P-2002 Series

VoIP Analog Telephone Adaptor

User's Guide

Version 3.60
10/2005

ZyXEL

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Certifications

Go to www.zyxel.com

1. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
2. Select the certification you wish to view from this page.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1°, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 1344 303034	ftp.zyxel.co.uk	

a. "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the Prestige 2002 Series VoIP Analog Telephone Adaptor.

Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Your Prestige is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your Prestige for its various applications and provide background information on the Prestige's features.

Note: Use the web configurator to configure your Prestige.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.

- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The Prestige 2002 series may be referred to as the Prestige or the device in this user's guide.

Graphics Icons Key

Prestige 	Computer 	Notebook computer 
Server 	Switch 	Router 
Telephone 		

CHAPTER 1
Introducing the Prestige

This chapter introduces the main features and applications of the Prestige.

1.1 Prestige VoIP Analog Telephone Adaptor Overview

The Prestige is a SIP-based VoIP analog telephone adaptor (ATA). Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP.

The Prestige allows you to use a traditional analog telephone to make and receive Voice over IP calls. You can call any landline or mobile telephone as well as IP telephones. You don't need to know if the recipient's connection type is an IP, cellular or landline based service. Calls received from IP telephones work exactly as you would expect from the traditional telephone service.

The Prestige's two Ethernet ports allow you to connect the Prestige to your LAN and connect your computer to the Prestige. This way your computer can still access the LAN without adding an extra Ethernet switch.

The Prestige's web configurator allows easy management and configuration.

1.2 Prestige 2002L VoIP Analog Telephone Adaptor with Lifeline

The Prestige 2002L has all of the features of the Prestige 2002 and adds the PSTN (Public Switched Telephone Network) lifeline feature. PSTN lifeline lets you have VoIP phone service and PSTN phone service at the same time.

1.3 Features

Your Prestige is packed with a number of features that make it flexible and easy to use. [1]

10/100Mbps Auto-negotiating Fast Ethernet Interfaces

The auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

1. Some features documented in this user's guide were not available in the Prestige 2002L at the time of writing.

Auto-crossover 10/100 Mbps Ethernet Interfaces

The Ethernet interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

PSTN Lifeline

The Prestige 2002L has a **LINE** port for connecting a PSTN line. You can receive incoming PSTN phone calls even while someone else connected to the Prestige is making VoIP phone calls. You can dial a (prefix) number to make an outgoing PSTN call. You can still make PSTN phone calls if the Prestige 2002L loses power.

REN

A Ringer Equivalence Number is used to determine the number of devices that may be connected to the telephone line. The Prestige can support three devices per telephone port.

Dynamic Jitter Buffer

The Prestige has a built-in adaptive, buffer that helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.

Multiple SIP Accounts

The Prestige allows you to simultaneously use multiple voice (SIP) accounts and assign them to one or both telephone ports.

STUN

Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (STUN) allows SIP to pass through NAT routers.

Multiple Voice Channels

The Prestige can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.

Voice Coding

The Prestige can use the following voice codecs (coder/decoders).

- G.711
- G.729

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.

Comfort Noise Generation

The Prestige generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).

Echo Cancellation

The Prestige supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

QoS (Quality of Service)

Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. The Prestige supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the Prestige to tag voice frames so they can be prioritized over the network.

Fax Tone Detection and Pass-through

The Prestige automatically detects fax messages and sends them over PCM G.711.

Auto-provisioning

Your voice service provider can automatically update your Prestige's configuration via an auto-provisioning server.

Auto Firmware Upgrade

The Prestige gives you the option to upgrade to a newer firmware version if it finds one during auto-provisioning. Your voice service provider must have an auto-provisioning server and a server set up with firmware in order for this feature to work.

Manual Firmware Upgrades

Use the web configurator to upload updated firmware to your Prestige.

Ease of Installation

Your Prestige is designed for quick, intuitive and easy installation. Physically, its compact size and lightness make it easy to position anywhere in your busy office.

1.4 LEDs

The following graphic displays the labels of the LEDs.

Figure 1 LEDs

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR/VoIP	Green	On	The Prestige is receiving power.
		Blinking	The Prestige is self-testing.
	Orange	On	The VoIP SIP registration was successful.
		Off	The Prestige is not receiving power.
LAN	Green	On	The Prestige has an Ethernet connection with the cable/DSL modem.
		Blinking	The Prestige is sending/receiving data to/from the cable/DSL modem.
		Off	The Prestige doesn't have an Ethernet connection with the cable/ DSL modem.
PC	Green	On	The Prestige has an Ethernet connection with a computer.
		Blinking	The Prestige is sending/receiving data to /from the computer.
		Off	The Prestige does not have an Ethernet connection with a computer.
Phone 1-2	Green	On	The telephone(s) connected to this port is (are) in use.
		Blinking	The telephone(s) connected to this port is (are) ringing.
		Off	The telephone(s) connected to this port is (are) not in use.

1.5 Applications

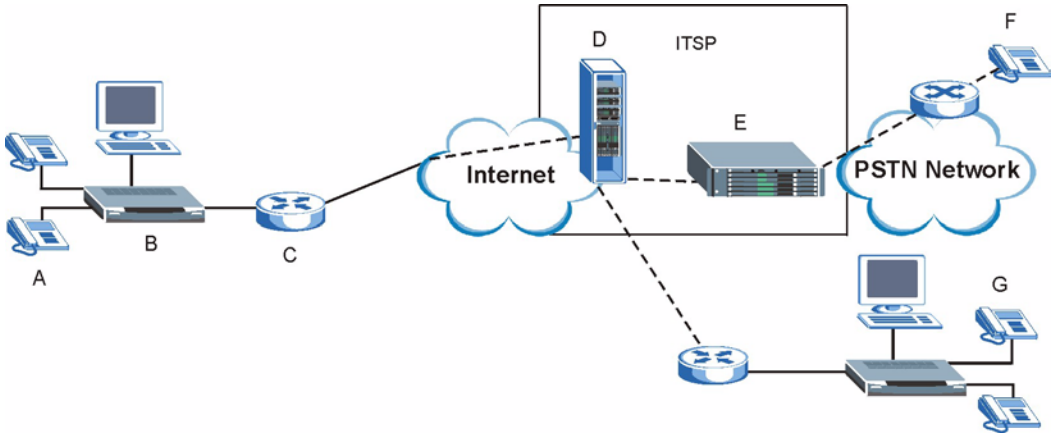
Here are some examples of how you can use your Prestige.

1.5.1 Make Calls via Internet Telephony Service Provider

In a home or small office environment, you can use the Prestige to make and receive VoIP telephone calls through an Internet Telephony Service Provider (ITSP).

The following figure shows a basic example of how you would make a VoIP call through an ITSP. You use your analog phone (A in the figure) and the Prestige (B) changes the call into VoIP. The Prestige then sends your call through your modem or router (C) to the Internet and the ITSP's SIP server. The VoIP call server forwards calls to PSTN phones (F) through a trunking gateway (E) to the PSTN network. The VoIP call server forwards calls to IP phones (G) through the Internet.

Figure 2 Internet Telephony Service Provider Application

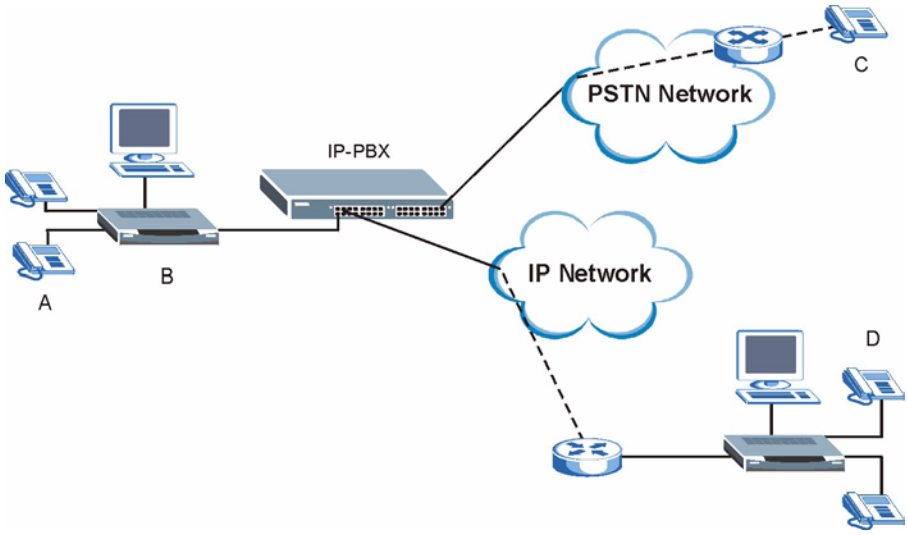


1.5.2 Make Calls via IP-PBX

If your company has an IP-PBX (Internet Protocol Private Branch Exchange), you can use the Prestige to make and receive VoIP telephone calls through it.

In this example, you use your analog phone (A in the figure) and the Prestige (B) changes the call into VoIP and sends it to the IP-PBX. The IP-PBX forwards calls to PSTN phones (C) to the PSTN network. The IP-PBX forwards calls to IP phones (D) through an IP network (this could include the Internet).

Figure 3 IP-PBX Application

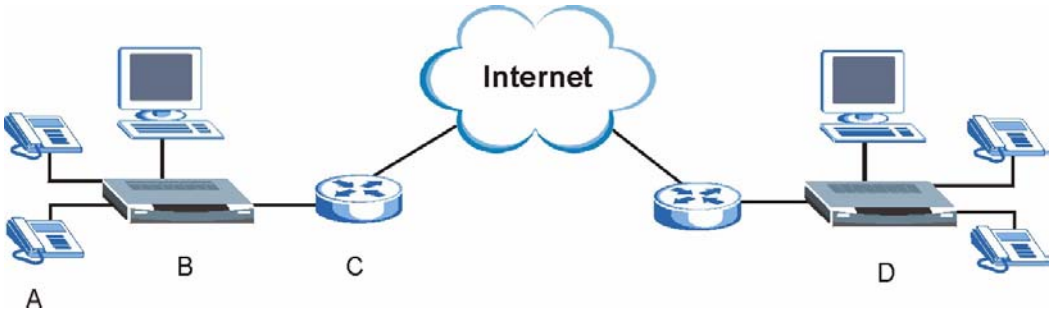


1.5.3 Make Peer-to-peer Calls

Use the Prestige to make a call to the recipient's IP address without using a SIP proxy server Peer-to-peer calls are also called "Point to Point" or "IP-to-IP" calls. You must know the peer's IP address in order to do this.

The following figure shows a basic example of how you would make a peer-to-peer VoIP call. You use your analog phone (A in the figure) and the Prestige (B) changes the call into VoIP. The Prestige then sends your call through your modem or router (C) and the Internet to the peer VoIP device (D).

Figure 4 Peer-to-peer Calling



CHAPTER 2
Introducing the Web Configurator

This chapter describes how to access the Prestige web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy Prestige setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

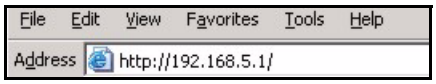
See the **Troubleshooting** chapter if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

2.2 Accessing the Prestige Web Configurator

Note: If your LAN has multiple Prestige 2002s, you may need to disconnect your Prestige's LAN port to avoid accessing the wrong Prestige. Reconnect the LAN port after the **Login** screen displays.

1. Make sure your Prestige hardware is properly connected and prepare your computer/ computer network to connect to the Prestige (refer to the Quick Start Guide).
2. Launch your web browser.
3. Enter the Prestige's management IP address (default 192.168.5.1) or IP address. The Prestige 2002 has a management IP address since by default the Prestige is set to receive a dynamically assigned IP address and thus has no default IP address. Use the Prestige's management IP address or its IP address (after it receives one). If your computer is directly connected to the Prestige, make sure your computer's IP address is in the same subnet as the Prestige's IP address or management IP address that you want to access.

Figure 5 Web Configurator IP Address



4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

Figure 6 Enter Password

5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 7 Change Password

6 You should now see the web configurator **MAIN MENU** screen (see Figure 8 on page 32).

Note: The Prestige automatically logs you out if the management session is idle for five minutes. Simply log back in if this happens to you.

