to the Gateway when the Gateway queries the DHCP server for an IP address and a boot file, during boot and at half lease-time.

To enable using DHCP options 66, 67, select the **Use DHCP code options 66, 67** check box. When this check box is selected:

- Option 66 (**Boot Server Host Name**) is set as the IP of the TFTP server for the "root" configuration file.
- Option 67 (**Bootfile Name**) is set as the name of the "root" configuration file.

By default, the DHCP options 66, 67 are enabled.

Command Syntax

```
IPG.Config.Network.Wan >set options6667 {y | n}
IPG.Config.Network.Wan >no set options6667

IPG.Config.Network.Wan >se o {y | n}
IPG.Config.Network.Wan >no set o
```

Argument Description

y	Enables DHCP options 66, 67.
n	Disables DHCP options 66, 67.

18.2.11 Enabling the Auto Config Mode

The **set autoconfig** command, in WAN Configuration mode, enables the Auto Config mode. The **no** form of the command restores the Auto Config mode to the default value.

By default, the Auto Config is enabled.

Command Syntax

```
IPG.Config.Network.Wan >set autoconfig {y | n}
IPG.Config.Network.Wan >no set autoconfig

IPG.Config.Network.Wan >se a {y | n}
IPG.Config.Network.Wan >se a
```

Argument Description

y	Enables Auto Config.
n	Disables Auto Config.

18.2.12 Setting the TFTP/HTTP Server IP Address

The **set tftpip** command, in WAN Configuration mode, sets the TFTP/HTTP server's IP address. The **no** form of the command removes the TFTP/HTTP server's IP address.

Command Syntax

```
IPG.Config.Network.Wan >set tftpip A.B.C.D
IPG.Config.Network.Wan >no set tftpip

IPG.Config.Network.Wan >se t STRING
IPG.Config.Network.Wan >no se t
```

Argument Description

A.B.C.D	The TFTP/HTTP server's IP address.

18.2.13 Setting the File Name

The **set file** command, in WAN Configuration mode, sets the file name. The **no** form of the command removes the file name.

The file name is the name of the ROM image file that you wish to download. The format of the file name must be one of the following:

- Loader file: upgr_211_x_xx.rom
- Configuration file: ipg_xxxx.cfg
- Application file: h323_211_xxxx.rom, mgcp_211_xxxx.rom or sip_211_xxxx.rom

Command Syntax

```
IPG.Config.Network.Wan >set file STRING
IPG.Config.Network.Wan >no set file

IPG.Config.Network.Wan >se f STRING
IPG.Config.Network.Wan >no se f
```

Argument Description

STRING	File name.

18.3 WAN Displaying Commands

Table 18-3 lists the WAN displaying commands.

Table 18-3: The Available WAN Displaying Commands

Command	Description
show all	Displays the entire WAN configuration.
show dhcp	Displays the status of the use of DHCP server for obtaining the network IP parameters.
show ipaddress	Displays the IP address of the WAN interface.

Command	Description
show netmask	Displays the subnet mask of the WAN interface.
show ipgateway	Displays the IP address of the WAN interface's default gateway.
show ipdns	Displays the IP address of the DNS.
show dnshostname	Displays the host-name of the unit
show dnsdomainname	Displays the domain-name of the unit
show id	Displays the DHCP automatic configuration ID.
show options6667	Displays whether DHCP options 66, 67 is enabled.
show autoconfig	Displays the Automatic Configuration mode status.
show tftpip	Displays the TFTP\HTTP server's IP address.
show file	Displays the file name.

18.3.1 Displaying all the WAN Configuration

The **show all** command, in WAN Configuration mode, displays the entire WAN configuration.

Command Syntax

```
IPG.Config.Network.Wan >show all

IPG.Config.Network.Wan >sh all
```

Example

```
IPG.Config.Network.Wan >show all
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > dhcp|dh                = y
IPG.Config.Network.Wan > *** DHCP configuration ***
IPG.Config.Network.Wan > IP address             = 10.2.197.190
IPG.Config.Network.Wan > IP Subnet Mask         = 255.255.224.0
IPG.Config.Network.Wan > IP Gateway             = 10.2.193.223
IPG.Config.Network.Wan > Domain Name Server IP  = 10.2.127.100
IPG.Config.Network.Wan > DHCP Server IP         = 10.2.193.223
IPG.Config.Network.Wan > IP address TFTP server = 0.0.0.0
IPG.Config.Network.Wan > Domain Name            =
IPG.Config.Network.Wan > Root Configuration File =
IPG.Config.Network.Wan > ID Configuration File  =
IPG.Config.Network.Wan > id|id                  = 0
IPG.Config.Network.Wan > options6667|o          = y
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > *** Automatic configuration ***
IPG.Config.Network.Wan > autoconfig|a           = n
IPG.Config.Network.Wan > tftpip|t               = 10.2.171.203
IPG.Config.Network.Wan > file|f                 = ipg_211s.cfg
IPG.Config.Network.Wan >
```

18.3.2 Displaying the Status of the DHCP Server

The **show dhcp** command, in WAN Configuration mode, displays the status of the use of DHCP server for obtaining the network IP parameters.

Command Syntax

```
IPG.Config.Network.Wan >show dhcp

IPG.Config.Network.Wan >sh dh
```

Example

```
IPG.Config.Network.Wan >show dhcp
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > dhcp|dh                = y
```

18.3.3 Displaying the IP address of the WAN Interface

The **show ipaddress** command, in WAN Configuration mode, displays the IP address of the WAN interface.

Command Syntax

```
IPG.Config.Network.Wan >show ipaddress

IPG.Config.Network.Wan >sh ipa
```

Example

```
IPG.Config.Network.Wan >show ipaddress
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > ipaddress|ipa       =
```

18.3.4 Displaying the Subnet Mask of the WAN Interface

The **show netmask** command, in WAN Configuration mode, displays the subnet mask of the WAN interface.

Command Syntax

```
IPG.Config.Network.Wan >show netmask

IPG.Config.Network.Wan >sh n
```

Example

```
IPG.Config.Network.Wan >show netmask
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > netmask|n       = 255.255.0.0
```

- Displaying the IP Address of the WAN Interface's Default Gateway

The **show ipgateway** command, in WAN Configuration mode, displays the IP address of the WAN interface's default gateway.

Command Syntax

```
IPG.Config.Network.Wan >show ipgateway

IPG.Config.Network.Wan >sh ipg
```

Example

```
IPG.Config.Network.Wan >show ipgateway
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > ipgateway|ipg       = 10.1.1.1
```

18.3.5 Displaying the IP Address of the DNS Server

The **show ipdns** command, in WAN Configuration mode, displays the IP address of the DNS Server.

Command Syntax

```
IPG.Config.Network.Wan >show ipdns

IPG.Config.Network.Wan >sh ipd
```

18.3.6 Displaying the Host Name of the Unit

The **show dnshostname** command, in WAN Configuration mode, displays the host name of the unit

Command Syntax

```
IPG.Config.Network.Wan >show dnshostname

IPG.Config.Network.Wan >sh dnsh
```

18.3.7 Displaying the Domain Name of the Unit

The **show dnsdomainname** command, in WAN Configuration mode, displays the domain name of the unit.

Command Syntax

```
IPG.Config.Network.Wan >show dnsdomainname STRING

IPG.Config.Network.Wan >sh dnsd
```

18.3.8 Displaying the DHCP Automatic Configuration ID

The **show id** command, in WAN Configuration mode, displays the DHCP automatic configuration ID.

Command Syntax

```
IPG.Config.Network.Wan >show id

IPG.Config.Network.Wan >sh id
```

Example

```
IPG.Config.Network.Wan >show id
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > id|id                    = 0
```

18.3.9 Displaying the DHCP Options 66, 67 Status

The **show options6667** command, in WAN Configuration mode, displays whether DHCP options 66, 67 are enabled.

Command Syntax

```
IPG.Config.Network.Wan >show options6667

IPG.Config.Network.Wan >sh o
```

Example

```
IPG.Config.Network.Wan >show options6667
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > options6667|o           = y
```

18.3.10 Displaying the Auto Config Mode Status

The **show autoconfig** command, in WAN Configuration mode, displays the Automatic Configuration mode status.

Command Syntax

```
IPG.Config.Network.Wan >show autoconfig

IPG.Config.Network.Wan >sh a
```

Example

```
IPG.Config.Network.Wan >show autoconfig
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > autoconfig|a            = y
```

18.3.11 Displaying the TFTP\HTTP Server's IP Address

The **show tftpip** command, in WAN Configuration mode, displays the TFTP\HTTP server's IP address.

Command Syntax

```
IPG.Config.Network.Wan >show tftpip

IPG.Config.Network.Wan >sh t
```

Example

```
IPG.Config.Network.Wan >show tftpip
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > tftpip|t                = 10.2.197.9
```

18.3.12 Displaying the File Name

The **show file** command, in WAN Configuration mode, displays the configuration file name.

Command Syntax

```
IPG.Config.Network.Wan >show file

IPG.Config.Network.Wan >sh f
```

Example

```
IPG.Config.Network.Wan >show file
IPG.Config.Network.Wan >show file
IPG.Config.Network.Wan >
IPG.Config.Network.Wan > file|f                  = ipg_211s.cfg
```

19 LAN Configuration via Telnet

The LAN CLI allows you to configure the following LAN settings:

- LAN IP address and subnet mask.

19.1 Default LAN Configuration

Table 19-1: Default LAN Configuration

Parameter	Default Value
Default IP address of the LAN interface	192.168.100.1
Default IP address of the DHCP client	192.168.100.100

19.2 LAN Configuration Commands

Table 19-2 lists the LAN configuration commands.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Table 19-2: The Available LAN Configuration Commands

Command	Description
`lan`	Enters into LAN Configuration mode.
`set ipaddress`	Sets the IP address of the LAN interface.
`set ipnetmask`	Sets the subnet mask of the LAN interface.

19.2.1 Entering into LAN Configuration Mode

The **lan** command, in Network Configuration mode, enters into LAN Configuration mode.

The prompt-line that is displayed in response to the command indicates that LAN Configuration mode has been entered.

Command Syntax

```
IPG.Config.Network >lan
IPG.Config.Network.Lan >
```

```
IPG.Config.Network >la
IPG.Config.Network.Lan >
```

19.2.2 Setting the IP Address of the LAN Interface

The **set ipaddress** command, in LAN Configuration mode, sets the IP address of the LAN interface. The **no** form of the command removes the IP address.

Command Syntax

```
IPG.Config.Network.Lan >set ipaddress A.B.C.D
```

```
IPG.Config.Network.Lan >no set ipaddress

IPG.Config.Network.Lan >se ipa A.B.C.D
IPG.Config.Network.Lan >no se ipa
```

Argument Description

A.B.C.D	IP address.

19.2.3 Setting the Subnet Mask of the LAN Interface

The **set ipnetmask** command, in LAN Configuration mode, sets the subnet mask of the LAN interface. The **no** form of the command removes the subnet mask.

Command Syntax

```
IPG.Config.Network.Lan >set ipnetmask A.B.C.D
IPG.Config.Network.Lan >no set ipnetmask

IPG.Config.Network.Lan >se ipn A.B.C.D
IPG.Config.Network.Lan >no se ipn
```

Argument Description

A.B.C.D	IP network mask.

19.3 LAN Displaying Commands

Table 19-3 lists the LAN displaying commands.

Table 19-3: The Available LAN Displaying Commands

Command	Description
show all	Displays the entire LAN configuration.
show ipaddress	Displays the IP address of the LAN interface.

Command	Description
show ipnetmask	Displays the subnet mask of the LAN interface.

19.3.1 Displaying all the LAN Configuration

The **show all** command, in LAN Configuration mode, displays the entire LAN configuration.