2.3 Resetting the Prestige

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the back of the Prestige. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will also be reset to "1234".

2.3.1 Procedure To Use The Reset Button

Make sure the **PWR/VoIP** LED is on (not blinking) before you begin this procedure.

1. Press the **RESET** button for five to ten seconds (release it when the **PWR/VoIP** LED begins to blink). When the **PWR/VoIP** LED starts blinking, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.
2. Disconnect and reconnect the Prestige's power.
3. Wait for the PWR LED to stop blinking and stay on steady.
4. Press the **RESET** button for five to ten seconds (release it when the **PWR/VoIP** LED begins to blink). When the **PWR/VoIP** LED starts blinking, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.

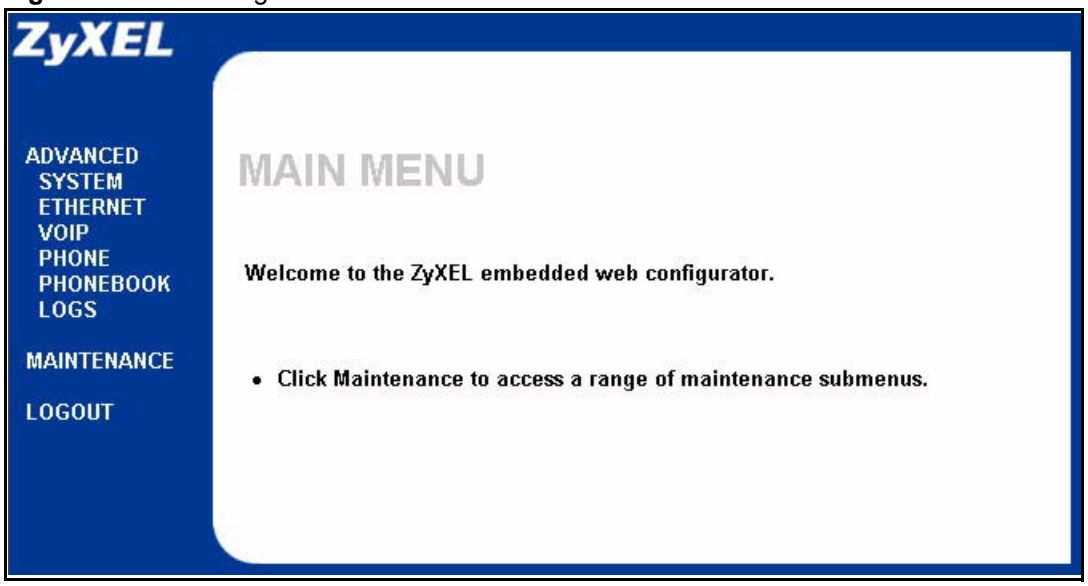
2.4 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

Note: Click the Help icon (located in the top right corner of most screens) to view online help.

Click a link under **ADVANCED** to configure Prestige features.

Figure 8 Web Configurator



The following table describes the navigation panel and sub-menus.

Table 2 Web Configurator Screens Summary

LINK	TAB	FUNCTION
SYSTEM	General	Use this screen to configure general system settings.
	Password	Use this screen to change your password.
	Time Setting	Use this screen to change your Prestige's time and date.
ETHERNET	Ethernet	Use this screen to configure your Prestige's Ethernet interface settings.
	MGNT	Use this screen to configure your Prestige's management IP address.
VOIP	VoIP	Use this screen to configure your Prestige's Voice over IP settings.
	QoS	Use this screen to configure your Prestige's Quality of Service settings.
PHONE	Phone Port	Use this screen to configure your Prestige's phone settings.
PHONE BOOK	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
	Lifeline	Use this screen to configure your Prestige's settings for PSTN calls (Prestige 2002L only).
	Call Forward	Use this screen to configure your Prestige to block or redirect calls.
LOGS	View Log	Use this screen to view the logs.
MAINTENANCE	Status	This screen contains administrative and system-related information.
	F/W Upload	Use this screen to upload firmware to your Prestige.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your Prestige.
	Restart	This screen allows you to reboot the Prestige without turning the power off.
LOGOUT		Click this label to exit the web configurator.

2.5 Common Screen Command Buttons

The following table shows common command buttons found on many web configurator screens.

Table 3 Common Screen Command Buttons

Apply	Click **Apply** to save your changes back to the Prestige.
Reset/Cancel	Click **Reset** or **Cancel** to begin configuring this screen afresh.

CHAPTER 3
System Screens

This chapter provides information on the System screens.

3.1 System Overview

This chapter describes the **SYSTEM** screens.

3.2 General Setup

General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

3.2.1 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

3.3 General Setup Configuration

Click **SYSTEM** in the navigation panel and then **General Setup** to display the following screen.

Figure 9 System General

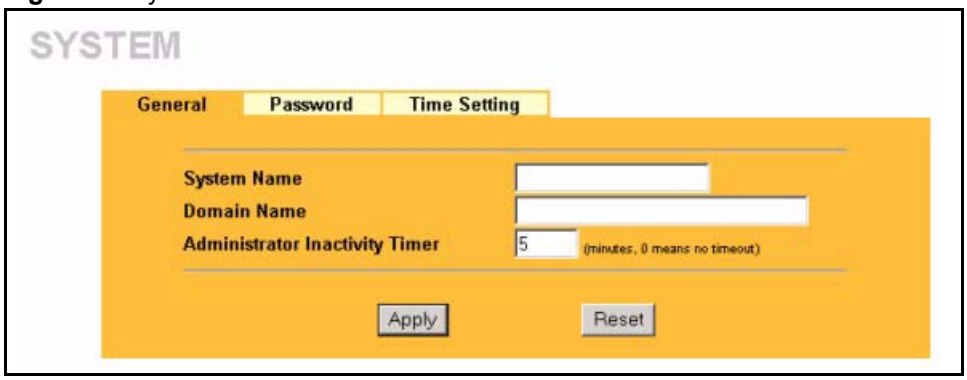


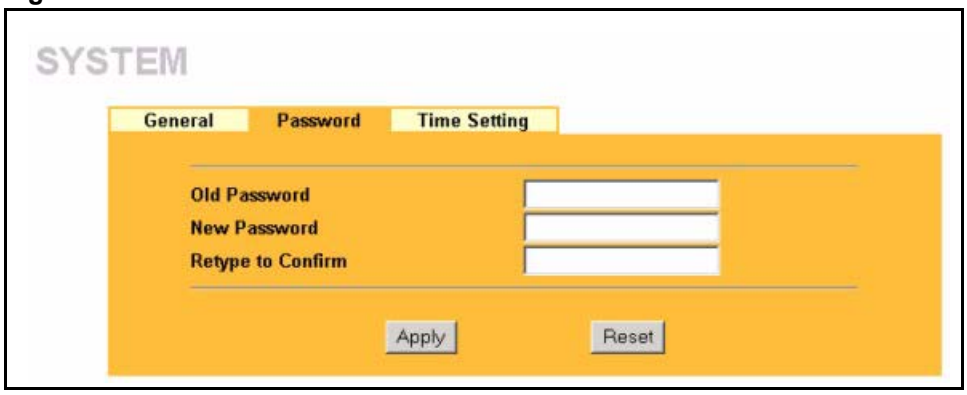
Table 4 System General

LABEL	DESCRIPTION
System Name	This is for identification purposes. Enter your computer's "Computer Name".
Domain Name	The Domain Name entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

3.4 Configuring Password

To change your Prestige's password (recommended), click **SYSTEM** in the navigation panel, and then the **Password** tab. The screen appears as shown. This screen allows you to change the Prestige's password.

Figure 10 Password



The following table describes the labels in this screen.

Table 5 Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field. Use up to 32 ASCII characters.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

3.5 Pre-defined NTP Time Servers List

The Prestige uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Note: The Prestige can use this pre-defined list of time servers regardless of the Time Protocol you select.

When the Prestige uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Prestige goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

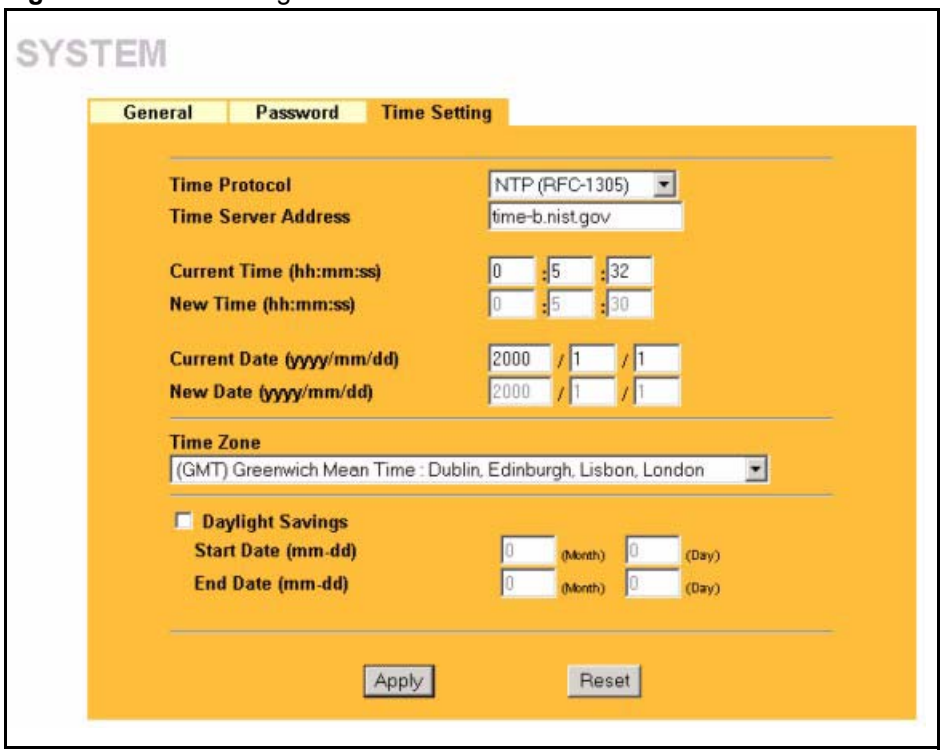
Table 6 Pre-defined NTP Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

3.6 Configuring Time Setting

To change your Prestige's time and date, click **SYSTEM** in the navigation panel, then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the Prestige's time based on your local time zone.

Figure 11 Time Setting



The following table describes the labels in this screen.

Table 7 Time Setting

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305),** is similar to Time (RFC 868). Select **None** to enter the time and date manually.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Current Time	This field displays the time of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server. When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**.
Current Date	This field displays the date of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Date	This field displays the last updated date from the time server. When you select **None** in the **Time Protocol** field, enter the new date in this field and then click **Apply**.

Table 7 Time Setting (continued)

LABEL	DESCRIPTION
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 4
Ethernet Screens

This chapter describes how to configure the Prestige's Ethernet and management IP addresses settings.

4.1 ETHERNET Overview

The Prestige has two Ethernet ports. Connect the **LAN** Ethernet port to a cable/DSL modem or router or an Ethernet LAN switch, which in turn connects you to the Internet or your company's IP-PBX. Connect the **PC** Ethernet port to your computer. The Prestige bridges network traffic between the two Ethernet ports so your computer can still access the Internet or the company LAN. Both Ethernet ports use the same IP address and subnet mask.

4.1.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then the ISP should assign you a dynamic IP address when the connection is established.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.20, for your Prestige, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address.

4.1.2 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Prestige can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields.
- If the ISP did not give you DNS server information, leave the **DNS Server** fields set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

4.1.3 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius).

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

For more information on PPPoE, see Appendix D on page 131.

4.2 Configuring Ethernet

Click **ETHERNET** in the navigation panel to display the **ETHERNET** screen. Use the **ETHERNET Ethernet** screen to configure the Prestige's Ethernet interfaces with Internet account information from your ISP. Your ISP may have already configured some of the fields for you.

You can manage the Prestige through the Ethernet IP address, but you may not always know the Prestige's IP address (especially if the IP address is dynamic). Use the **Mgnt Port** screen (see Figure 13 on page 44) to configure a static IP address that you use to access the Prestige for management.

Figure 12 ETHERNET

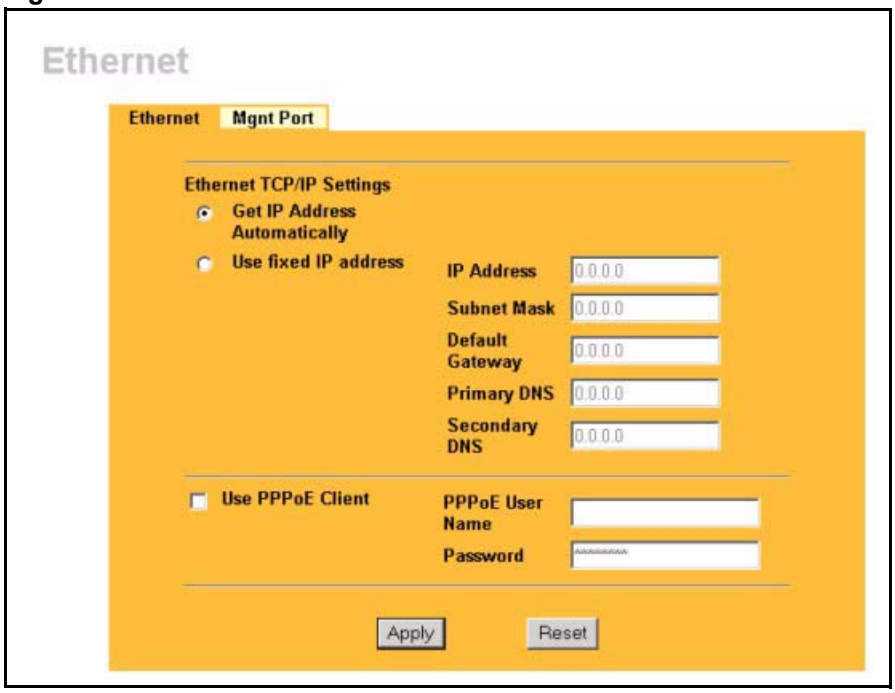


Table 8 ETHERNET

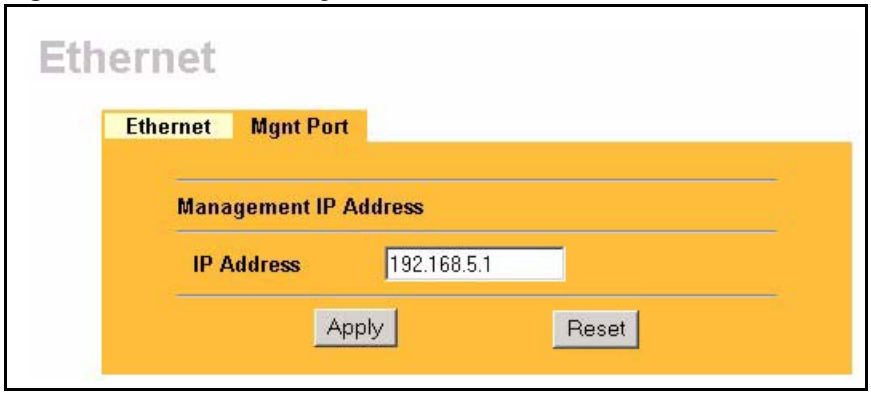
LABEL	DESCRIPTION
Get IP Address Automatically	Select this option if you have a dynamic IP address.
Use Fixed IP Address	Select this option if the ISP assigned you a static IP address.
IP Address	Type the (static) IP address assigned to you by your ISP.
Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Default Gateway	Enter the gateway IP address assigned to you by your ISP (if given).
Primary/Secondary DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS servers are extremely important because without them, you must know the IP address of a computer before you can access it. Specify the DNS servers.
Use PPPoE Client	Select **Use PPPoE Client** if your ISP provides a PPPoE user name and password.
PPPoE User Name	Enter the user name exactly as your ISP assigned it (maximum 72 characters).
Password	Enter the password exactly as your ISP assigned it.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

4.3 Configuring the Ethernet Management Port

Click **ETHERNET** in the navigation panel and then **Mgnt Port** to open the following screen. Use the **ETHERNET Mgnt Port** screen to configure a static IP address through which you can manage the Prestige.

Note: The management port is a separate logical Ethernet interface that you can access from a computer connected to either of the Prestige's physical Ethernet interfaces.

Figure 13 ETHERNET Mgnt Port



The following table describes the labels in this screen.

Note: The management port's subnet mask is fixed at 255.255.255.0.

Table 9 ETHERNET Mgnt Port

LABEL	DESCRIPTION
IP Address	Type the (static) IP address through which to manage the Prestige. This management IP address can be on a different subnet from the Ethernet port's IP address, but the computer you use for management must be on the same subnet as this management IP address.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 5
Introduction to VoIP

This chapter provides background information on VoIP and SIP.

5.1 Introduction to VoIP

VoIP is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service. A company could alternatively set up an IP-PBX and provide it's own VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

5.2 Introduction to SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

5.2.1 SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

5.2.1.1 SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

5.2.1.2 SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

5.2.2 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 10 SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK
4. ACK		
	5.Dialogue (voice traffic)	
6. BYE		
		7. OK

1. A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
2. B sends a response indicating that the telephone is ringing.
3. B sends an OK response after the call is answered.
4. A then sends an ACK message to acknowledge that B has answered the call.
5. Now A and B exchange voice media (talk).
6. After talking, A hangs up and sends a BYE request.
7. B replies with an OK response confirming receipt of the BYE request and the call is terminated.

5.2.3 SIP Servers

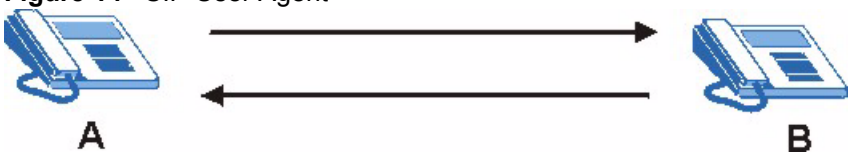
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

5.2.3.1 SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent to receive the call.

Figure 14 SIP User Agent



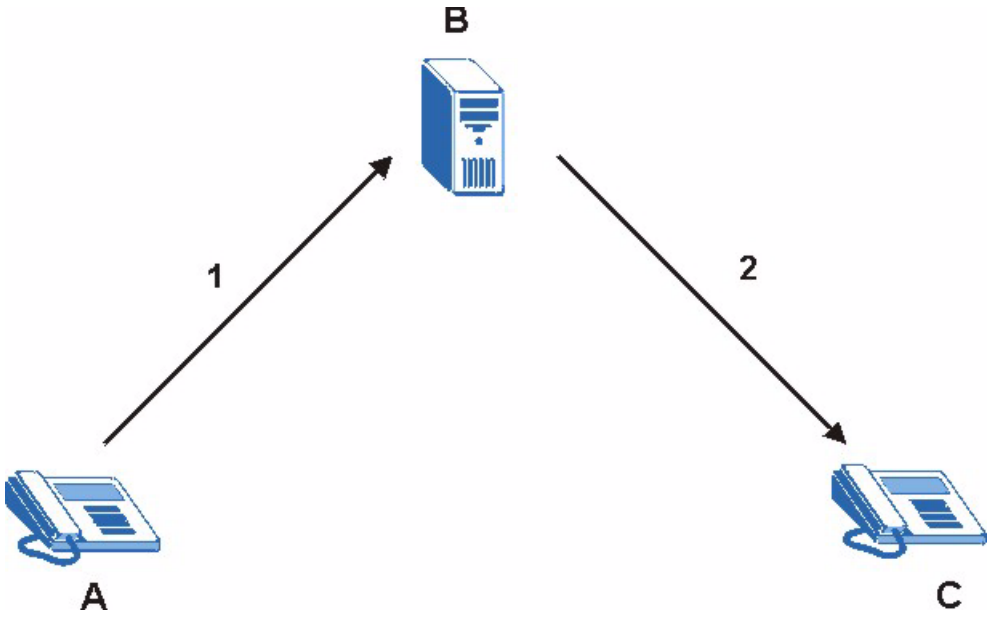
5.2.3.2 SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

1. The client device (A in the figure) sends a call invitation to the SIP proxy server (B).
2. The SIP proxy server forwards the call invitation to C.

Figure 15 SIP Proxy Server



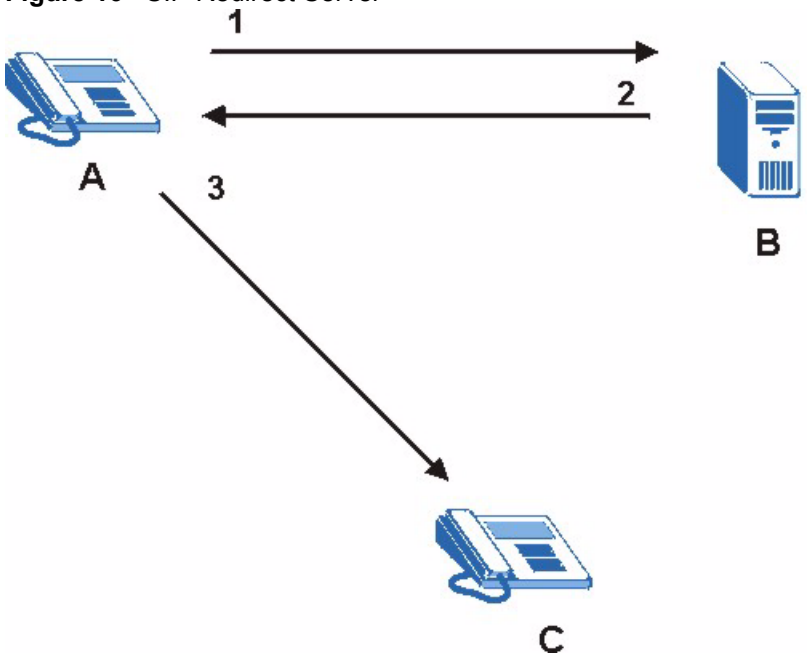
5.2.3.3 SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

1. Client device A sends a call invitation for C to the SIP redirect server (B).
2. The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
3. Client device A then sends the call invitation to client device C.

Figure 16 SIP Redirect Server



5.2.3.4 SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

5.2.4 RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

5.3 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

In the simplest form, NAT changes the source IP address of a packet received from a device to another IP address before forwarding the packet towards the destination. When the response comes back, NAT translates the destination address back to the device's IP address and forwards it to the device.

NAT routers are commonly used to translate private (or internal) IP addresses in packet headers to public (or external) IP addresses and vice versa. A NAT router maps a private IP address and port pair to a public IP address and port, and whenever the NAT router receives a packet with that public IP address and port, it knows how to reroute the packet back to the private IP address and port.

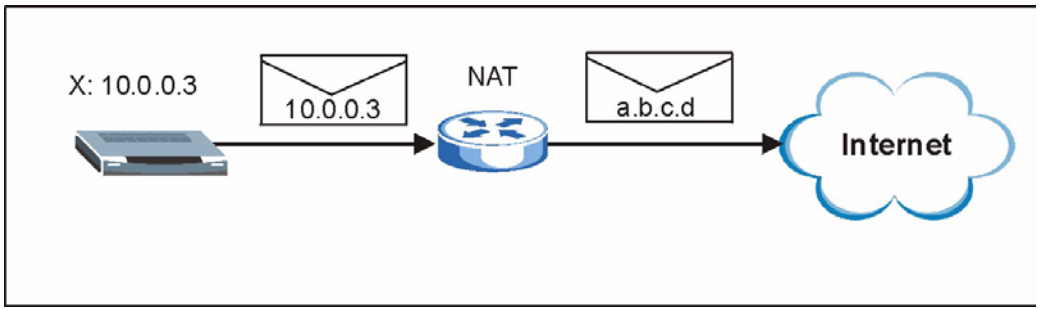
NAT may be implemented on a device that is between your Prestige and the Internet.