Command Syntax

```
IPG.Config.Network.Lan >show all

IPG.Config.Network.Lan >sh all
```

Example

```
IPG.Config.Network.Lan >show all
IPG.Config.Network.Lan >
IPG.Config.Network.Lan > ipaddress|ipa           = 192.168.100.1
IPG.Config.Network.Lan > ipnetmask|ipn           = 255.255.255.0
```

19.3.2 Displaying the IP Address of the LAN Interface

The **show ipaddress** command, in LAN Configuration mode, displays the IP address of the LAN interface.

Command Syntax

```
IPG.Config.Network.Lan >show ipaddress

IPG.Config.Network.Lan >sh ipa
```

Example

```
IPG.Config.Network.Lan >show ipaddress
IPG.Config.Network.Lan >
IPG.Config.Network.Lan > ipaddress|ipa           = 192.168.100.1
```

19.3.3 Displaying the Subnet Mask of the LAN Interface

The **show ipnetmask** command, in LAN Configuration mode, displays the Subnet Mask of the LAN interface.

Command Syntax

```
IPG.Config.Network.Lan >show ipnetmask

IPG.Config.Network.Lan >sh ipn
```

Example

```
IPG.Config.Network.Lan >show ipnetmask
IPG.Config.Network.Lan >
```

```
IPG.Config.Network.Lan > ipnetmask|ipn            = 255.255.255.0
```

20 Security Configuration via Telnet

In today's networks security is very important for protecting the Gateway and your local network from hackers.

The following security features are available in the Getaway using the Telnet management interface:

- Advanced security - specifying a list of IP addresses that can manage the Gateway (up to eight IP addresses can be set in the IP address list).
- DHCP security – to receive an IP address and other configuration parameters only from a DHCP server that is listed in the IP address list (up to eight IP addresses can be set in the IP address list).

NOTE **To permit management of the Gateway only to specified stations, you must enter the IP address for each station allowed.**

If no stations are specified, all stations are permitted to manage the Gateway.

20.1 Default Security Configuration

Table 20-1: Default Security Configuration

Parameter	Default Value
Advanced Security	Disabled
DHCP Security	Disabled

20.2 Security Configuration Commands

Table 20-2 lists the security configuration commands.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Table 20-2: The Available Security Configuration Commands

Command	Description
`security`	Enters into Security Configuration mode.

Command	Description
`set advsecurity`	Enables the use of advanced security on secured IP and/or port.
`set dhcpsecurity`	Enables the DHCP security.
`set ip`***N***`address`	Sets the IP address of a station that is permitted to manage the Access 211 Gateway. *N* ranges from 1 to 8.

20.2.1 Entering into Security Configuration Mode

The **security** command, in Global Configuration mode, enters into Security Configuration mode.

The prompt-line that is displayed in response to the command indicates that Security Configuration mode has been entered.

Command Syntax

```
IPG.Config >security
IPG.Config.Security >

IPG.Config >se
IPG.Config.Security >
```

20.2.2 Enabling Advanced Security

The **set advsecurity** command, in Security Configuration mode, enables the use of advanced security on a secured IP. The **no** form of the command disables the advanced security.

By default, the advanced security is disabled.

Command Syntax

```
IPG.Config.Security >set advsecurity {y | n}
IPG.Config.Security >no set advsecurity

IPG.Config.Security >se a {y | n}
IPG.Config.Security >no se a
```

Argument Description

y	Enables advanced security.
n	Disables advanced security.

20.2.3 Enabling DHCP Security

The **set dhcpsecurity** command, in Security Configuration mode, enables the DHCP security. The **no** form of the command disables the DHCP security.

Select this option to enable the Access 211 Gateway, when in DHCP mode, to receive an IP address and other configuration parameters from a DHCP server only if it is listed in the IP address list.

For more information regarding the DHCP protocol, see Understanding DHCP.

By default, the DHCP security is disabled.

Command Syntax

```
IPG.Config.Security >set dhcpsecurity {y | n}
IPG.Config.Security >no set dhcpsecurity

IPG.Config.Security >se d {y | n}
IPG.Config.Security >no se d
```

Argument Description

y	Enables DHCP security.
n	Disables DHCP security.

20.2.4 Setting Management IP Addresses

Optionally, up to eight IP addresses can be set for stations that are permitted to manage the Access 211 Gateway. To set the IP addresses, use the **set ip1address**, **set ip2address**, … **set ip8address** commands, in Security Configuration mode, as required. The **no** form of this command removes the corresponding configured IP address.

Command Syntax

```
IPG.Config.Security >set ipNaddress A.B.C.D
IPG.Config.Security >no set ipNaddress

IPG.Config.Security >se ipN A.B.C.D
IPG.Config.Security >no se ipN
```

Argument Description

N	Sequential number of IP address, ranging from 1 to 8
A.B.C.D	Management IP Address *N*.

Example

```
IPG.Config.Security >set ip3address 10.2.71.74
```

20.3 Security Displaying Commands

Table 20-3 lists the security displaying commands.

Table 20-3: The Available Security Displaying Commands

Command	Description
`show all`	Displays all the security parameters.
`show advsecurity`	Displays the status of advanced security on secured IP and/or port.
`show dhcpsecurity`	Displays the DHCP security status.
`show ip`***N***`address`	Displays the IP address of a station that is permitted to manage the Access 211 Gateway.

20.3.1 Displaying all the Security Parameters

The **show all** command, in Global Configuration mode, displays all the security parameters.

Command Syntax

```
IPG.Config.Security >show all

IPG.Config.Security >sh all
```

Example

```
IPG.Config.Security >show all

IPG.Config.Security >
IPG.Config.Security > advsecurity     |a    =
IPG.Config.Security > dhcpsecurity    |d    =
IPG.Config.Security > ip1address=
IPG.Config.Security > ip2address=
IPG.Config.Security > ip3address=  192.168.100.3
IPG.Config.Security > ip4address=
IPG.Config.Security > ip5address=
IPG.Config.Security > ip6address=
IPG.Config.Security > ip7address=
IPG.Config.Security > ip8address=
```

20.3.2 Displaying the Advanced Security Status

The **show advsecurity** command, in Security Configuration mode, displays the status of advanced security on secured IP and/or port.

Command Syntax

```
IPG.Config.Security >show advsecurity

IPG.Config.Security >sh a
```

Example

```
IPG.Config.Security >show advsecurity
IPG.Config.Security >
IPG.Config.Security > advsecurity     |a    =
```

20.3.3 Displaying the DHCP Security Status

The **show dhcpsecurity** command, in Security Configuration mode, displays the DHCP security status.

Command Syntax

```
IPG.Config.Security >show dhcpsecurity

IPG.Config.Security >sh d
```

Example

```
IPG.Config.Security >show advsecurity
IPG.Config.Security >
IPG.Config.Security > advsecurity     |a    =
```

20.3.4 Displaying the Management IP Addresses

The **show ip***N***address** command, in Security Configuration mode, displays the IP address of a station that has been configured with the corresponding **set ip***N***address** command, to be permitted to manage the Access 211 Gateway. If the corresponding IP address has not been configured, the command displays an empty field (e.g., "ip4address= ").

Command Syntax

```
IPG.Config.Security >show ipNaddress

IPG.Config.Security >sh ipN
```

Example

```
IPG.Config.Security >show ip3address

IPG.Config.Security >
IPG.Config.Security > ip3address=  192.168.100.3
```

21 HTTP Configuration via Telnet

Blocking the Gateway management via Telnet is possible for HTTP.

21.1 Default HTTP Configuration

Table 21-1: Default HTTP Configuration

Parameter	Default Value
Configuration via HTTP	Enabled

21.2 HTTP Configuration Commands

Table 21-2 lists the HTTP (Hypertext Transfer Protocol) configuration commands.

NOTE After entering and saving all configurations, you MUST reset the Gateway.

Table 21-2: The Available HTTP Configuration Commands

Command	Description
`http`	Enters into HTTP Configuration mode.
`set`	Enables/disables configuration via HTTP.

21.2.1 Entering into HTTP Configuration Mode

The **http** command, in Global Configuration mode, enters into HTTP Configuration mode.

The prompt-line that is displayed in response to the command indicates that HTTP Configuration mode has been entered.

Command Syntax

```
IPG.Config >http
IPG.Config.HTTP >

IPG.Config >ht
IPG.Config.HTTP >
```

21.2.2 Enabling/Disabling Configuration via HTTP

The **set** command, in HTTP Configuration mode, enables/disables configuration via HTTP.

By default, configuration via HTTP is enabled.

Command Syntax

```
IPG.Config.HTTP >set {enable | disable}
IPG.Config.HTTP >se {e | d}
```

Argument Description

enable	Enables configuration via HTTP.
disable	Disables configuration via HTTP.

21.3 HTTP Displaying Commands

Table 21-3 lists the HTTP displaying commands.

Table 21-3: The Available HTTP Displaying Commands

Command	Description
show	Displays the HTTP configuration status.

21.3.1 Displaying the HTTP Configuration Status

The **show** command, in HTTP Configuration mode, displays the HTTP configuration status.

Command Syntax

```
IPG.Config.HTTP >show
IPG.Config.HTTP >sh
```

Example

```
IPG.Config.HTTP >show
IPG.Config.HTTP > HTTP = enable
```

22 Configuring VLANs via Telnet

NOTE VLANs temporarily cannot be activated in the current version.

VLAN (Virtual Local Area Network) logically group a set of stations to communicate as if they were on the same LAN segment. Traffic between VLANs is restricted. Unicast and broadcast traffic is forwarded only to LAN segments of the same VLAN. The Access 211 Gateway enables you to configure up to eight 802.1Q-compatible VLANs. A VLAN is identified by a unique number from 1 to 4095 (VLAN ID). By default, the VLAN configuration is disabled and traffic is free to travel between all EdgeGate ports.

VLAN tagging is required to identify traffic from more than one VLAN on the same port. A "tag" is simply the VLAN identification number (VLAN ID), as specified in the 802.1Q standard. The tag is included in the packets forwarded across the LAN. You can allow the AC-211 to connect to non 802.1Q-compliant devices by adding/removing the tag from packets according to tag definitions in the VLAN configuration table.

The Access 211 Gateway is factory set with VLAN ID default value of 1 assigned to all the ports of the unit. Each port must have a default ID. All packets received on the Access 211 Gateway ports without a VLAN tag will inherit the default VLAN ID of the receiving port as their VLAN ID.

To further refine the VLAN configuration and assign a VLAN per protocol, for frames where the EdgeGate is the source or the destination, use the Voice and Management Services Configuration. The user can assign VLAN and priority tags to outgoing frames. This will help devices such as switches and routers in the LAN to serve the frames with higher priority queues and with lower delays. Service VLANs can be defined also for security reasons.

22.1 Default VLAN Configuration

Table 22-1: Default VLAN Configuration

Parameter	Default Value
Using VLANs	Disabled
Default ports' VLAN ID	1, untagged

22.2 VLAN Configuration Commands

Table 22-2 lists the Virtual LAN (VLAN) configuration commands.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Remember that on the Access 211, the WAN port is Port 2 and on the Access 241, the WAN port is Port 5.

Table 22-2: The Available VLAN Configuration Commands

Command	Description
`vlan`	Enters into VLAN Configuration mode.
`set`	Enables using VLANs.
`create`	Creates a new VLAN.
`delete`	Deletes an existing VLAN.
`addports`	Adds a port list to a VLAN and/or sets the default VLAN for the specified port list.
`remove`	Removes port list from a VLAN.
`management`	Assigns a unique VLAN tag and/or a priority tag to all management packets including ping and voice.
`call`	Assigns a unique VLAN tag and/or a priority tag to the start frames of the VoIP call session.
`rtp`	Assigns a unique VLAN tag and/or a priority tag and/or priority using the ToS (Type of Service) field to the outgoing RTP (Real-time Transport Protocol) frames.

22.2.1 Entering into VLAN Configuration Mode

The **vlan** command, in Global Configuration mode, enters into VLAN Configuration mode.

The prompt-line that is displayed in response to the command indicates that VLAN Configuration mode has been entered.

Command Syntax

```
IPG.Config >vlan
IPG.Config.VLAN >

IPG.Config >v
IPG.Config.VLAN >
```

22.2.2 Enabling Using VLANs

The **set** command, in VLAN Configuration mode, enables using VLANs.