5.3.1 NAT Example

See the following figure. The Prestige (X) sends packets to the Internet. The Prestige's IP address is 10.0.0.3. This is a private or internal IP address. The NAT router maps the private source IP address to a public source IP address (a.b.c.d). The public source IP address is also known as the external IP address.

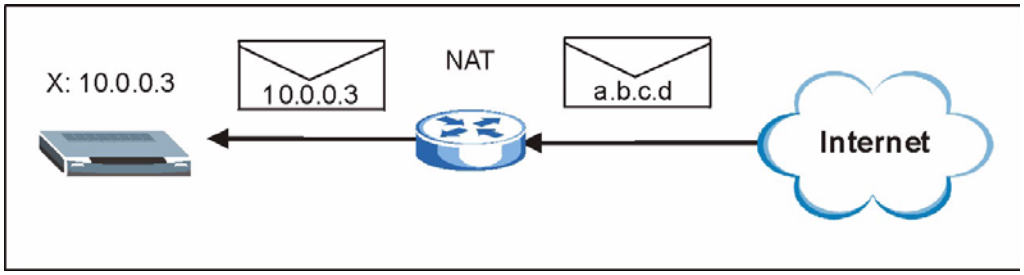
Note: The NAT figures in this chapter use lower-case letters (like a.b.c.d for example) to represent public IP addresses.

Figure 17 NAT: Outgoing



When the NAT router receives packets with destination address IP address a.b.c.d, the NAT router changes a.b.c.d back to the private IP address 10.0.0.3 and sends it to the Prestige.

Figure 18 NAT: Incoming



5.3.2 NAT Types

This section discusses the following NAT types that may be implemented on a router in front of the Prestige.

- Full Cone
- Restricted Cone
- Port Restricted Cone
- Symmetric

The following table summarizes how these NAT types handle outgoing and incoming packets. Read the following sections for more details and examples.

Table 11 NAT Types

	FULL CONE	RESTRICTED CONE	PORT RESTRICTED CONE	SYMMETRIC
Incoming Packets	Any external host can send packets to the mapped external IP address and port.	Only external hosts with an IP address to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	Only external hosts with an IP address and port to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	A host on the external network can only send packets to the specific mapped external IP address and port that the NAT router used in sending a packet to the external host's IP address and port.
Outgoing Packets	The NAT router maps the internal IP address and port of all outgoing packets to a single IP address and port on the external network.			The NAT router maps the internal IP address and port of each outgoing packet to a different external IP address and port for each different destination IP address and port.

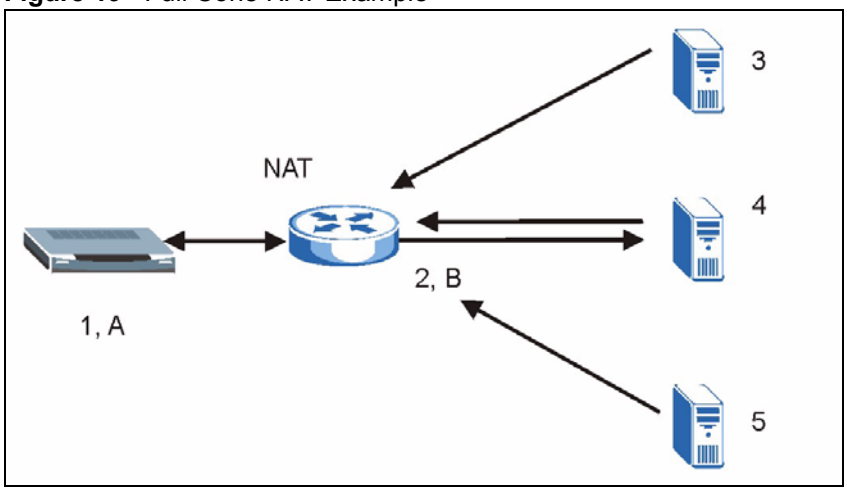
The examples in these NAT type sections describe NAT translation between internal (private) and external (public) IP addresses.

5.3.2.1 Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the NAT router maps the source address of all packets sent from the Prestige's internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The NAT router also performs NAT on all incoming packets sent to IP address **2** and port **B** and sends them to IP address **1**, port **A**.

Figure 19 Full Cone NAT Example



5.3.2.2 Restricted Cone NAT

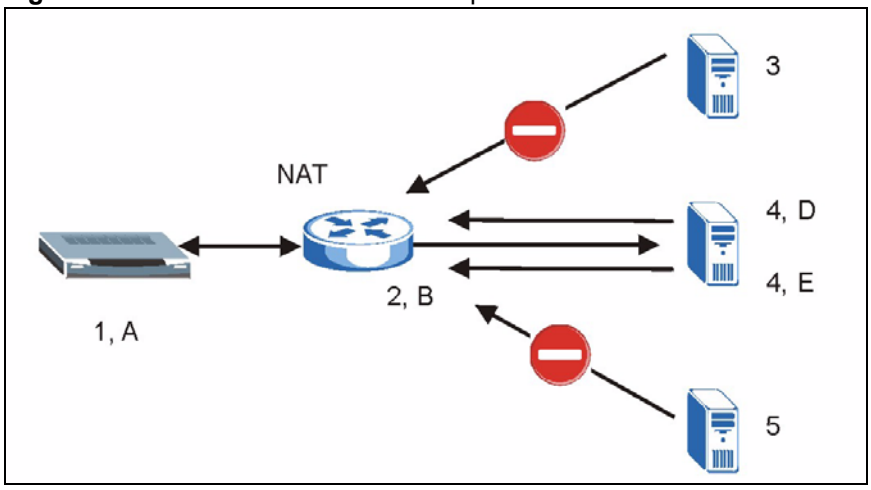
As in full cone NAT, a restricted cone NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the NAT router maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network.

The difference from full cone NAT is in how the restricted cone NAT router handles packets coming in from the external network. A host on the external network (IP address **3** or IP address **4** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address.

A Prestige with IP address **1** and port **A** sends packets to IP address **3** and IP address **4**. The NAT router changes the Prestige's IP address to **2** and port to **B**.

Both **4, D** and **4, E** can send packets to **2**, **B** since **1**, **A** has already sent packets to **4**. The NAT router will perform NAT on the packets from **4, D** and **4, E** and send them to the Prestige at IP address **1**, port **A**. Packets have not been sent from **1**, **A** to **3** or **5**, so **3** and **5** cannot send packets to **1**, **A**.

Figure 20 Restricted Cone NAT Example



5.3.2.3 Port Restricted Cone NAT

As in full cone NAT, a port restricted cone NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the NAT router maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network.

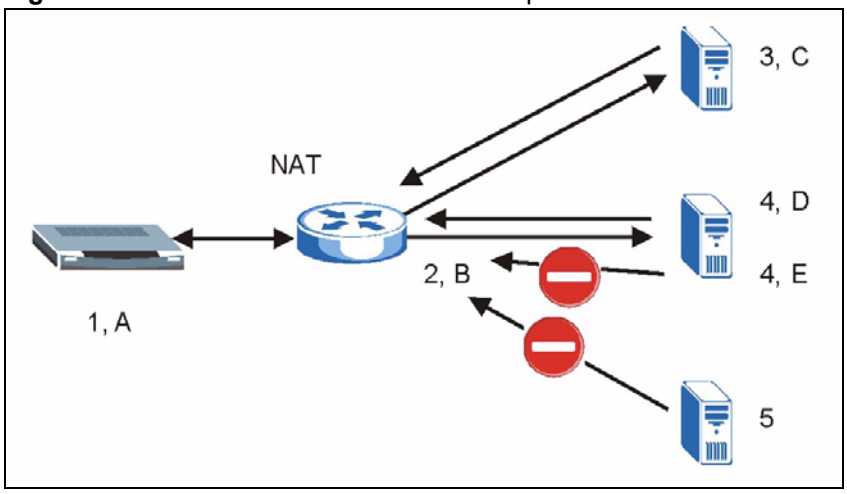
The difference from full cone and restricted cone NAT is in how the port restricted cone NAT router handles packets coming in from the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A Prestige with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The NAT router changes the Prestige's IP address to **2** and port to **B**.

Since **1**, **A** has already sent packets to **3**, **C** and **4**, **D,** they can send packets back to **2**, **B** and the NAT router will perform NAT on them and send them to the Prestige at IP address **1**, port **A**.

Packets have not been sent from **1**, **A** to **4**, **E** or **5**, so they cannot send packets to **1**, **A**.

Figure 21 Port Restricted Cone NAT Example



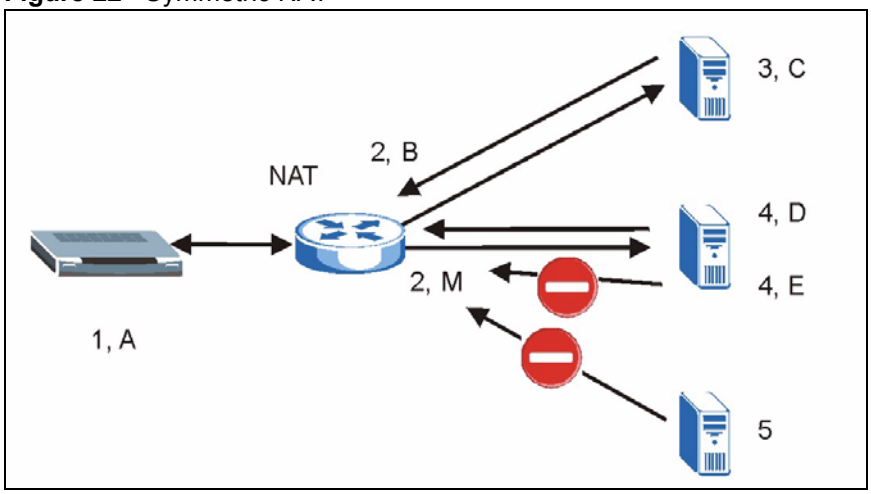
5.3.2.4 Symmetric NAT

The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different destination IP address and port.

In the following example, the NAT router maps the Prestige's source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **B**. The NAT router uses a different mapping (IP address **2** and port **M**) when the Prestige sends packets to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

Figure 22 Symmetric NAT



5.4 NAT and SIP

Some NAT routers are not SIP-friendly and will stop your voice sessions.

The Prestige must register its public IP address with a SIP register server. If there is a NAT router between the Prestige and the SIP register server, the Prestige probably has a private IP address. The Prestige lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the Prestige's IP address from inside the SIP message and maps it to your SIP identity. If the Prestige has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity.

A SIP ALG (Application Layer Gateway), the fake WAN address on SIP and RTP, STUN, or outbound proxy features allow the Prestige to use its public IP address in the SIP messages.

5.4.1 SIP ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Prestige registers with the SIP register server, the SIP ALG translates the Prestige's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Prestige is behind a SIP ALG.

5.4.2 Use NAT Address on SIP and RTP

If you know the NAT router's public IP address and SIP port number, you can use the Use NAT feature to manually configure the Prestige to use a them in the SIP messages. This eliminates the need for STUN or a SIP ALG.

You must also configure the NAT router to forward traffic with the SIP port number to the Prestige.

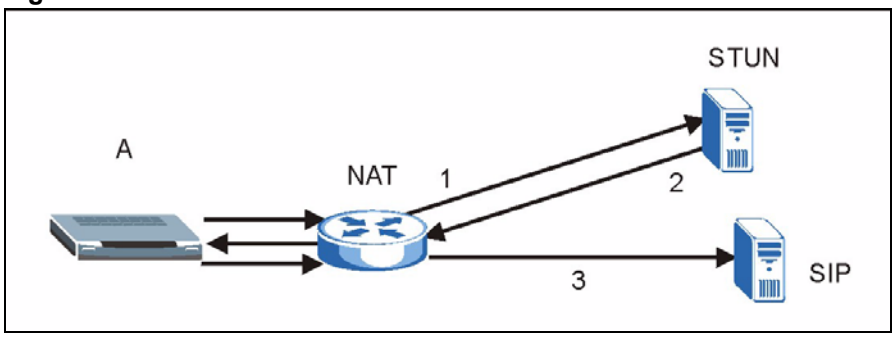
5.4.3 STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the Prestige to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the Prestige to find the public IP address that NAT assigned, so the Prestige can embed it in the SIP data stream. STUN does not work with symmetric NAT routers (see Section 5.3.2.4 on page 52) or firewalls. See RFC 3489 for details on STUN.

The following figure shows how STUN works.

1. The Prestige (A) sends SIP packets to the STUN server.
2. The STUN server finds the public IP address and port number that the NAT router used on the Prestige's SIP packets and sends them to the Prestige.
3. The Prestige uses the public IP address and port number in the SIP packets that it sends to the SIP server.

Figure 23 STUN



5.4.4 Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the Prestige's VoIP traffic. This allows the Prestige to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the Prestige to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).

5.5 Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

5.6 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The Prestige supports the following codecs.

5.6.1 G.711

G.711 is a Pulse Code Modulation (PCM) waveform codec. G.711 provides very good sound quality but requires 64kbps of bandwidth.

5.6.2 G.729

G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

5.7 PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.[1]

5.8 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your voice service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

1. The Prestige does not support pulse dialing at the time of writing.

CHAPTER 6
VoIP Screens

This chapter describes how to configure advanced VoIP and QoS settings.

6.1 VoIP Introduction

VoIP is the sending of voice signals over the Internet Protocol. This chapter covers the configuration of the **VoIP** screens.

6.2 VoIP Configuration

Click **VoIP** in the navigation panel to display the following screen. Use this screen to configure the Prestige's VoIP settings. You should have a voice account already set up and have VoIP information from your VoIP service provider.

Figure 24 VoIP

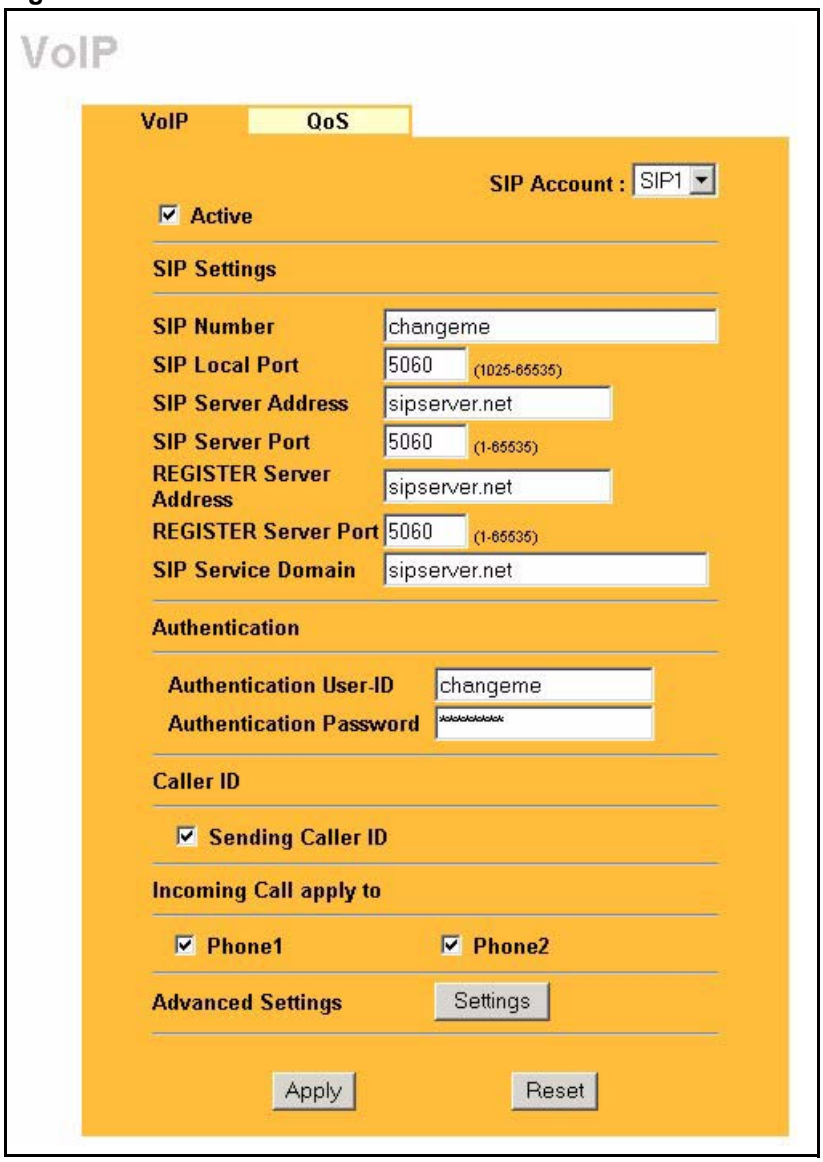


Table 12 VoIP

LABEL	DESCRIPTION
SIP Account	You can configure the Prestige to use multiple SIP accounts. Select one to configure its settings on the Prestige.
Active	Select this check box to have the Prestige use this SIP account. Clear the check box to have the Prestige not use this SIP account.
SIP Number	Enter your SIP number in this field (use the number or text that comes before the @ symbol in a full SIP URI). You can use up to 127 ASCII characters.
SIP Local Port	Use this field to configure the Prestige's listening port for SIP. Leave this field set to the default if you were not given a local port number for SIP.
SIP Server Address	Type the IP address of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server.

Table 12 VoIP (continued)

LABEL	DESCRIPTION
SIP Server Port	Enter the SIP server's listening port for SIP in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for SIP.
REGISTER Server Address	Enter the SIP register server's address in this field. **If you were not given a register server address, then enter the address from the** SIP Server Address **field again here.**
REGISTER Server Port	Enter the SIP register server's listening port for SIP in this field. **If you were not given a register server port, then enter the port from the** SIP Server Port **field again here.**
SIP Service Domain	Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a full SIP URI). You can use up to 127 ASCII Extended set characters.
Authentication User ID	This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.
Authentication Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Sending Caller ID	Select this check box to show identification information when you make VoIP phone calls. Clear the check box to not show identification information when you make VoIP phone calls.
Incoming Call apply to	**Phone 1** and **Phone 2** correspond to the Prestige's physical **PHONE 1** and **2** ports, respectively. Select whether you want to receive calls for this SIP account on **Phone 1**, **Phone 2** or both. If you select both, you will not know which SIP account a call is coming in on.
Advanced Settings	Click **Settings** to open a screen where you can configure the Prestige's advanced VoIP settings like SIP server settings, the RTP port range and the coding type.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

6.3 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Prestige device. The Prestige allows you to record custom tones for the **Caller Ringing Tone** and **On Hold Tone** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 13 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	120 seconds for all custom tones combined
Time per Individual Tone	20 seconds
Total Number of Tones Recordable	Ten You can record up to ten different custom tones but the total time must be 120 seconds or less. For example you could record up to ten 12-second tones or up to six 20-second tones.

6.3.0.1 Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1101~1108 on your phone followed by the "#" key.
3. Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.
4. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

6.3.0.2 Listening to Custom Tones

Do the following to listen to a custom tone:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1201~1208 followed by the "#" key to listen to the tone.
3. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

6.3.0.3 Deleting Custom Tones

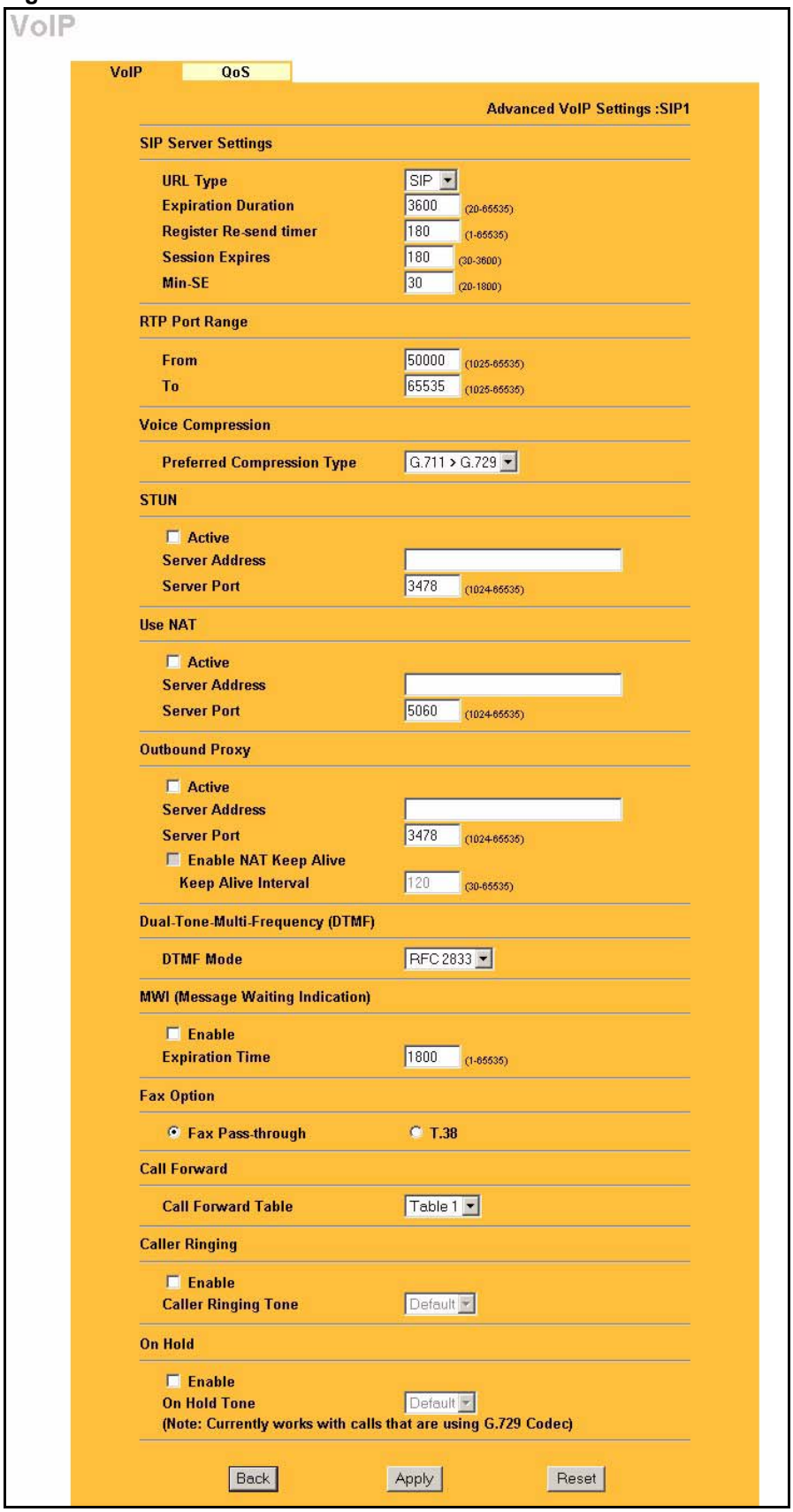
Do the following to delete a custom tone:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1301~1308 followed by the "#" key to delete the tone of your choice. Press 14 followed by the "#" key if you wish to clear all your custom tones.
3. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

6.4 Advanced VoIP Settings Configuration

Click **VoIP** in the navigation panel, select a SIP account and then click **Settings** to display the following screen.

Figure 25 VoIP Advanced



The following table describes the labels in this screen.