Once the VLAN configuration table is set and the VLANs are enabled, packets received at one of the Gateway's ports will be forwarded only to ports of the same VLAN.

Traffic addressed to the EdgeGate unit (Web management or VoIP protocol frames) will be received and transmitted on any of the defined VLANs.

By default, the VLANs are disabled.

Command Syntax

```
IPG.Config.VLAN >set {enable | disable}
IPG.Config.VLAN >se {e | d}
```

Argument Description

enable	Enables using VLANs.
disable	Disables using VLANs.

22.2.3 Creating a New VLAN

The **create** command, in VLAN Configuration mode, creates a new VLAN..

Command Syntax

```
IPG.Config.VLAN >create VLAN-TAG
IPG.Config.VLAN >cr VLAN-TAG
```

Argument Description

VLAN-TAG	VLAN tag number in the range <1-4095>.

22.2.4 Deleting an Existing VLAN

The **delete** command, in VLAN Configuration mode, deletes an existing VLAN.

Command Syntax

```
IPG.Config.VLAN >delete VLAN-TAG
IPG.Config.VLAN >d VLAN-TAG
```

Argument Description

VLAN-TAG	VLAN tag number in the range <1-4095>.

22.2.5 Adding Ports to a VLAN and Setting the Port's Default VLAN

The **addports** command, in VLAN Configuration mode, adds a port list to a VLAN and/or sets the default VLAN for the specified port list.

Command Syntax

```
IPG.Config.VLAN >addports [default] VLAN-TAG PORT-LIST {t | u}
IPG.Config.VLAN >a [d] VLAN-TAG PORT-LIST {t | u}
```

Argument Description

default	Sets the default VLAN for the port list.
VLAN-TAG	VLAN tag number in the range <1-4095>.
PORT-LIST	The port list in format "1 2" (with a space between the ports).
t	Sets the port list as tagged members in the VLAN.
u	Sets the port list as untagged members in the VLAN.

22.2.6 Removing Ports from a VLAN

The **remove** command, in VLAN Configuration mode, removes a port list from a VLAN.

Command Syntax

```
IPG.Config.VLAN >remove VLAN-TAG PORT-LIST
IPG.Config.VLAN >re VLAN-TAG PORT-LIST
```

Argument Description

VLAN-TAG	VLAN tag number in the range <1-4095>.
PORT-LIST	The port list in format "1 2" (with a blank between the ports).

22.2.7 Assigning VLAN and Priority Tag to the Management Packets

The **management** command, in VLAN Configuration mode, assigns a unique VLAN tag and/or a priority tag to all management packets including ping and voice. The **no** form of the command removes the assigned parameters.

Command Syntax

```
IPG.Config.VLAN >management {vlan <vlan-id> | priority <priority>}
IPG.Config.VLAN >no management {vlan | priority}

IPG.Config.VLAN >m {v <vlan-id> | p <priority>}
IPG.Config.VLAN >no m {v | p}
```

Argument Description

vlan <*vlan-id*>	Sets management VLAN tag in the range <1-4095>.
priority <*priority*>	Sets management VLAN priority in the range <0-7>.

22.2.8 Assigning VLAN and Priority Tag VoIP Call Session Start Frames

The **call** command, in VLAN Configuration mode, assigns a unique VLAN tag and/or a priority tag to the start frames of the VoIP call session. The **no** form of the command removes the assigned parameters.

Command Syntax

```
IPG.Config.VLAN >call {vlan <vlan-id> | priority <priority>}
IPG.Config.VLAN >no call {vlan | priority}

IPG.Config.VLAN >ca {v <vlan-id> | p <priority>}
IPG.Config.VLAN >no ca {v | p}
```

Argument Description

vlan *<vlan-id>*	Sets management VLAN tag in the range <1-4095>.
priority *<priority>*	Sets management VLAN priority in the range <0-7>.

22.2.9 Assigning VLAN, Priority Tag and ToS to the Outgoing RTP Frames

The **rtp** command, in VLAN Configuration mode, assigns a unique VLAN tag and/or a priority tag and/or priority using the ToS (Type of Service) field to the outgoing RTP (Real-time Transport Protocol) frames. The **no** form of the command removes the assigned parameters.

Command Syntax

```
IPG.Config.VLAN >rtp {vlan <vlan-id> | priority <priority> | tos
<tos>}
IPG.Config.VLAN >no rtp {vlan | priority | tos}

IPG.Config.VLAN >rt {v <vlan-id> | p <priority> | t <tos>}
IPG.Config.VLAN >no ca {v | p | t}
```

Argument Description

vlan *<vlan-id>*	Sets management VLAN tag in the range <1-4095>.
priority *<priority>*	Sets management VLAN priority in the range <0-7>.
tos *<tos>*	Sets management ToS value in the range <0-255>.

22.3 VLAN Displaying Commands

Table 22-3 lists the Virtual LAN (VLAN) displaying commands.

Table 22-3: The Available VLAN Displaying Commands

Command	Description
`show vlan`	Displays the VLAN configuration.
`show service`	Displays the service VLAN configuration.

22.3.1 Displaying the VLAN Configuration

The **show vlan** command, in VLAN Configuration mode, displays the VLAN configuration.

Command Syntax

```
IPG.Config.VLAN >show vlan

IPG.Config.VLAN >sh v
```

Example

```
IPG.Config.VLAN >show vlan
IPG.Config.VLAN >
IPG.Config.VLAN >  VLANs [disable]
IPG.Config.VLAN >
IPG.Config.VLAN >         PORT    1    2
IPG.Config.VLAN >
=========================================================
IPG.Config.VLAN > VLAN DEFAULT    1    1
IPG.Config.VLAN >
=========================================================
IPG.Config.VLAN >    1            U    U
```

22.3.2 Displaying the Service VLAN Configuration

The **show service** command, in VLAN Configuration mode, displays the service VLAN configuration.

The command displays the following service VLANs configuration:

- Management VLAN - all management packets including ping and voice.
- RTP Frames - outgoing RTP (Real-time Transport Protocol) frames.
- Call - the start frames of the VoIP call session

Command Syntax

```
IPG.Config.VLAN >show service

IPG.Config.VLAN >sh s
```

Example

```
IPG.Config.VLAN >show service
IPG.Config.VLAN >
```

```
IPG.Config.VLAN >  Service     VLAN  Priority  TOS
IPG.Config.VLAN >  -------     ----  --------  ---

IPG.Config.VLAN >  Management     1
IPG.Config.VLAN >  Call
IPG.Config.VLAN >  RTP
IPG.Config.VLAN >  -------     ----  --------  ---
IPG.Config.VLAN >
```

23 Interface Configuration via Telnet

23.1 Default Interface Configuration

Table 23-1: Default Interface Configuration

Parameter	Default Value
Interface's state	Enabled
Interface's speed mode	Auto-negotiation
Interface's flow control	Disabled

23.2 Interface Configuration Commands

Table 23-2 lists the Interface configuration commands.

NOTE **Changing the Interface configuration does not require reset.**

Remember that on the Access 211, the WAN port is Port 2 and on the Access 241, the WAN port is Port 5.

Table 23-2: The Available Interface Configuration Commands

Command	Description
`interface`	Enters into Interface Configuration mode.
`set state`	Sets the interface's state.
`set duplexspeed`	Sets the interface's duplex speed mode.
`set flowcontrol`	Enables flow control on the interface.

23.2.1 Entering into Interface Configuration Mode

The **interface** command, in Global Configuration mode, enters into Interface Configuration mode.

The prompt-line that is displayed in response to the command indicates that Interface Configuration mode has been entered.

Command Syntax

```
IPG.Config >interface
IPG.Config.Interface >

IPG.Config >in
IPG.Config.Interface >
```

23.2.2 Setting the Interface's State

The **set state** command, in Interface Configuration mode, sets the interface's state. The **no** form of the command restores the interface's state to its default.

By default, the interface's state is enabled.

Command Syntax

```
IPG.Config.Network.Wan >set <port> state {enable | disable}
IPG.Config.Network.Wan >no set <port> state

IPG.Config.Network.Wan >se <port> s {e | d}
IPG.Config.Network.Wan >no se <port> s
```

Argument Description

port	Interface number in the range <1-2> (where 1=LAN, 2=WAN).
enable	Enables interface.
disable	Disables interface.

23.2.3 Setting the Interface's Duplex Speed

The **set duplexspeed** command, in Interface Configuration mode, sets the interface's duplex speed mode. The **no** form of the command restores the interface's duplex speed mode to its default.

By default, the interface's duplex speed mode is auto-negotiation.

Command Syntax

```
IPG.Config.Network.Wan >set <port> duplexspeed {autonegotiate |
half10 | full10 | half100 | full100}
IPG.Config.Network.Wan >no set <port> duplexspeed

IPG.Config.Network.Wan >se <port> d {a | half10 | full10 | half100 |
full100}
IPG.Config.Network.Wan >no se <port> d
```

Argument Description

port	Interface number in the range <1-2> (where 1=LAN, 2=WAN).
autonegotiate	Sets the interface's duplex speed mode to auto-negotiation.
half10	Sets the interface's duplex speed mode to half duplex 10M.

full10	Sets the interface's duplex speed mode to full duplex 10M.
half100	Sets the interface's duplex speed mode to half duplex 100M.
full100	Sets the interface's duplex speed mode to full duplex 100M.

23.2.4 Enabling Flow Control on the Interface

The **set flowcontrol** command, in Interface Configuration mode, enables flow control on the interface. The **no** form of the command restores the flow control status to its default.

By default, the flow control on all interfaces is disabled (off).

Command Syntax

```
IPG.Config.Network.Wan >set <port> flowcontrol {on | off}
IPG.Config.Network.Wan >no set <port> flowcontrol

IPG.Config.Network.Wan >se <port> f {on | of}
IPG.Config.Network.Wan >no se <port> f
```

Argument Description

port	Interface number in the range <1-2> (where 1=LAN, 2=WAN).
on	Enables flow control.
off	Disables flow control.

23.3 Interface Displaying Commands

Table 23-3 lists the Interface displaying commands.

Table 23-3: The Available Interface Displaying Commands

Command	Description
show	Displays the specified interface configuration.
show all	Displays the configuration of all the interfaces.

23.3.1 Displaying the Specified Interface Configuration

The **show** command, in Global Configuration mode, displays the specified interface configuration.

Command Syntax

```
IPG.Config.Interface >show <port>

IPG.Config.Interface >sh <port>
```

Argument	Description
port	Interface number in the range <1-2> (where 1=LAN, 2=WAN).

Example

```
IPG.Config.Interface >show 1
IPG.Config.Interface >
IPG.Config.Interface > Port=1 enable  flow control=off  autonegotiate
```

23.3.2 Displaying the Configuration of all the Interfaces

The **show all** command, in Global Configuration mode, displays the configuration of all the interfaces.

Command Syntax

```
IPG.Config.Interface >show all

IPG.Config.Interface >sh all
```

Example

```
IPG.Config.Interface >show all
IPG.Config.Interface >
IPG.Config.Interface > Port=1 enable   flow control=off autonegotiate
IPG.Config.Interface > Port=2 enable   flow control=off autonegotiate
```

24 Executing Reports via Telnet

The report commands allow you to see the following information:

- the interfaces' statistics;
- the configuration download status.

24.1 Reports Commands

Table 24-1 lists the reports commands.

Table 24-1: The Available Reports Commands

Command	Description
`report`	Enters into Report mode.
`statistics`	Enters into Statistics mode.
`show`	Displays the interfaces' statistics.
`reset`	Clears the interfaces' statistics.
`download`	Enters into Download mode.
`show`	Displays the configuration download status.

24.1.1 Entering into Report Mode

The **report** command, in Enable mode, enters into Report mode.

The prompt-line that is displayed in response to the command indicates that Report mode has been entered.

Command Syntax

```
IPG >report
IPG.Report >

IPG >r
IPG.Report >
```

24.1.2 Entering into Statistics Mode

The **statistics** command, in Report mode, enters into Statistics mode.

The prompt-line that is displayed in response to the command indicates that Statistics mode has been entered.

Command Syntax

```
IPG.Report >statistics
IPG.Report.Statistics >

IPG.Report >s
IPG.Report.Statistics >
```

24.1.3 Displaying the Interfaces' Statistics

The **show** command, in Statistics mode, displays the interfaces' statistics.

The interfaces' parameters that can be displayed are listed in Table 24-2.

Command Syntax

```
IPG.Report.Statistics >show {<port> | all} {<parameter> | all}

IPG.Report.Statistics >sh {<port> | all} {<parameter> | all}
```

Argument Description

<port> | **all**	Displays the interface statistics. The port range is <1-2> (where 1=LAN, 2=WAN). For displaying the statistics of all the interfaces, use the **all** keyword.
<parameter> | **all**	Displays the statistics for the specified parameters by the parameter number listed in Table 24-2. For displaying the statistics of all the parameters, use the **all** keyword.

Example

```
IPG.Report.Statistics >show 2 all
IPG.Report.Statistics >
IPG.Report.Statistics > Port=2 100TX      Link=Up
DuplexSpeed=full100
IPG.Report.Statistics > 1|RxOctets=122567112
IPG.Report.Statistics > 2|TxOctets=39460353
IPG.Report.Statistics > 3|RxPackets=433391
IPG.Report.Statistics > 4|TxPackets =86278
IPG.Report.Statistics > 5|RxTotalOctets=0
IPG.Report.Statistics > 6|RxTotalPackets=0
IPG.Report.Statistics > 7|RxBroadcastPackets=370807
IPG.Report.Statistics > 8|RxMulticastPackets=0
IPG.Report.Statistics > 9|RxCrcErrors=0
IPG.Report.Statistics > 10|RxOverSize=0
IPG.Report.Statistics > 11|RxFragments=0
IPG.Report.Statistics > 12|RxJabber=0
IPG.Report.Statistics > 13|RxCollision=0
IPG.Report.Statistics > 14|RxLateCollisionPackets=0
IPG.Report.Statistics > 15|64_Packets=0
```

```
IPG.Report.Statistics > 16|65_127_Packets=1024500
IPG.Report.Statistics > 17|128_255_Packets=40713
IPG.Report.Statistics > 18|256_511_Packets=126066
IPG.Report.Statistics > 19|512_1023_Packets=51354
IPG.Report.Statistics > 20|1024_1522_Packets=46
IPG.Report.Statistics > 21|RxMacErrorPackets=0
IPG.Report.Statistics > 22|DroppedPackets=0
IPG.Report.Statistics > 23|TxMulticastPackets=0
IPG.Report.Statistics > 24|TxBroadcastPackets=416
IPG.Report.Statistics > 25|RxUnderSizePackets=0
IPG.Report.Statistics > 26|link=Up
IPG.Report.Statistics > 27|duplexspeed=full100
IPG.Report.Statistics > 28|Type=100BaseTX
IPG.Report.Statistics > 29|ExtendedType=100BaseTX
```

Table 24-2: Interface Statistics Parameters

Parameter Number (to be used in the *show* command	Parameter Name	Description
1	RxOctets	This counter is incremented once for every received byte.
2	TxOctets	This counter is incremented once for every sent byte.
3	RxPackets	This counter is incremented once for every received frame.
4	TxPackets	This counter is incremented once for every sent frame.
5	RxTotalOctets	N/A
6	RxTotalPackets	N/A
7	RxBroadcastPackets	This counter is incremented once for every received broadcast frame.
8	RxMulticastPackets	This counter is incremented once for every received multicast frame.
9	RxCrcErrors	N/A
10	RxOverSize	N/A
11	RxFragments	N/A
12	RxJabber	N/A
13	RxCollision	N/A
14	RxLateCollisionPackets	N/A
15	64_Packets	This counter is incremented once for every received and transmitted packet that is 64 bytes in size. This counter includes rejected, received, and

Parameter Number (to be used in the *show* command	Parameter Name	Description
		transmitted packets.
16	65_127_Packets	This counter is incremented once for every received and transmitted packet that is 65 to 127 bytes in size. This counter includes rejected, received, and transmitted packets.
17	128_255_Packets	This counter is incremented once for every received and transmitted packet that is 128 to 255 bytes in size. This counter includes rejected, received, and transmitted packets.
18	256_511_Packets	This counter is incremented once for every received and transmitted packet that is 256 to 511 bytes in size. This counter includes rejected, received, and transmitted packets.
19	512_1023_Packets	This counter is incremented once for every received and transmitted packet that is 512 to 1023 bytes in size. This counter includes rejected, received, and transmitted packets.
20	1024_1522_Packets	This counter is incremented once for every received and transmitted packet that is 1024 to MaxFrameSize bytes (1518) in size. This counter includes rejected, received, and transmitted packets.
21	RxMacErrorPackets	N/A
22	DroppedPackets	N/A
23	TxMulticastPackets	Number of Multicast packets sent. This counter does not include Broadcast packets.
24	TxBroadcastPackets	Number of Broadcast packet sent.
25	RxUnderSizePackets	N/A
26	link	The link status (Up/Down).
27	duplexspeed	The interface duplex mode (HALF/FULL and line speed (10/100 Mbps).
28	Type	The interface type (e.g. 100BaseTX).

Parameter Number (to be used in the *show* command	Parameter Name	Description
29	extendedtype	N/A

24.1.4 Clearing the Interfaces' Statistics

The **reset** command, in Statistics mode, clears the interfaces' statistics.

Command Syntax

```
IPG.Report.Statistics >reset {<port> | all} {<counter> | all}

IPG.Report.Statistics >r {<port> | all} {<counter> | all}
```

Argument Description

<*port*> | **all**	Clears the interface statistics, the port range is <1-2> (where 1=LAN, 2=WAN). For clearing all the interfaces statistics use the **all** keyword.
<*counter*> | **all**	Clears the statistics for the specified counters by the counter number listed in Table 24-2. For clearing all the counters statistics use the **all** keyword.

24.1.5 Entering into Download Mode

The **download** command, in Report mode, enters into Download mode.

The prompt-line that is displayed in response to the command indicates that Download mode has been entered.

Command Syntax

```
IPG.Report >download
IPG.Report.Download >

IPG.Report >d
IPG.Report.Download >
```

24.1.6 Displaying the Configuration Download Status

The **show** command, in Report mode, displays the configuration download status.

Command Syntax

```
IPG.Report.Download >show

IPG.Report.Download >sh
```

Example

```
IPG.Report.Download >show
IPG.Report.Download > Download Session Configuration Summary
IPG.Report.Download > ====================================
IPG.Report.Download > Overall Status            = done
IPG.Report.Download > IP TFTP Server            = 10.2.171.203
IPG.Report.Download > Update Type               = auto
IPG.Report.Download >
IPG.Report.Download > *** Root Configuration Update ***
IPG.Report.Download > File            = ipg_211s.cfg
IPG.Report.Download > Status          = done
IPG.Report.Download >
IPG.Report.Download > *** Loader Download ***
IPG.Report.Download > File            = upgr_211_4_55_23.rom
IPG.Report.Download > Version         = 4.55.23
IPG.Report.Download > Status          = done
IPG.Report.Download >
IPG.Report.Download > *** Application Download ***
IPG.Report.Download > File            = sip_211_4_55_23.rom
IPG.Report.Download > SIP   Version   = 4.55.23
IPG.Report.Download > Status          = done
```

25 Protocol H.323 Configuration via Telnet

H.323 is a standard approved by the International Telecommunication Union (ITU) to promote compatibility in videoconference transmissions over IP networks. H.323 was originally promoted as a way to provide consistency in audio, video and data packet transmissions in the event that a Local Area Network (LAN) did not provide Guaranteed Service Quality (QoS).

If the Gateway has H.323 installed you need to configure the Gatekeeper IP address and other H.323 parameters with the CLI configuration.

25.1 Default H.323 Configuration

Table 25-1: Default H.323 Configuration

Parameter	Default Value
Dial plan	>#|[2-9]xxxxxxxxx|1[2-9]xxxxxxxxx|x.T
Caller ID	FSK

25.2 H.323 Configuration Commands

Table 25-2 lists the H.323 configuration commands.

Table 25-2: The Available H.323 Configuration Commands

Command	Description
`h323`	Enters into H.323 configuration mode.
`set gatekeeperip`	Sets the gatekeeper IP address.
`set dialplan`	Sets the dial plan matching string.
`set 1number`	Sets the phone number of line 1.
`set 2number`	Sets the phone number of line 2.
`set 1cidname`	Sets the caller ID for line 1.
`set 2cidname`	Sets the caller ID for line 2.

25.2.1 Entering into H.323 Configuration Mode

The **h323** command, in Global Configuration mode, enters into H.323 Configuration mode.

The prompt-line that is displayed in response to the command indicates that H.323 Configuration mode has been entered.

Command Syntax

```
IPG.Config >h323
IPG.Config.H323 >

IPG.Config >h3
IPG.Config.H323 >
```

25.2.2 Setting the Gatekeeper IP Address

The **set gatekeeperip** command, in H.323 Configuration mode, sets the gatekeeper IP address. The **no** form of the command removes the gatekeeper IP address.

The gatekeeper IP address must be set.

Command Syntax

```
IPG.Config.H323 >set gatekeeperip A.B.C.D
IPG.Config.H323 >no set gatekeeperip A.B.C.D

IPG.Config.H323 >se g A.B.C.D
IPG.Config.H323 >no se g A.B.C.D
```

Argument Description

A.B.C.D	The gatekeeper IP address.

25.2.3 Setting the Dial Plan Matching String

The **set dialplan** command, in H.323 Configuration mode, sets the dial plan matching string. The **no** form of the command removes the dial plan.

For more information regarding the dial plan refer to Using the Dial Plan for SIP, H.323 and PSTN.

By default, the dial plan is >#|[2-9]xxxxxxxxx|1[2-9]xxxxxxxxx|x.T.

Command Syntax

```
IPG.Config.H323 >set dialplan STRING
IPG.Config.H323 >no set dialplan

IPG.Config.H323 >se d STRING
IPG.Config.H323 >no se d
```

Argument Description

STRING	Dial plan matching string.

25.2.4 Setting the Phone Number of Line 1

The **set 1number** command, in H.323 Configuration mode, sets the phone number of line 1. The **no** form of the command removes the phone number of line 1.

Command Syntax

```
IPG.Config.H323 >set 1number <number>
IPG.Config.H323 >no set 1number

IPG.Config.H323 >se 1n <number>
IPG.Config.H323 >no se 1n
```

Argument Description

number	Phone number of line 1.

25.2.5 Setting the Phone Number of Line 2

The **set 2number** command, in H.323 Configuration mode, sets the phone number of line 2. The **no** form of the command removes the phone number of line 2.

Command Syntax

```
IPG.Config.H323 >set 2number <number>
IPG.Config.H323 >no set 2number

IPG.Config.H323 >se 2n <number>
IPG.Config.H323 >no se 2n
```

Argument Description

number	Phone number of line 2.

25.2.6 Setting the Caller ID for Line 1

The **set 1cidname** command, in H.323 Configuration mode, sets the caller ID for line 1. The **no** form of the command removes the caller ID for line 1.

Set the "Name" you want to show on the called party's Caller ID display. When you make a call from a line of the Gateway with the Caller ID inserted, the remote called party will receive this string.

By default, the Gateway US version is factory set to FSK (Bellcore) CID.

Command Syntax

```
IPG.Config.H323 >set 1cidname STRING
IPG.Config.H323 >no set 1cidname

IPG.Config.H323 >se 1c STRING
IPG.Config.H323 >no se 1c
```

Argument	Description
STRING	Caller ID for line 1.

25.2.7 Setting the Caller ID for Line 2

The **set 2cidname** command, in H.323 Configuration mode, sets the caller ID for line 2. The **no** form of the command removes the caller ID for line 2.