Table 14 VoIP Advanced

LABEL	DESCRIPTION
Advanced VoIP Settings	This read-only field displays the number of the SIP account that you are configuring. The changes that you save in this page affect the Prestige's settings with the SIP account displayed here.
SIP Server Settings	
URL Type	Select **SIP** to have the Prestige include the domain name with the SIP number in the SIP messages that it sends. Select **TEL** to have the Prestige use the SIP number without a domain name in the SIP messages that it sends.
Expiration Duration	This field sets how long an entry remains registered with the SIP register server. After this time period expires, the SIP register server deletes the Prestige's entry from the database of registered SIP numbers. The register server can use a different time period. The Prestige sends another registration request after half of this configured time period has expired.
Register Re-send Timer	Use this field to set how long the Prestige waits before sending a repeat registration request if a registration attempt fails or there is no response from the registration server.
Session Expires	Use this field to set the longest time that the Prestige will allow a SIP session to remain idle (without traffic) before dropping it.
Min-SE	When two SIP devices negotiate a SIP session, they must negotiate a common expiration time for idle SIP sessions. This field sets the shortest expiration time that the Prestige will accept. The Prestige checks the session expiration values of incoming SIP INVITE requests against the minimum session expiration value that you configure here. If the session expiration of an incoming INVITE request is less than the value you configure here, the Prestige negotiates with the other SIP device to increase the session expiration value to match the Prestige's minimum session expiration value.
RTP Port Range	Real time Transport Protocol is used to handle voice data transfer. Use this field to configure the Prestige's listening port range for RTP traffic. Leave these fields set to the defaults if you were not given a range of RTP ports to use.
Preferred Compression Type	Use this field to select the type of voice coder/decoder (codec) that you want the Prestige to use. G.711 provides higher voice quality than G.729 but requires 64kbps of bandwidth while G.729 only requires 8kbps. Select **G.711>G.729** if you want the Prestige to first attempt to use the G.711 codec and then the G.729 codec if the peer is not set up to use G.711. Select **G.711 only** if you want the Prestige to only use the G.711 codec when making VoIP calls. You will not be able to connect to a peer that is not set up to use G.711. Select **G.729>G.711** if you want the Prestige to first attempt to use the G.729 codec and then the G.711 codec if the peer is not set up to use G.729. Select **G.729 only** if you want the Prestige to only use the G.729 codec when making VoIP calls. You will not be able to connect to a peer that is not set up to use G.729.
STUN	Use STUN if there is a NAT router between the Prestige and the voice service provider's SIP server. You do not need to use STUN if the NAT router is also a SIP ALG.
Server Address	Your VoIP service provider must host a STUN server in order for you to use STUN. Type the IP address of the STUN server in this field.

Table 14 VoIP Advanced (continued)

LABEL	DESCRIPTION
Server Port	Enter the STUN server's listening port for STUN requests in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for STUN.
Use NAT	Enable this feature to use a NAT router's public IP address and SIP port number in the Prestige's SIP messages. You must also configure the NAT router to forward traffic with this port number to the Prestige. This eliminates the need for STUN or a SIP ALG.
IP Address	Enter the NAT router's public IP address or domain name (up to 127 ASCII characters) in this field.
Server Port	Enter the port number that your SIP sessions use with the public IP address of the NAT router.
Outbound Proxy	Enable this feature if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Prestige to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the Prestige to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name (up to 127 ASCII characters) of the SIP outbound proxy server in this field.
Server Port	Enter the SIP outbound proxy server's listening port for SIP outbound proxy requests in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for the SIP outbound proxy server.
Enable NAT Keep Alive	You must have outbound proxy enabled to use NAT keep alive. Enable NAT keep alive to have the Prestige send SIP notify messages to the SIP server. Use this to keep a NAT router located between the Prestige and the SIP server from timing out and dropping your Prestige's SIP NAT sessions.
Keep Alive Interval	Set how often (in seconds) the Prestige should send SIP notify messages to the SIP server.
DTMF Mode	The Dual-Tone MultiFrequency (DTMF) mode sets how the Prestige handles the tones that your telephone makes when you push its buttons. It is recommended that you use the same mode that your VoIP service provider uses. Select **RFC 2833** to send the DTMF tones in RTP packets. Select **PCM** (Pulse Code Modulation) to include the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) could distort the tones. Select **SIP INFO** to send the DTMF tones in SIP messages.
MWI (Message Waiting Indication)	Enable Message Waiting Indication (MWI) to have your phone give you a message–waiting (beeping) dial tone when you have a voice message(s). Your voice service provider must have a messaging system that supports this feature.
Expiration Time	Use this field to set how long the SIP server should continue providing the message waiting service after receiving a SIP SUBSCRIBE message from the Prestige. The SIP server stops providing the message waiting service if it has not received another SIP SUBSCRIBE message from the Prestige before this time period expires.

Table 14 VoIP Advanced (continued)

LABEL	DESCRIPTION
Fax Option	Use this field to set how the Prestige handles fax messages. You can select either the **Fax Pass-through** or the **T.38** fax methods. Select **Fax Pass-through** to have the Prestige send fax messages over G.711. The peer devices must also use G.711. Select **T.38** to have the Prestige send fax messages over the IP network as UDP or TCP/IP packets. It provides better transmission quality than fax pass-through but may have inter operability problems. The peer devices must also use T.38.
Call Forward Table	Select which call forwarding table you want the Prestige to use to block or redirect calls. You can use a different call forwarding table for each SIP account or use the same call forwarding table for both.
Caller Ringing	Select the **Enable** check box to activate a custom caller ringing tone for incoming calls. The caller ringing tone is the sound that incoming callers will hear when they call you. Use the **Caller Ringing Tone** drop-down list box to choose a tone. The caller ringing tone currently works with calls that are using the G.729 codec.
On Hold	Select the **Enable** check box to activate a custom on hold tone for callers on hold. The on hold tone is the sound callers will hear when you put them on hold. Use the **On Hold Tone** drop-down list box to choose a tone. The on hold tone currently works with calls that are using the G.729 codec.
Back	Click **Back** to return to the VoIP screen without saving configuration changes.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

6.5.1 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the Prestige) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

6.5.2 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[1]

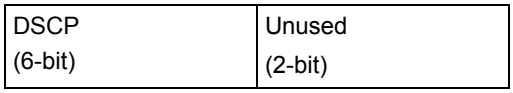
1. The Prestige does not support DiffServ at the time of writing.

6.5.2.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 26 DiffServ: Differentiated Service Field



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

6.5.3 VLAN

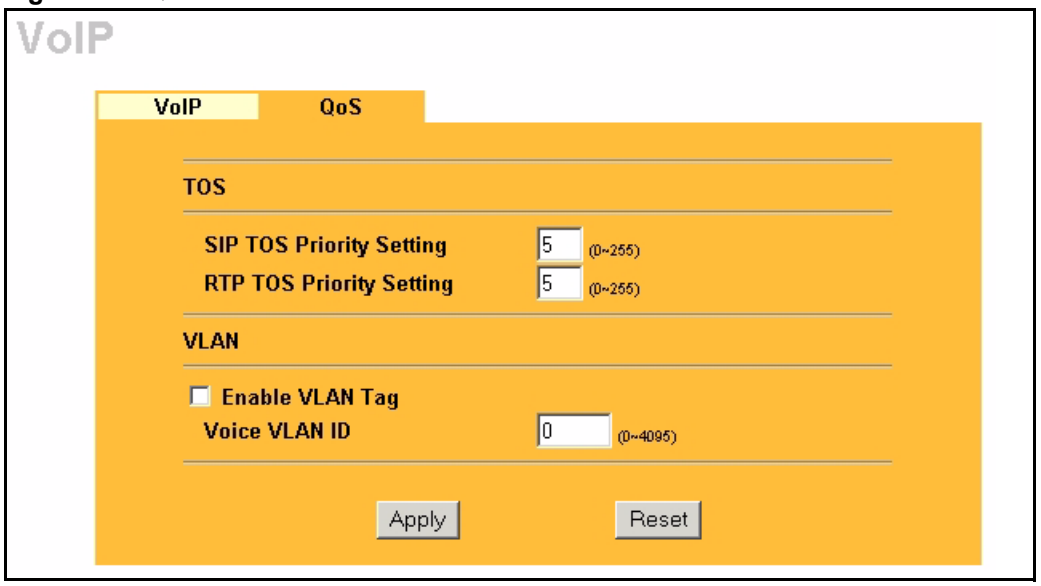
Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your Prestige can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the Prestige to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

6.6 QoS Configuration

Click **VoIP** in the navigation panel and then **QoS** to display the following screen.

Figure 27 QoS



The following table describes the labels in this screen.

Table 15 QoS

LABEL	DESCRIPTION
SIP TOS Priority	Type a priority for voice transmissions. The Prestige applies Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority	Type a priority for voice transmissions. The Prestige applies Type of Service priority tags with this priority to RTP traffic that it transmits.
Enable VLAN Tag	Enable VLAN tagging if the Prestige needs to be a member of a VLAN group in order to communicate with the SIP server. Your LAN and gateway must also be set up to use VLAN tags. Some switches also give priority to voice traffic based on its VLAN tag. Disable VLAN tagging if the Prestige does not need to be a member of a VLAN group to communicate with the SIP server.
Voice VLAN ID	Type the VLAN ID (VID) from 0 to 4095 for the Prestige to add to voice Ethernet frames that it sends out to the network.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 7
Phone

This chapter covers how to adjust the Prestige's phone settings.

7.1 Phone Introduction

You can configure the volume, echo cancellation and VAD settings for each individual phone port on the Prestige. You can also select which SIP account to use for making outgoing calls.

7.1.1 Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Prestige reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

7.1.2 Comfort Noise Generation

When using VAD, the Prestige generates and sends comfort noise when the other party is not speaking. Comfort noise uses the lowest possible transmission bandwidth to match the background noise. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

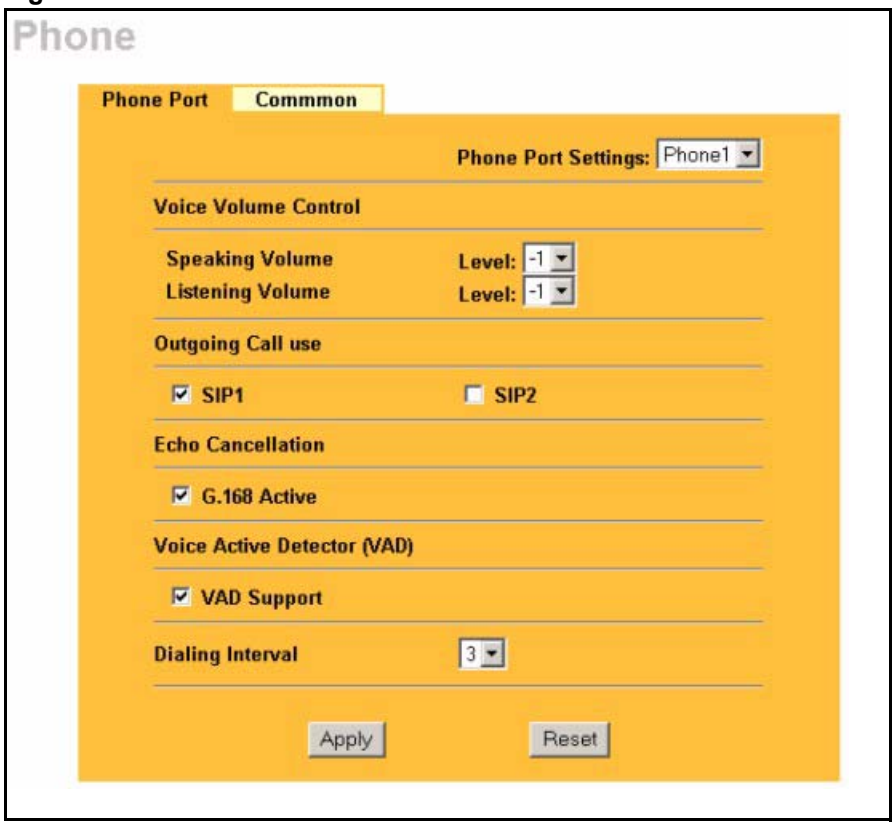
7.1.3 Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

7.2 Phone Port Configuration

Click **PHONE** in the navigation panel to display the following screen. Use this screen to configure phone port settings that are specific to an individual phone port.

Figure 28 Phone Port



The following table describes the labels in this screen.

Table 16 Phone Port

LABEL	DESCRIPTION
Phone Port Settings	Use this field to select the phone port that you want to configure.
Speaking Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it sends to the peer device. -1 is the quietest and 1 is the loudest.
Listening Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it receives from the peer device and sends to your phone. -1 is the quietest and 1 is the loudest.
Outgoing Call use	**SIP 1** and **SIP 2** correspond to the Prestige's SIP accounts. Select whether you want the phone(s) attached to this phone port to use SIP account 1, 2 or both when you make a call. If you select both SIP accounts, the Prestige will first try to use SIP account 2 and then SIP account 1 when you make a call.
G.168 Active	Select this check box to cancel the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
VAD Support	Select this check box to use Voice Activity Detection (VAD). VAD reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Dialing Interval	When you are dialing a telephone number the Prestige waits this long after you stop pressing the buttons before initiating the call. Select how many seconds you want the Prestige to wait after the last input on the telephone's keypad before dialing (making) a call.