Set the "Name" you want to show on the called party's Caller ID display. When you make a call from a line of the Gateway with the Caller ID inserted, the remote called party will receive this string.

By default, the Gateway US version is factory set to FSK (Bellcore) CID.

Command Syntax

```
IPG.Config.H323 >set 2cidname STRING
IPG.Config.H323 >no set 2cidname

IPG.Config.H323 >se 2c STRING
IPG.Config.H323 >no se 2c
```

Argument	Description
STRING	Caller ID for line 2.

25.3 H.323 Displaying Commands

Table 25-3 lists the H.323 displaying commands.

Table 25-3: The Available H.323 Displaying Commands

Command	Description
show all	Displays the entire H.323 configuration.
show gatekeeperip	Displays the gatekeeper IP address.
show dialplan	Displays the dial plan matching string.
show 1number	Displays the phone number of line 1.
show 2number	Displays the phone number of line 2.
show 1cidname	Displays the caller ID for line 1.
show 2cidname	Displays the caller ID for line 2.

25.3.1 Displaying all the H.323 Configuration

The **show all** command, in H.323 Configuration mode, displays the entire H.323 configuration.

Command Syntax

```
IPG.Config.H323 >show all
IPG.Config.H323 >sh all
```

25.3.2 Displaying the Gatekeeper IP Address

The **show gatekeeperip** command, in H.323 Configuration mode, displays the gatekeeper IP address.

Command Syntax

```
IPG.Config.H323 >show gatekeeperip
IPG.Config.H323 >sh g
```

25.3.3 Displaying the Dial Plan Matching String

The **show dialplan** command, in H.323 Configuration mode, displays the dial plan matching string.

Command Syntax

```
IPG.Config.H323 >show dialplan
IPG.Config.H323 >sh d
```

25.3.4 Displaying the Phone Number of Line 1

The **show 1number** command, in H.323 Configuration mode, displays the phone number of line 1.

Command Syntax

```
IPG.Config.H323 >show 1number
IPG.Config.H323 >sh 1n
```

25.3.5 Displaying the Phone Number of Line 2

The **show 2number** command, in H.323 Configuration mode, displays the phone number of line 2.

Command Syntax

```
IPG.Config.H323 >show 2number
```

```
IPG.Config.H323 >sh 2n
```

25.3.6 Displaying the Caller ID for Line 1

The **show 1cidname** command, in H.323 Configuration mode, displays the caller ID for line 1.

Command Syntax

```
IPG.Config.H323 >show 1cidname
IPG.Config.H323 >sh 1c
```

25.3.7 Displaying the Caller ID for Line 2

The **show 2cidname** command, in H.323 Configuration mode, displays the caller ID for line 2.

Command Syntax

```
IPG.Config.H323 >show 2cidname STRING
IPG.Config.H323 >sh 2c STRING
```

26 Protocol MGCP Configuration via Telnet

The MGCP (Media Gateway Control Protocols) is designed to control Telephony Gateways from external call control elements called media gateway controllers or call agents. A telephony gateway is a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks.

If the Gateway has MGCP installed you need to configure the Call Agent IP address and other MGCP parameters with Telnet.

26.1 Default MGCP Configuration

Table 26-1: Default MGCP Configuration

Parameter	Default Value
Call Agent Address	Obtained from a DNS server
Call Agent port	2427
Endpoint domain name	Gateway's IP address

26.2 MGCP Configuration Commands

Table 26-2 lists the MGCP configuration commands.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Table 26-2: The Available MGCP Configuration Commands

Command	Description
`mgcp`	Enters into MGCP Configuration mode.
`set addresscallagent`	Sets the IP address of the call agent.
`set portcallagent`	Sets the port number of the call agent.
`set endpointdomain`	Sets the endpoint domain name.

26.2.1 Entering into MGCP Configuration Mode

The **mgcp** command, in Global Configuration mode, enters into MGCP Configuration mode.

The prompt-line that is displayed in response to the command indicates that MGCP Configuration mode has been entered.

Command Syntax

```
IPG.Config >mgcp
IPG.Config.Mgcp>

IPG.Config >m
IPG.Config.Mgcp >
```

26.2.2 Setting the Call Agent's IP Address

The **set addresscallagent** command, in MGCP Configuration mode, sets the IP address of the call agent. The **no** form of the command removes the call agent's IP address.

By default, the call agent's IP address is obtained from a DNS server.

Command Syntax

```
IPG.Config.Mgcp >set addresscallagent A.B.C.D
IPG.Config.Mgcp >no addresscallagent

IPG.Config.Mgcp >se a A.B.C.D
IPG.Config.Mgcp >no set a
```

Argument Description

A.B.C.D	The IP address of the MGCP call agent.

26.2.3 Setting the Call Agent's Port

The **set portcallagent** command, in MGCP Configuration mode, sets the port number of the call agent. The **no** form of the command restores the call agent's port number to its default value.

By default, the call agent's port number is 2427.

Command Syntax

```
IPG.Config.Mgcp >set portcallagent <port>
IPG.Config.Mgcp >no portcallagent

IPG.Config.Mgcp >se a <port>
IPG.Config.Mgcp >no set p
```

Argument Description

port	The port number of the MGCP call agent.

26.2.4 Setting the Endpoint Domain Name

The **set endpointdomain** command, in MGCP Configuration mode, sets the endpoint domain name. The **no** form of the command removes the endpoint domain name.

By default, the endpoint domain name is the Gateway's IP address.

Command Syntax

```
IPG.Config.Mgcp >set endpointdomain STRING
IPG.Config.Mgcp >no endpointdomain

IPG.Config.Mgcp >se e STRING
IPG.Config.Mgcp >no set e
```

Argument Description

STRING	The endpoint domain name.

26.3 MGCP Displaying Commands

Table 26-3 lists the MGCP displaying commands.

Table 26-3: The Available MGCP Displaying Commands

Command	Description
show all	Displays all the MGCP parameters.
show addresscallagent	Displays the IP address of the call agent.
show portcallagent	Displays the port number of the call agent.
show endpointdomain	Displays the endpoint domain name.
phone-line	Displays the phone line status.

26.3.1 Displaying the Call Agent's IP Address

The **show all** command, in MGCP Configuration mode, displays all the MGCP parameters.

Command Syntax

```
IPG.Config.Mgcp >show all

IPG.Config.Mgcp >sh all
```

Example

```
IPG.Config.Mgcp >show all
IPG.Config.Mgcp >
IPG.Config.Mgcp > addresscallagent|a  = 10.2.11.2
IPG.Config.Mgcp > portcallagent|p     = 1212
IPG.Config.Mgcp > endpointdomain|e    =
```

26.3.2 Displaying the Call Agent's IP Address

The **show addresscallagent** command, in MGCP Configuration mode, displays the IP address of the call agent.

Command Syntax

```
IPG.Config.Mgcp >show addresscallagent

IPG.Config.Mgcp >sh a
```

Example

```
IPG.Config.Mgcp >show addresscallagent
IPG.Config.Mgcp >
IPG.Config.Mgcp > addresscallagent|a  = 10.2.11.2
```

26.3.3 Displaying the Call Agent's Port

The **show portcallagent** command, in MGCP Configuration mode, displays the port number of the call agent.

Command Syntax

```
IPG.Config.Mgcp >show portcallagent

IPG.Config.Mgcp >sh p
```

Example

```
IPG.Config.Mgcp >show portcallagent
IPG.Config.Mgcp >
IPG.Config.Mgcp > portcallagent|p     = 1212
```

26.3.4 Displaying the Endpoint Domain Name

The **show endpointdomain** command, in MGCP Configuration mode, displays the endpoint domain name.

Command Syntax

```
IPG.Config.Mgcp >show endpointdomain

IPG.Config.Mgcp >sh e
```

Example

```
IPG.Config.Mgcp >show endpointdomain
IPG.Config.Mgcp >
IPG.Config.Mgcp > endpointdomain|e    =
```

26.3.5 Displaying the Phone line Status

The **phone-line** command, in MGCP Configuration mode, displays the phone line status.

Command Syntax

```
IPG.Config.Mgcp >phone-line

IPG.Config.Mgcp >p
```

Example

```
IPG.Config.Mgcp >phone-line 1
IPG.Config.Mgcp>
IPG.Config.Mgcp>***LocalEndpointName: aaln/1@62.90.104.43 ***
IPG.Config.Mgcp > Registered=Yes
IPG.Config.Mgcp > Endpoint State=Normal mode - process events
IPG.Config.Mgcp > Event states=on hook
IPG.Config.Mgcp > Capabilities:  PCMU
IPG.Config.Mgcp > Call Active =No
IPG.Config.Mgcp >
```

27 Protocol SIP Configuration via Telnet

The SIP (Session Initiation Protocol) is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality.

If the Gateway has SIP installed you must configure the SIP Server IP address and other SIP parameters.

Set the SIP server settings, NAT settings and STUN server settings according to the way the Gateway is connected to the network:

- If the Gateway does not reside behind a NAT server and has an outbound (global) IP address you only need to set the SIP Server's *IP address*, *port* and *domain name*.
- If the Gateway resides behind a NAT server and wishes to communicate with the SIP server via a ***Proxy*** server:
  - Set the *SIP server IP address* and p*ort* to the values of the Proxy server's IP address and port.
  - Set the *domain name* to the SIP Server's Domain name.
- If the Gateway resides behind a NAT server and wishes to communicate with the SIP server using ***STUN*** support:
  - Set the SIP server's *IP address*, p*ort* and *domain name* to the values of the SIP server's IP address, port and domain name.
  - Set the ***STUN*** Server's *IP address* and *port* to the IP and port of the STUN server.
- If the Gateway resides behind a NAT server and the outbound (global) IP is ***Static*** the Gateway could be configured to use the outbound (global) IP also for the SIP protocol.
  - Set the SIP server's *IP address*, p*ort* and *domain name* to the values of the SIP server's IP address, port and domain name.
  - Set the *NAT IP address* to the value of the Gateway's outbound IP address.

For more information regarding the NAT protocol see Understanding NAT and NAPT.

27.1 Default SIP Configuration

Table 27-1: Default SIP Configuration

Parameter	Default Value
SIP server port number for line 1	5060
SIP server port number for line 2	5061
Dial plan	|[2-9]xxxxxxxxx|1[2-9]xxxxxxxxx|x.T|>#
RTP/RTPC NAT port base	16384
Support PRACK method with provisional response reliability	Disabled
SIP Registration Timer value	1800 seconds
SIP call control transport protocol	UDP

27.2 SIP Configuration Commands

Table 27-2 lists the SIP (Session Initiation Protocol) configuration commands.

NOTE **After entering and saving all configurations, you MUST reset the Gateway.**

Table 27-2: The Available SIP Configuration Commands

Command	Description
`sip`	Enters into SIP (Session Initiation Protocol) Configuration mode.
`set sipserver_ip`	Sets the SIP server's IP address.
`set sipport`	Sets the SIP server's port number.
`set domain_name`	Sets the SIP server's domain name.
`set sendreg`	Enables/disables sending REGISTER request.
`set dialplan`	Sets the dial plan matching string.
`set transport`	Sets the SIP call control transport protocol (TCP or UDP).
`set 1number`	Sets the phone number of line 1.
`set 2number`	Sets the phone number of line 2.
`set 1cidname`	Sets the caller ID for line 1.
`set 2cidname`	Sets the caller ID for line 2.

Command	Description
set 1port	Sets the SIP port for line 1.
set 2port	Sets the SIP port for line 2.
set 1aec	Sets the AEC for line 1.
set 2aec	Sets the AEC for line 2.
set 1username	Sets the user name for line 1.
set 2username	Sets the user name for line 2.
set 1password	Sets the password for line 1.
set 2password	Sets the password for line 2.
set nat_ip	Sets the NAT IP address.
set rtp_port	Sets the RTP/RTCP port base.
set stunserver_ip	Sets the STUN server IP address.
set stunport	Sets the STUN server port.