Table 16 Phone Port (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

7.3 Supplementary Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, … are generally available from your voice service provider. The Prestige supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding (see Section 8.3 on page 77)
- Three-Way Conference
- Internal Calls (see Section 11.3 on page 93)

Note: To take full advantage of the supplementary phone services available though the Prestige's phone ports, you may need to subscribe to the services from your voice service provider.

7.3.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Prestige.

You can invoke all the supplementary services by using the flash key.

7.3.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 17 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

7.3.2.1 European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

7.3.2.2 European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press "0".
- Disconnect the first call and answer the second call.

  Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.

- Put the first call on hold and answer the second call.

  Press the flash key and then "2".

7.3.2.3 European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call. to operate the Intercom.
3. After you hear the ring signal or the second party answers it, hang up the phone.

7.3.2.4 European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press "3" to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

7.3.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 18 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

7.3.3.1 USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

7.3.3.2 USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

7.3.3.3 USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call. to operate the Intercom.
3. After you hear the ring signal or the second party answers it, hang up the phone.

7.3.3.4 USA Three-Way Conference

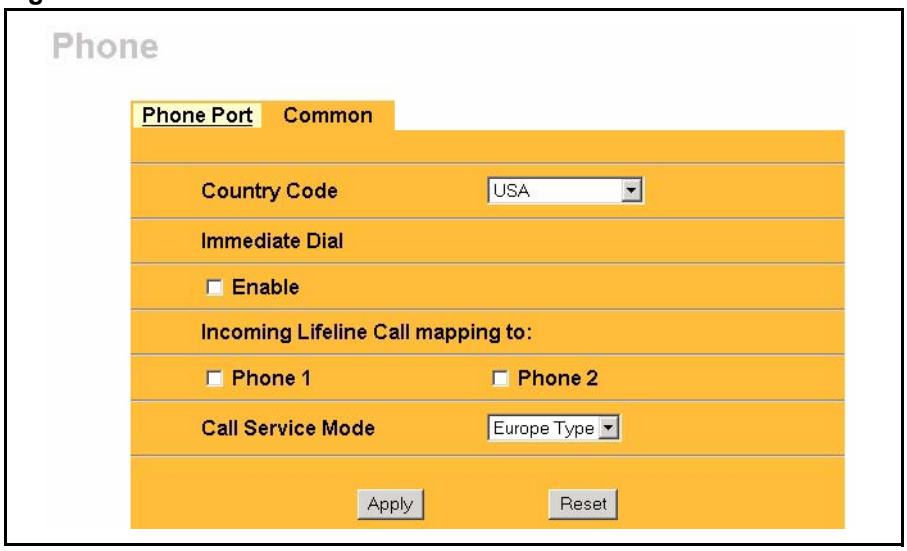
Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key, wait for the sub-command tone and press "3" to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key, wait for the sub-command tone and press "2".

7.4 Common Phone Configuration

Click **PHONE** in the navigation panel and then **Common** to display the following screen. Use this screen to configure general phone settings.

Figure 29 Phone Common



The following table describes the labels in this screen.

Table 19 Phone Common

LABEL	DESCRIPTION
Country Code	Use the drop-down list box to select the country where your Prestige is located.
Immediate Dial	Use immediate dial to have the Prestige make calls right away instead of waiting for the dialing interval (the time period it waits to make sure you are done pressing the keys). In order to use immediate dial, enable it here. Then press the pound (#) key on your telephone's keypad after dialing a phone number (this has the Prestige make the call right away).
Incoming Lifeline Call mapping to (Lifeline models only)	**Phone 1** and **Phone 2** correspond to the Prestige's physical **PHONE 1** and **2** ports, respectively. Select whether you want to receive regular (PSTN) phone calls on **Phone 1**, **Phone 2** or both. If you select both, all of the phones connected to the Prestige's **PHONE** ports will ring when a call comes in on the PSTN line.
Call Service Mode	Use this field to set how the Prestige handles supplementary phone services (call hold, call waiting, call transfer and three-way conference calls). Select the mode that your voice service provider supports. Select **Europe Type** to use the supplementary phone services in European mode. Select **USA Type** to use the supplementary phone services American mode. **Note:** To take full advantage of the supplementary phone services available though the Prestige's phone ports, you may need to subscribe to the services from your voice service provider.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 8
Phone Book

This chapter covers how to configure the Prestige's phone book.

8.1 Phone Book Introduction

You can use the phone book feature to configure speed dial entries, call forwarding tables and the lifeline settings.

8.1.1 Speed Dial

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers.

8.1.1.1 Peer-to-Peer Calls

You can call another VoIP device directly without going through a SIP server. You must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The Prestige sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

You do not need to configure a SIP account on the Prestige 2002 in order to make a peer-to-peer VoIP call. You must still configure a SIP account on the Prestige 2002L in order to make a peer-to-peer VoIP call.

8.1.2 Lifeline (Prestige 2002L)

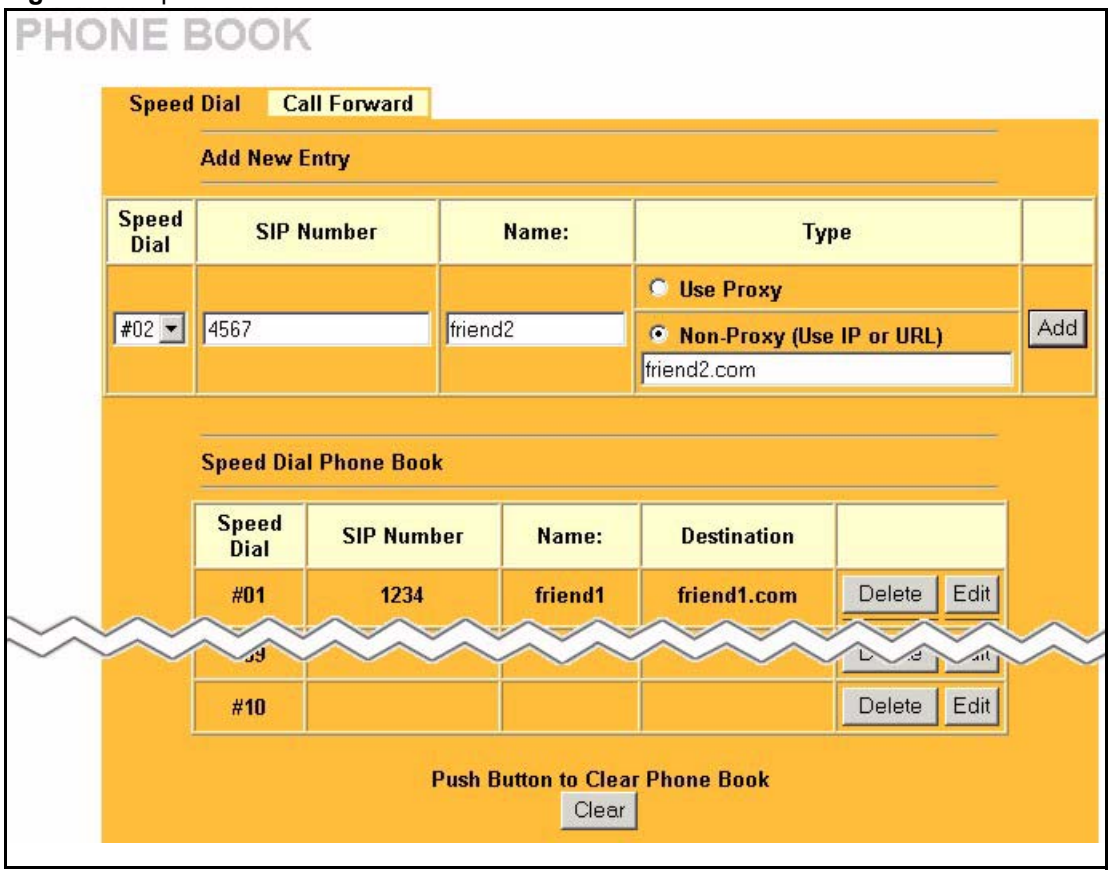
With lifeline you can make and receive regular phone calls. Use a prefix number to make a regular call. When the Prestige 2002L does not have power, you can make regular calls without dialing a prefix number.

You can also specify phone numbers that should always use the regular phone service (without having to dial a prefix number). Do this for emergency numbers (like those for contacting police, fire or emergency medical services).

8.2 Speed Dial Configuration

Click **PHONEBOOK** in the navigation panel and then **Speed Dial** to display the following screen.

Figure 30 Speed Dial



The following table describes the labels in this screen.

Table 20 Speed Dial

LABEL	DESCRIPTION
Add New Entry	Use this section of the screen to edit and save new or existing speed dial phone book entries.
Speed Dial	Select a speed dial key combination from the drop-down list box. After configuring the speed dial entry and adding it to the phonebook, dial this speed dial key combination to use the speed dial entry to make a call.
SIP Number	Enter the SIP number of the party that you will call (use the number or text that comes before the @ symbol in a full SIP URI). You can use up to 127 ASCII characters.
Name	Enter a descriptive name to identify the party that you will use this entry to call. You can use up to 127 ASCII characters.
Type	Select **Use Proxy** if calls to this party use your SIP account configured in the **VoIP** screen. Select **Non-Proxy (Use IP or URL)** if calls to this party use a different SIP server or go directly to the callee's VoIP phone (peer-to-peer). Enter the SIP server's or the party's IP address or domain name (up to 127 ASCII Extended set characters).
Add	Click this button to save the entry in the speed dial phone book. The speed dial entry displays in the **Speed Dial Phone Book** section of the screen.
Speed Dial Phone Book	This section of the screen displays the currently saved speed dial entries. You can configure up to 10 entries and use them to make calls.

Table 20 Speed Dial (continued)