27.2.1 Entering into SIP Configuration Mode

The **sip** command, in Global Configuration mode, enters into SIP (Session Initiation Protocol) Configuration mode.

The prompt-line that is displayed in response to the command indicates that SIP Configuration mode has been entered.

Command Syntax

```
IPG.Config >sip
IPG.Config.SIP >

IPG.Config >si
IPG.Config.SIP >
```

27.2.2 Setting the SIP Server's IP Address

The **set sipserver_ip** command, in SIP Configuration mode, sets the SIP server's IP address. The **no** form of the command removes the SIP server's IP address.

If a Domain name is entered for the SIP Server IP, DNS requests will be done to acquire the IP and port of the Server.

Command Syntax

```
IPG.Config.SIP >set sipserver_ip A.B.C.D | <domain-name>
IPG.Config.SIP >no set sipserver_ip
```

```
IPG.Config.SIP >se sips A.B.C.D | <domain-name>
IPG.Config.SIP >no set sips
```

Argument Description

A.B.C.D	SIP server's IP address.
Domain-name	SIP server's Domain name.

27.2.3 Setting the SIP Server's Port Number

The **set sipport** command, in SIP Configuration mode, sets the SIP server's port number. The **no** form of the command sets the SIP server's port number to its default value.

By default, the SIP server's port number is 5060.

Command Syntax

```
IPG.Config.SIP >set sipport <port>
IPG.Config.SIP >no set sipport

IPG.Config.SIP >se sipp <port>
IPG.Config.SIP >no sipp
```

Argument Description

port	Port of SIP Server.

27.2.4 Setting the SIP Server's Domain Name

The **set domain_name** command, in SIP Configuration mode, sets the SIP server's domain name. The **no** form of the command removes the domain name.

Command Syntax

```
IPG.Config.SIP >set domain_name STRING
IPG.Config.SIP >no set domain_name

IPG.Config.SIP >se do STRING
IPG.Config.SIP >no do
```

Argument Description

STRING	Domain name, used in registration as *user@domainname*.

27.2.5 Enabling/Disabling Sending REGISTER Request

The **set sendreg** command, in SIP Configuration mode, enables/disables sending REGISTER requests. The **no** form of the command disables sending REGISTER requests.

Command Syntax

```
IPG.Config.SIP >set sendreg YES|NO
IPG.Config.SIP >no set sendreg

IPG.Config.SIP >se se YES|NO
IPG.Config.SIP >no se
```

Argument Description

YES	Enables sending REGISTER requests.
NO	Disables sending REGISTER requests.

27.2.6 Setting the Dial Plan Matching String

The **set dialplan** command, in SIP Configuration mode, sets the dial plan matching string. The **no** form of the command removes the dial plan.

For more information regarding the dial plan refer to Using the Dial Plan for SIP, H.323 and PSTN.

By default, the dial plan is >#|[2-9]xxxxxxxxx|1[2-9]xxxxxxxxx|x.T.

Command Syntax

```
IPG.Config.SIP >set dialplan STRING
IPG.Config.SIP >no set dialplan

IPG.Config.SIP >se di STRING
IPG.Config.SIP >no di
```

Argument Description

STRING	Dial plan matching string.

27.2.7 Setting the SIP Call Control Transport Protocol

The **set transport** command, in SIP Configuration mode, sets the SIP call control transport protocol (TCP or UDP). The **no** form of the command removes the dial plan.

By default, the SIP call control transport protocol is UDP.

Command Syntax

```
IPG.Config.SIP >set transport STRING
IPG.Config.SIP >no set transport

IPG.Config.SIP >se t STRING
IPG.Config.SIP >no se t
```

Argument Description

STRING	Transport protocol type (TCP or UDP).

27.2.8 Setting the Phone Number of Line 1

The **set 1number** command, in SIP Configuration mode, sets the phone number of line 1. The **no** form of the command removes the phone number of line 1.

Command Syntax

```
IPG.Config.SIP >set 1number <number>
IPG.Config.SIP >no set 1number

IPG.Config.SIP >se 1n <number>
IPG.Config.SIP >no se 1n
```

Argument Description

number	Phone number of line 1.

27.2.9 Setting the Phone Number of Line 2

The **set 2number** command, in SIP Configuration mode, sets the phone number of line 2. The **no** form of the command removes the phone number of line 2.

Command Syntax

```
IPG.Config.SIP >set 2number <number>
IPG.Config.SIP >no set 2number

IPG.Config.SIP >se 2n <number>
IPG.Config.SIP >no se 2n
```

Argument Description

number	Phone number of line 2.

27.2.10 Setting the Caller ID for Line 1

The **set 1cidname** command, in SIP Configuration mode, sets the caller ID for line 1. The **no** form of the command removes the caller ID for line 1.

Set the "Name" you want to show on the called party's Caller ID display. When you make a call from a line of the Gateway with the Caller ID inserted, the remote called party will receive this string.

Command Syntax

```
IPG.Config.SIP >set 1cidname STRING
IPG.Config.SIP >no set 1cidname

IPG.Config.SIP >se 1c STRING
IPG.Config.SIP >no se 1c
```

Argument Description

STRING	Caller ID for line 1.

27.2.11 Setting the Caller ID for Line 2

The **set 2cidname** command, in SIP Configuration mode, sets the caller ID for line 2. The **no** form of the command removes the caller ID for line 2.

Set the "Name" you want to show on the called party's Caller ID display. When you make a call from a line of the Gateway with the Caller ID inserted, the remote called party will receive this string.

By default, the Gateway US version is factory set to FSK (Bellcore) CID.

Command Syntax

```
IPG.Config.SIP >set 2cidname STRING
IPG.Config.SIP >no set 2cidname

IPG.Config.SIP >se 2c STRING
IPG.Config.SIP >no se 2c
```

Argument Description

STRING	Caller ID for line 2.

27.2.12 Setting the SIP Port for Line 1

The **set 1port** command, in SIP Configuration mode, sets the SIP port for line 1. The **no** form of the command restores the SIP port for line 1 to its default value.

Command Syntax

```
IPG.Config.SIP >set 1port STRING
IPG.Config.SIP >no set 1port

IPG.Config.SIP >se 1po STRING
IPG.Config.SIP >no se 1po
```

Argument Description

STRING	SIP port for line 1.

27.2.13 Setting the SIP Port for Line 2

The **set 2port** command, in SIP Configuration mode, sets the SIP port for line 2. The **no** form of the command restores the SIP port for line 2 to its default value.

Command Syntax

```
IPG.Config.SIP >set 2port STRING
IPG.Config.SIP >no set 2port

IPG.Config.SIP >se 2po STRING
IPG.Config.SIP >no se 2po
```

Argument Description

STRING	SIP port for line 2.

27.2.14 Setting the AEC for Line 1

The **set 1aec** command, in SIP Configuration mode, sets the AEC for line 1. The **no** form of the command removes the AEC for line 1.

The AEC (Automatic Echo Cancellation) reduces the amount of feedback the called party hears when the calling party is using a speakerphone.

Command Syntax

```
IPG.Config.SIP >set 1aec STRING
IPG.Config.SIP >no set 1aec

IPG.Config.SIP >se 1a STRING
IPG.Config.SIP >no se 1a
```

Argument Description

STRING	AEC for line 1 (ON or OFF).

27.2.15 Setting the AEC for Line 2

The **set 2aec** command, in SIP Configuration mode, sets the AEC for line 2. The **no** form of the command removes the AEC for line 2.

The AEC (Automatic Echo Cancellation) reduces the amount of feedback the called party hears when the calling party is using a speakerphone.

Command Syntax

```
IPG.Config.SIP >set 2aec STRING
IPG.Config.SIP >no set 2aec

IPG.Config.SIP >se 2a STRING
IPG.Config.SIP >no se 2a
```

Argument Description

STRING	AEC for line 2 (ON or OFF).

27.2.16 Setting the User Name for Line 1

The **set 1username** command, in SIP Configuration mode, sets the user name for line 1. The **no** form of the command removes the user name for line 1.

Command Syntax

```
IPG.Config.SIP >set 1username STRING
IPG.Config.SIP >no set 1username

IPG.Config.SIP >se 1u STRING
IPG.Config.SIP >no se 1u
```

Argument Description

STRING	User Name for line 1.

27.2.17 Setting the User Name for Line 2

The **set 2username** command, in SIP Configuration mode, sets the user name for line 2. The **no** form of the command removes the user name for line 2.

Command Syntax

```
IPG.Config.SIP >set 2username STRING
IPG.Config.SIP >no set 2username

IPG.Config.SIP >se 2u STRING
IPG.Config.SIP >no se 2u
```

Argument Description

STRING	User Name for line 2.

27.2.18 Setting the Password for Line 1

The **set 1password** command, in SIP Configuration mode, sets the password for line 1. The **no** form of the command removes the password for line 1.

Command Syntax

```
IPG.Config.SIP >set 1password STRING
IPG.Config.SIP >no set 1password

IPG.Config.SIP >se 1pa STRING
IPG.Config.SIP >no se 1pa
```

Argument Description

STRING	Password for line 1.

27.2.19 Setting the Password for Line 2

The **set 1password** command, in SIP Configuration mode, sets the password for line 2. The **no** form of the command removes the password for line 2.

Command Syntax

```
IPG.Config.SIP >set 2password STRING
IPG.Config.SIP >no set 2password

IPG.Config.SIP >se 2pa STRING
IPG.Config.SIP >no se 2pa
```

Argument Description

STRING	Password for line 2.

27.2.20 Setting the NAT IP Address

The **set nat_ip** command, in SIP Configuration mode, sets the NAT IP address. The **no** form of the command removes the NAT IP address.

Command Syntax

```
IPG.Config.SIP >set nat_ip A.B.C.D
IPG.Config.SIP >no set nat_ip

IPG.Config.SIP >se n A.B.C.D
IPG.Config.SIP >no se n
```

Argument Description

A.B.C.D	NAT IP address.

27.2.21 Setting the RTP/RTCP Port Base

The **set rtp_port** command, in SIP Configuration mode, sets the RTP/RTCP port base. The **no** form of the command removes the RTP/RTCP port base.

Command Syntax

```
IPG.Config.SIP >set rtp_port NUMBER
IPG.Config.SIP >no set rtp_port

IPG.Config.SIP >se r NUMBER
IPG.Config.SIP >no se r
```

Argument Description

NUMBER	Number of RTP/RTCP port base (Value range is 1-65535; Default is 16384).

27.2.22 Setting the STUN Server IP Address

The **stunserver_ip** command, in SIP Configuration mode, sets the STUN server's IP address. The **no** form of the command removes the STUN server's IP address.

Command Syntax

```
IPG.Config.SIP >set stunserver_ip A.B.C.D
IPG.Config.SIP >no set stunserver_ip

IPG.Config.SIP >se stuns A.B.C.D
IPG.Config.SIP >no se stuns
```

Argument Description

A.B.C.D	STUN server's IP address.

27.2.23 Setting the STUN Server Port

The **set stunport** command, in SIP Configuration mode, sets the STUN server port. The **no** form of the command removes the STUN server port.

Command Syntax

```
IPG.Config.SIP >set stunport NUMBER
IPG.Config.SIP >no set stunport

IPG.Config.SIP >se stunp NUMBER
IPG.Config.SIP >no se stunp
```

Argument Description

NUMBER	Number of port (The value range is 1-65535; the default value is 5678).

27.3 SIP Displaying Commands

Table 27-3 lists the SIP (Session Initiation Protocol) displaying commands.

Table 27-3: The Available SIP Displaying Commands

Command	Description
show all	Displays the entire SIP configuration.
show sipserver_ip	Displays the SIP server's IP address.
show sipport	Displays the SIP server's port number.
show domain_name	Displays the SIP server's domain name.
show sendreg	Displays the sending REGISTER request status.
show dialplan	Displays the dial plan matching string.
show transport	Displays the SIP call control transport protocol.
show 1number	Displays the phone number of line 1.
show 2number	Displays the phone number of line 2.
show 1cidname	Displays the caller ID for line 1.
show 2cidname	Displays the caller ID for line 2.
show 1port	Displays the SIP port for line 1.
show 2port	Displays the SIP port for line 2.
show 1aec	Displays the AEC for line 1.
show 2aec	Displays the AEC for line 2.
show 1username	Displays the user name for line 1.

Command	Description
show 2username	Displays the user name for line 2.
show 1password	Displays the password for line 1.
show 2password	Displays the password for line 2.
show nat_ip	Displays the NAT IP address.
show rtp_port	Displays the RTP/RTCP port base.
show stunserver_ip	Displays the STUN server IP address.
show stunport	Displays the STUN server port.
phone-line	Displays the phone line status.

27.3.1 Displaying all the SIP Configuration

The **show all** command, in Global Configuration mode, displays the entire SIP configuration.

Command Syntax

```
IPG.Config.SIP >show all

IPG.Config.SIP >sh all
```

Example

```
IPG.Config.SIP >show all
IPG.Config.SIP >
IPG.Config.SIP > *** SIP Server Settings ***
IPG.Config.SIP > sipserver_ip   |sips =
IPG.Config.SIP > sipport        |sipp =
IPG.Config.SIP > domain_name    |do =
IPG.Config.SIP > sendreg        |se =
IPG.Config.SIP >
IPG.Config.SIP > *** Gateway Settings ***
IPG.Config.SIP > dialplan       |di = ([2-9]xxxxx|1xxxxxxx|x.T|>#)
IPG.Config.SIP > transport      |t =
IPG.Config.SIP > 1number        |1n    =
IPG.Config.SIP > 2number        |2n    =
IPG.Config.SIP > 1cidname       |1c    =
IPG.Config.SIP > 2cidname       |2c    =
IPG.Config.SIP > 1port          |1po   =
IPG.Config.SIP > 2port          |2po   =
IPG.Config.SIP > 1aec           |1a    =
IPG.Config.SIP > 2aec           |2a    =
IPG.Config.SIP > 1username      |1u    =
IPG.Config.SIP > 2username      |2u    =
IPG.Config.SIP > 1password      |1pa   =
IPG.Config.SIP > 2password      |2pa   =
IPG.Config.SIP >
IPG.Config.SIP > *** NAT Settings ***
IPG.Config.SIP > nat_ip         |n =
IPG.Config.SIP > rtp_port       |r =
IPG.Config.SIP >
IPG.Config.SIP > *** STUN Server Settings ***
IPG.Config.SIP > stunserver_ip  |stuns =
IPG.Config.SIP > stunport       |stunp =
```

27.3.2 Displaying the SIP Server's IP Address

The **show sipserver_ip** command, in SIP Configuration mode, displays the SIP server's IP address.

Command Syntax

```
IPG.Config.SIP >show sipserver_ip

IPG.Config.SIP >sh sips
```

Example

```
IPG.Config.SIP >show sipserver_ip
IPG.Config.SIP >
IPG.Config.SIP > sipserver_ip   |sips =
```

27.3.3 Displaying the SIP Server's Port Number

The **show sipport** command, in SIP Configuration mode, displays the SIP server's port number.

Command Syntax

```
IPG.Config.SIP >show sipport

IPG.Config.SIP >show sipp
```

Example

```
IPG.Config.SIP >show sipport
IPG.Config.SIP >
IPG.Config.SIP > sipport        |sipp =
```

27.3.4 Displaying the SIP Server's Domain Name

The **show domain_name** command, in SIP Configuration mode, displays the SIP server's domain name.

Command Syntax

```
IPG.Config.SIP >show domain_name

IPG.Config.SIP >sh do
```

Example

```
IPG.Config.SIP >show domain_name
IPG.Config.SIP >
IPG.Config.SIP > domain_name    |do =
```

27.3.5 Displaying the Sending REGISTER Request Status

The **show sendreg** command, in SIP Configuration mode, displays the sending REGISTER request status.

Command Syntax

```
IPG.Config.SIP >show sendreg

IPG.Config.SIP >sh se
```

Example

```
IPG.Config.SIP >show sendreg
IPG.Config.SIP >
IPG.Config.SIP > sendreg        |se =
```

Argument Description

STRING	Send Registration Request (YES or NO).

27.3.6 Displaying the Dial Plan

The **show dialplan** command, in SIP Configuration mode, displays the dial plan matching string.

Command Syntax

```
IPG.Config.SIP >show dialplan

IPG.Config.SIP >sh di
```

Example

```
IPG.Config.SIP >show dialplan
IPG.Config.SIP >
IPG.Config.SIP > dialplan       |di = ([2-9]xxxxx|1xxxxxxx|x.T|>#)
```

27.3.7 Displaying the SIP Call Control Transport Protocol

The **show transport** command, in SIP Configuration mode, displays the SIP call control transport protocol.

Command Syntax

```
IPG.Config.SIP >show transport

IPG.Config.SIP >sh t
```

Example

```
IPG.Config.SIP >show transport
IPG.Config.SIP >
IPG.Config.SIP > transport      |t =
```

27.3.8 Displaying the Phone Number of Line 1

The **show 1number** command, in SIP Configuration mode, displays the phone number of line 1.

Command Syntax

```
IPG.Config.SIP >show 1number <number>

IPG.Config.SIP >sh 1n <number>
```

Example

```
IPG.Config.SIP >show 1number
IPG.Config.SIP >
IPG.Config.SIP > 1number          |1n  =
```

27.3.9 Displaying the Phone Number of Line 2

The **show 2number** command, in SIP Configuration mode, displays the phone number of line 2.

Command Syntax

```
IPG.Config.SIP >show 2number

IPG.Config.SIP >sh 2n
```

Example

```
IPG.Config.SIP >show 2number
IPG.Config.SIP >
IPG.Config.SIP > 2number          |2n  =
```

27.3.10 Displaying the Caller ID for Line 1

The **show 1cidname** command, in SIP Configuration mode, displays the caller ID for line 1.

Command Syntax

```
IPG.Config.SIP >show 1cidname STRING

IPG.Config.SIP >sh 1c STRING
```

Example

```
IPG.Config.SIP >show 1cidname
IPG.Config.SIP >
IPG.Config.SIP > 1cidname       |1c    =
```

27.3.11 Displaying the Caller ID for Line 2

The **show 2cidname** command, in SIP Configuration mode, displays the caller ID for line 2.

Command Syntax

```
IPG.Config.SIP >show 2cidname

IPG.Config.SIP >sh 2c
```

Example

```
IPG.Config.SIP >show 2cidname
IPG.Config.SIP >
IPG.Config.SIP > 2cidname        |2c    =
```

27.3.12 Displaying the SIP Port for Line 1

The **show 1port** command, in SIP Configuration mode, displays the SIP port for line 1.

Command Syntax

```
IPG.Config.SIP >show 1port

IPG.Config.SIP >sh 1po
```

Example

```
IPG.Config.SIP >show 1port
IPG.Config.SIP >
IPG.Config.SIP > 1port           |1po   =
```

27.3.13 Displaying the SIP Port for Line 2

The **show 2port** command, in SIP Configuration mode, displays the SIP port for line 2.

Command Syntax

```
IPG.Config.SIP >show 2port

IPG.Config.SIP >sh 2po
```

Example

```
IPG.Config.SIP >show 2port
IPG.Config.SIP >
IPG.Config.SIP > 2port           |2po   =
```

27.3.14 Displaying the AEC for Line 1

The **show 1aec** command, in SIP Configuration mode, displays the AEC for line 1.

Command Syntax

```
IPG.Config.SIP >show 1aec

IPG.Config.SIP >sh 1a
```

Example

```
IPG.Config.SIP >show 1aec
IPG.Config.SIP >
IPG.Config.SIP > 1aec           |1a    =
```

27.3.15 Displaying the AEC for Line 2

The **show 2aec** command, in SIP Configuration mode, displays the AEC for line 2.

Command Syntax

```
IPG.Config.SIP >show 2aec

IPG.Config.SIP >sh 2a
```

Example

```
IPG.Config.SIP >show 2aec
IPG.Config.SIP >
IPG.Config.SIP > 2aec           |2a    =
```

27.3.16 Displaying the User Name for Line 1

The **show 1username** command, in SIP Configuration mode, displays the user name for line 1.

Command Syntax

```
IPG.Config.SIP >show 1username

IPG.Config.SIP >sh 1u
```

Example

```
IPG.Config.SIP >show 1username
IPG.Config.SIP >
IPG.Config.SIP > 1username      |1u    =
```

27.3.17 Displaying the User Name for Line 2

The **show 2username** command, in SIP Configuration mode, displays the user name for line 2.

Command Syntax

```
IPG.Config.SIP >show 2username

IPG.Config.SIP >sh 2u
```

Example

```
IPG.Config.SIP >show 1username
IPG.Config.SIP >
```

```
IPG.Config.SIP > 2username      |2u    =
```

27.3.18 Showing if a Password for Line 1 Exists

The **show 1password** command, in SIP Configuration mode, shows whether or not a password for Line 1 exists. An existing password is represented by a sequence of asterisks.

Command Syntax

```
IPG.Config.SIP >show 1password

IPG.Config.SIP >sh 1pa
```

Example

```
IPG.Config.SIP >show 1password
IPG.Config.SIP >
IPG.Config.SIP > 1password      |1pa   = *****
```

27.3.19 Showing if a Password for Line 2 Exists

The **show 2password** command, in SIP Configuration mode, shows whether or not a password for Line 2 exists. An existing password is represented by a sequence of asterisks.

Command Syntax

```
IPG.Config.SIP >show 2password

IPG.Config.SIP >sh 2pa
```

Example

```
IPG.Config.SIP >show 2password
IPG.Config.SIP >
IPG.Config.SIP > 2password      |2pa   = *****
```

27.3.20 Displaying the NAT IP Address

The **show nat_ip** command, in SIP Configuration mode, displays the NAT IP address.

Command Syntax

```
IPG.Config.SIP >show nat_ip

IPG.Config.SIP >sh n
```

27.3.21 Displaying the RTP/RTCP Port Base

The **show rtp_port** command, in SIP Configuration mode, displays the RTP/RTCP port base.

Command Syntax

```
IPG.Config.SIP >show rtp_port
```

```
IPG.Config.SIP >sh r
```

27.3.22 Displaying the STUN Server IP Address

The **show stunserver_ip** command, in SIP Configuration mode, displays the STUN server's IP address.

Command Syntax

```
IPG.Config.SIP >show stunserver_ip
IPG.Config.SIP >sh stuns
```

27.3.23 Displaying the STUN Server Port

The **show stunport** command, in SIP Configuration mode, displays the STUN server port.

Command Syntax

```
IPG.Config.SIP >show stunport
IPG.Config.SIP >sh stunp
```

27.3.24 Displaying the Phone-line Status

The **phone-line** command, in SIP Configuration mode, displays the phone line status.

Command Syntax

```
IPG.Config.SIP >phone-line <line>
IPG.Config.SIP >p <line>
```

Argument Description

line	Line number in range <1-2>.

Example

```
IPG.Config.SIP >phone-line 1
IPG.Config.SIP >
IPG.Config.SIP >phone 1
IPG.Config.SIP > Phone number = 435293
IPG.Config.SIP > Registered   = Yes
IPG.Config.SIP > Call Active  = No
IPG.Config.SIP > State        = On Hook
```

27.3.25 Displaying the Phone-line Status for Pulse Metering

When Pulse Metering is active the status of Pulse Metering can be displayed with the Phone-line status command.

28 General Commands Mode

28.1 General Commands

Table 28-1: Available General Commands lists the general commands for rebooting the Gateway, resetting the configuration to the factory defaults and downloading a configuration file or software image.

Table 28-1: Available General Commands

Command	Description
commands	Enters into Commands mode.
reset	Reboots the Gateway.
default	Sets the configuration to the factory defaults.
copy	Downloads a software image or configuration file from a TFTP\HTTP server.
send	Sends information to the Syslog server.
ping	Pings another device from the LAN port.

28.1.1 Entering into Commands Mode

The **commands** command, in Enable mode, enters into Commands mode.

The prompt-line that is displayed in response to the command indicates that Commands mode has been entered.

Command Syntax

```
IPG >commands
IPG.Commands >

IPG >c
IPG.Commands >
```

28.1.2 Rebooting the Gateway

The **reset** command, in Commands mode, reboots the Gateway.
You can reset the gateway or reboot in and to enter the boot loader mode.
When using the **reset** command, the Gateway requests confirmation before rebooting.

Command Syntax

```
IPG.Commands >reset {power | downloader}
IPG.Commands >r {p | d}
```

Argument	Description
power	Resets the gateway.
downloader	Reboots the gateway to the boot loader mode.

Example 1

```
IPG.Commands >reset power
IPG.Commands > Warning! Reset system (y/n) ?
```

Example 2

```
IPG.Commands >reset downloader
IPG.Commands > Warning! Reset system and execute downloader (y/n) ?
```

28.1.3 Setting the Configuration to the Factory Defaults

The default command, in Commands mode, sets the configuration to the factory defaults.

When using the default command, the Gateway requests confirmation before setting the factory defaults.

Command Syntax

```
IPG.Commands >default

IPG.Commands >d
```

Example

```
IPG.Commands >default
IPG.Commands > Warning! Set Default Configuration (y/n) ?
```

28.1.4 Downloading Image or Configuration File Using TFTP\HTTP

The **copy** command, in Commands mode, downloads a software image or configuration file from a TFTP\HTTP server.

Command Syntax

```
IPG.Commands >copy A.B.C.D FILE-NAME

IPG.Commands >c A.B.C.D FILE-NAME
```

Argument Description

Argument	Description
A.B.C.D	IP address of the TFTP\HTTP server.
FILE-NAME	File name to copy.

28.1.5 Sending Data to Syslog via Telnet

28.1.5.1 Uploading the System Configuration to Syslog

The **send config** command, in Commands mode, uploads the system configuration from NVRAM to the Syslog server. The entries will be numbered. The last entry will be marked Total: #*xxx*, where *xxx* is the number of NVRAM entries. If not all entries were received you can repeat the request starting at any entry.

Command Syntax

```
IPG.Commands >send config [START-NUMBER]
IPG.Commands >s c [START-NUMBER]
```

Argument Description

START-NUMBER	Number of entry on NVRAM from which to start or proceed with the upload.

28.1.5.2 Sending SIP RTP Statistics of Active Calls to Syslog

The **send line** command, in Commands mode, displays the SIP RTP Statistics of the Active Call up to the time that the command is executed in the local Telnet screen and also sends SIP RTP Statistics of the Call to the Syslog server.

Command Syntax

```
IPG.Commands >send line [1|2|all]
IPG.Commands >s l [1|2|all]
```

Argument Description

1	Sends statistics for Line 1 only.
2	Sends statistics for Line 2 only.
all	Sends statistics for both lines.

28.1.6 Sending Pings

The **ping** command, in Commands mode, pings another device throught the LAN and WAN ports.

You can use this command to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of the following responses:

- Normal response - The normal response (hostname is alive) occurs within 1 to 10 seconds, depending on network traffic.
- Destination does not respond - If the host does not respond, a “no-response” message is returned.

- Unknown host - If the host does not exist, an "unknown host" message is returned.
- Destination unreachable - If the default gateway cannot reach the specified network, a "destination-unreachable" message is returned.

Command Syntax

```
IPG.Commands > ping <host> [<number>]
IPG.Commands >
IPG.Commands > p <host> [<number>]
IPG.Commands >
```

Argument Description

<host>	Destination host name (using DNS Server) or IP address.
<number>	(Optional). Number of echo packets to send in the range <1-100> (default 5).

29 Using the Gateway

To make a call, a Call Server (Gatekeeper/SIP Server/Call Agent) must be located on the network and visible to all Access 211 Gateway units. Placing a telephone call with the Access 211 Gateway for VoIP is the same as using a telephone with a standard telephone provider. Check with the Call Server's User's Manual for available call features.

29.1 First Call

Place the first call from one phone line to a second phone line on the same Access 211 Gateway unit. This step ensures that the Access 211 Gateway and the Call Server are operating properly and that all configuration information is correct.

29.2 Placing Calls

To place a call:

1. Make sure that all equipment is powered up.

2. Check that the Call Server is running and that all endpoints are registered.

3. Check for a dial tone on each of the Gateway's endpoints (phone lines), registered by the Call Server. A dial tone may not be present until the Gateway is addressed and powered up, the Call Server is running, and the endpoint (phone line) is registered. Keypad Configuration will be active for 10 minutes starting from boot.

4. Place a call using the assigned telephone numbers.

5. Hang up the handset to terminate the call.

29.3 Adding Units to the Network

You can add more Gateway units to the network, following the same procedure that is used to establish the first unit. Additional units can exist anywhere visible to the Call Server and all other Gateway units.

29.4 Advanced Calling Features for SIP

In the following subsections:

- An expression such as "**dial flash** + **7**" implies - "press on **flash**, then press on **7**" (the dialing sequence progresses as read from left to right).
- The Star (or Asterisk) key is represented by the symbol "*****".
- The term ***destination number*** within an expression implies "dial the destination number".

29.4.1 Call Waiting

If you are engaged in a call and another party calls your line, you hear a short tone on your line. The caller hears a ringing tone.

Press **flash** to toggle between calls.

29.4.2 Conference Call

To establish a conference, call the first number and then dial **flash** to hold the call, dial the second number and before or after being answered, dial **flash** once more to establish the 3-way call.

29.4.3 Forward a Call

To set the **Forward** option, dial: ***** + **2** + ***destination number***

All calls to the phone with **Forward** set will be received at the destination number.

To unset the **Forward** option: dial ***** + **3**

29.4.4 Attended Transfer Call

To perform an Attended Transfer Call (the first callee is part of the transfer until new callee answers) dial **flash** to hold the call, then dial the new number and wait to hear the ring. When the phone rings or after the new callee answers, put the handset down.

Before the new callee picks up the handset the phone will ring both at the destination number and at your line.

By picking up the handset, the callee at the destination number will be engaged in the call with the original caller.

If the callee at the destination number does not pick up the handset, you can receive the call by picking up the handset as long as the phone rings.

29.4.5 Blind Transfer Call

To perform a Blind Transfer when a call is received (a) dial *98;(b) dial the destination number. Once the transfer sequence is dialed, the first call is disconnected. The phone will ring at the destination number. This means a new call is automatically performed between the caller and the second callee. The first callee is disconnected from the call.)

29.4.6 Hold

To hold a call that you are receiving, press **flash** once. The caller will be at hold. To retrieve the call, press **flash** once more.

When the caller is at hold, you can run another call by dialing another number. When you put the handset down the phone will ring. Pick up the call and you will be engaged in a call with the original caller. If you wish you can then transfer the call as described in Attended Transfer Call or in Blind Transfer Call, or just proceed with the original call.

29.4.7 Conditional Call Forwarding

To activate “Conditional Call Forwarding”, dial *1 and then dial the destination number. If the call has been made and the phone has not been picked up within 20 seconds, the call is forwarded to the destination number. To cancel Call Forwarding, dial *3.

29.4.8 Do Not Disturb (DND)

To activate DND, dial *4. The caller will hear the "busy" tone. To cancel DND, dial *5

29.4.9 Redialing of Last Received Call

To dial the last received call, dial *69.

29.4.10 Block Last Received Call

To block the last received caller, dial *60. To start accepting calls from the blocked number again, dial *80, or dial *60 to accept the previously blocked number and block the latest received caller.

29.4.11 Auto Redial

When a number is dialed and the dialed number is busy, the Caller can activate Auto Redial by hanging up, dialing *66 and laying the handset down again. The Gateway will periodically dial the busy number for a default period of 30 minutes. When the dialed number is reached the Caller will be notified with a special distinctive ring. By picking up the phone, the caller will be immediately in the call.

If the called party hangs up and the caller does not pick up the phone when the special ring tone is heard, then on the next attempt to use the phone the Caller will get a busy signal indicating that the Auto Redial service succeeded. To place the next call, the caller needs to hang up and pick up the phone again.

To cancel the periodic Auto Redialing before the timeout has been reached, dial *86.

29.4.12 Block Sending CID per Call

The user can block sending Caller ID per a call, by dialing *70 before dialing the telephone number.

29.4.13 Anonymous Caller Rejection (ACR)

Enables the callee to reject all calls from an anonymous callers. The default keypad value to activate rejecting anonymous calls is *77. To re-activate receiving anonymous calls dial *87.

29.4.14 Support for Pulse Metering per Telephone Line

Pulse Metering is performed by periodically sending a 16 KHz tone pulse during a call to the telephone line. Pulse Metering can be used as call-charge pulses for pay phones. Each pulse signals "one-unit" of charge. The Pulse Metering option is activated when the unit receives a propriety SIP INFO message.

29.4.15 SIP Line Problem Tone Indicator

A Fast Busy tone is played to indicate to the user that there is a problem with the WAN connection or that the SIP Proxy server replied with an error code. The following network errors are indicated:

1. Proxy server responds with an error reply code to an INVITE. The tone will not be played if any of the following error codes are returned: 401, 402, 404, 407, 410, 480, 486, 487, 6xx.
2. The WAN link has been disconnected.

When the unit is not registered with the Proxy server the Fast Busy tone is not played and there is no dial tone.

29.5 Advanced Calling Features for H.323

In the following subsections:

- An expression such as "dial flash + 7" implies "press on flash, then press on 7" (the dialing sequence progresses as read from left to right).
- The Star (or Asterisk) key is represented by the symbol "*".
- The term *destination number* within an expression implies "dial the destination number".

29.5.1 Call Waiting

If you are engaged in a call and another party calls your line, you hear a short tone on your line. The caller hears a ringing tone.

To accept the new call, dial **flash + ∗**. To return to the origin call, dial **flash + ∗** again.

29.5.2 Conference Call

If you are engaged in a call and wish to add a third party, dial **flash + 7**, then dial the third party's number. Once the third party answers the call, a 3-way call is established.

To drop the conference, dial **flash + 8**.

29.5.3 Forward a Call

To set the **Forward** option, dial; **∗ + 2 +** ***destination number***.

All calls to the phone with **Forward** set will be received at the destination number.

To cancel the **Forward** option: dial **∗ + 3.**

29.5.4 Transfer Call

To transfer a call that you are receiving to another number, dial **flash + 4 +** ***destination number*** and put the handset down.

The phone will ring both at the destination number and at your line.

By picking up the handset, the callee at the destination number will be engaged in the call with the original caller. Your phone will stop ringing.

If the callee at the destination number does not pick up the handset, you can receive the call by picking up the handset as long as the phone rings.

29.5.5 Hold

To hold a call that you are receiving, press **flash + 1**. The caller will be at hold.

You can then run another call by dialing another number. When you put the handset down the phone will ring. Pick up the phone and you will be engaged in a call with the original caller. If you wish, you can then transfer the call as described in Transfer call or just proceed with the original call.

29.6 Advanced Calling Features for MGCP

Advanced calling features are supported. Refer to your Call Agent for the advanced calling features supported.

29.7 PSTN (FXO) Calling

NOTE The features in this chapter are operable only on the AC-241-FXO gateway

29.7.1 Outgoing PSTN Calls

You can use either the phone connected to port Phone1 or the one connected to port Phone2 to make a call over the public switched telephone network. The call will be routed to the PSTN line if the dialed number matches the FXO Dial Plan configured in the gateway.

29.7.2 Receiving PSTN Calls

PSTN calls are received only on the phone connected to the Phone 1 port.

29.7.3 Call Waiting

Call waiting will be activated if the first port (Phone 1) is busy.

29.7.4 Conference Call

Applicable in Version 5.2 and later.

A Conference call can be set between an incoming FXO call, the first FXS port and an additional VoIP call.