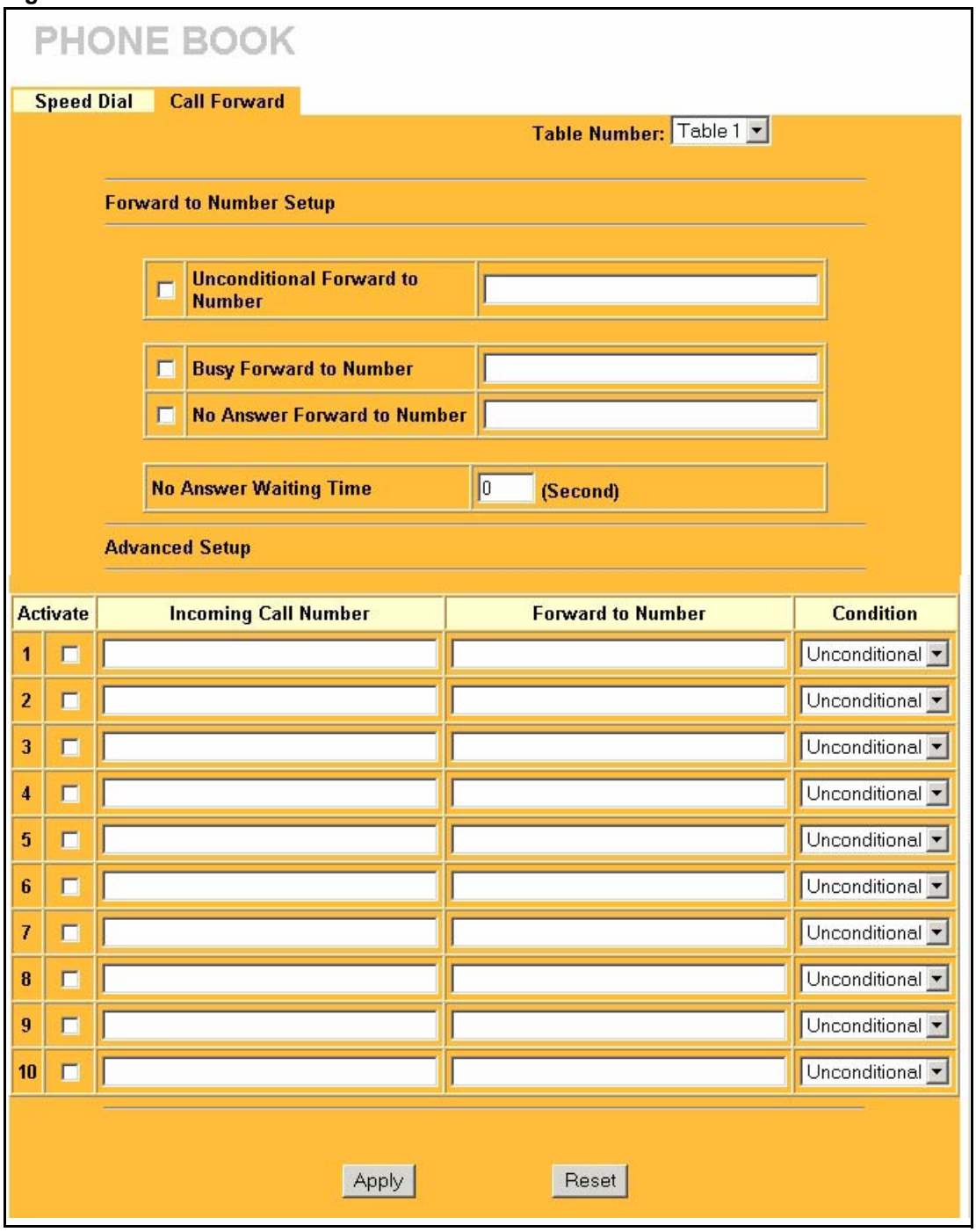
LABEL	DESCRIPTION
Speed Dial	This is the entry's speed dial key combination. Press this key combination on a telephone attached to the Prestige in order to call the party named in this entry.
Name	This is the descriptive name of the party that you will use this speed dial entry to call.
SIP Number	This is the SIP number of the party that you will call.
Type	This field displays **Use Proxy** if calls to this party use one of your SIP accounts. This field displays the SIP server's or the party's IP address or domain name if calls to this party do not use one of your SIP accounts.
Delete	Click this button to remove an entry from the speed dial phone book.
Edit	Click this button to change the speed dial entry. The speed dial entry displays in the **Add New Entry** section of the screen where you can edit it.
Clear	Click this button to remove all of the entries from the speed dial phone book.

8.3 Call Forward

Click **PHONEBOOK** in the navigation panel and then **Call Forward** to display the following screen.

Use this screen to configure the Prestige to block or redirect calls. You can configure a different call forwarding table for each SIP account or use the same call forwarding table for both.

Figure 31 Call Forward



The following table describes the labels in this screen.

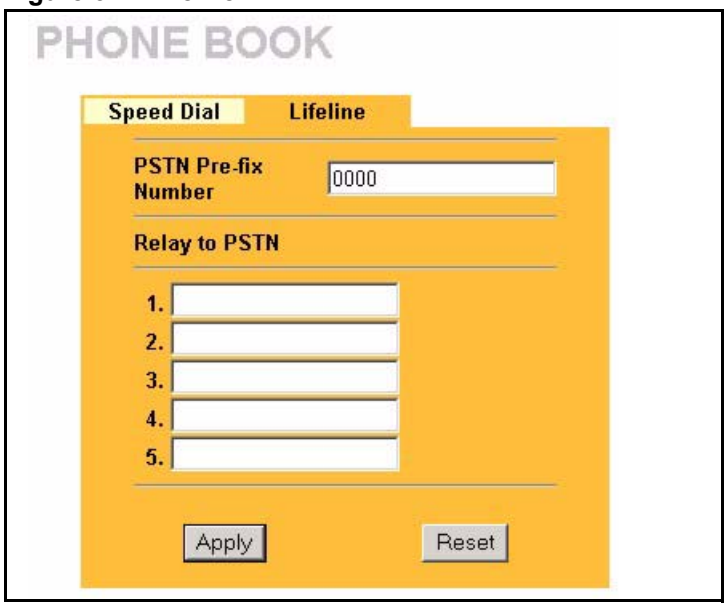
Table 21 Call Forward

LABEL	DESCRIPTION
Table Number	Select which call forwarding table you want to configure. You can configure a different call forwarding table for each SIP account or use the same call forwarding table for both.
	The following applies to the number fields in this screen. For a SIP number, use the number or text that comes before the @ symbol in a full SIP URI. You can use up to 127 ASCII characters.
Forward to Number Setup	These are the global call forwarding settings that define the default action to take on incoming calls that do not match any of the **Advanced Setup** call forwarding entries.
Unconditional Forward to Number	Enable this feature to have the Prestige forward all incoming calls to the number that you configure regardless of whether or not the phone(s) connected to the phone port(s) is busy.
Busy Forward to Number	Enable this feature to have the Prestige forward incoming calls to the number that you configure when the phone(s) connected to the phone port(s) is busy. With call waiting a second call is only forwarded after being rejected.
No Answer Forward to Number	Enable this feature to have the Prestige forward incoming calls to the number that you configure whenever you do not answer the call after a specific time period.
No Answer Waiting Time	Set how long the Prestige should let a call ring before considering the call unanswered.
Advanced Setup	Configure **Advanced Setup** call forwarding entries to have the Prestige perform specific actions on calls from specific numbers. If a caller's number does not match the **Incoming Call Number** of any of these entries, the Prestige performs the default action configured in the **Forward to Number Setup** section.
Activate	Select this check box to turn on an call forwarding entry.
Incoming Call Number	You can set the Prestige to take a particular action on incoming calls from a number that you specify here.
Forward to Number	You can set the Prestige to forward incoming calls to a number that you specify here.
Condition	Select under what circumstances you want the Prestige to use this call forwarding entry. Select **Unconditional** to have the Prestige immediately forward any calls from the number specified in the **Incoming Call Number** field to the number in the **Forward to Number** field. Select **Busy** to have the Prestige forward any calls from the number specified in the **Incoming Call Number** field to the number in the **Forward to Number** field when your SIP account has a call connected. Select **No Answer** to have the Prestige forward any calls from the number specified in the **Incoming Call Number** field to the number in the **Forward to Number** field when the **No Answer Waiting Time** period expires (whether or not the no answer feature is enabled in the **Forward to Number Setup** section). Select **Block** to have the Prestige reject calls from the number specified in the call forwarding entry. Select **Accept** to have the Prestige allow calls from the number specified in the **Incoming Call Number** field.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4 Lifeline Configuration (Prestige 2002L)

Click **PHONEBOOK** in the navigation panel and then **Lifeline** to display the following screen.

Figure 32 Lifeline



The following table describes the labels in this screen.

Table 22 Lifeline

LABEL	DESCRIPTION
PSTN Pre-fix Number	Specify the prefix number for dialing regular calls.
Relay to PSTN	Use these fields to specify phone numbers to which the Prestige will always send calls through the regular phone service without the need of dialing a prefix number. These numbers must be for phones on the PSTN (not VoIP phones).
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 9
Logs

This chapter contains information about the Prestige's **Logs** screen. Refer to the Appendices for example log message explanations.

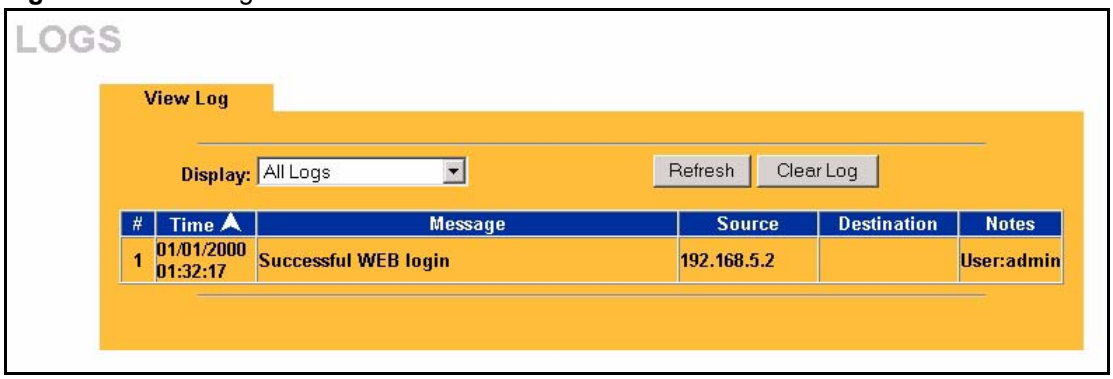
9.1 Viewing Logs

The web configurator allows you to look at all of the Prestige's logs in one location.

Click **LOGS** in the navigation panel to open the **View Log** screen. Use the **View Log** screen to display the Prestige's logs.

Log entries in red indicate system error logs. Once the log table is full, old logs are deleted as new logs are created. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 33 View Log



The following table describes the labels in this screen.

Table 23 View Log

LABEL	DESCRIPTION
Display	Select **All Logs** to view all of the Prestige's logs. Select **System Maintenance** to view the Prestige's maintenance logs. Select **System Error** to view the Prestige's error logs. Select **SIP** to view Session Initiation Protocol logs. Select **RTP** to view Real time Transport Protocol logs. Select **FSM** to view Finite State Machine logs. These logs record phone actions.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
Time	This field displays the time the log was recorded. To configure the Prestige's time and date, see Chapter 3 on page 35.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.

Table 23 View Log (continued)

LABEL	DESCRIPTION
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.

9.2 Log Message Descriptions

The following tables provide descriptions of example log messages.

Table 24 System Error Logs

LOG MESSAGE	DESCRIPTION
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 25 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The device has adjusted its time based on information from the time server.
`Time calibration failed`	The device failed to get information from the time server.
`WAN interface gets IP: %s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`Successful WEB login`	Someone has logged on to the device's web configurator interface.
`WEB login failed`	Someone has failed to log on to the device's web configurator interface.
`Successful FTP login`	Someone has logged on to the device via ftp.
`FTP login failed`	Someone has failed to log on to the device via ftp.
`Time initialized by Daytime Server`	The device got the time and date from the Daytime server.
`Time initialized by Time server`	The device got the time and date from the time server.
`Time initialized by NTP server`	The device got the time and date from the NTP server.
`Connect to Daytime server fail`	The device was not able to connect to the Daytime server.
`Connect to Time server fail`	The device was not able to connect to the Time server.
`Connect to NTP server fail`	The device was not able to connect to the NTP server.

Table 25 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`Too large ICMP packet has been dropped`	The device dropped an ICMP packet that was too large.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The device is saving configuration changes.

Table 26 SIP Logs

LOG MESSAGE	DESCRIPTION
`SIP Registration Success by SIP:SIP Phone Number`	The listed SIP account was successfully registered with a SIP register server.
`SIP Registration Fail by SIP:SIP Phone Number`	An attempt to register the listed SIP account with a SIP register server was not successful.
`SIP UnRegistration Success by SIP:SIP Phone Number`	The listed SIP account's registration was deleted from the SIP register server.
`SIP UnRegistration Fail by SIP:SIP Phone Number`	An attempt to delete the listed SIP account's registration from the SIP register server failed.

Table 27 RTP Logs

LOG MESSAGE	DESCRIPTION
`Error, RTP init fail`	The initialization of an RTP session failed.
`Error, Call fail: RTP connect fail`	A VoIP phone call failed because the RTP session could not be established.
`Error, RTP connection cannot close`	The termination of an RTP session failed.

Table 28 FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number`	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
`VoIP Call Established Ph[Phone Port] -> Outgoing Call Number`	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call made from a phone connected to the listed phone port has terminated.

Table 29 FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start from SIP[SIP Port Number]`	A VoIP phone call came to the Prestige from the listed SIP number.
`VoIP Call Established Ph[Phone Port] <- Outgoing Call Number`	A VoIP phone call was set up from the listed SIP number to the Prestige.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call that came into the Prestige has terminated.

Table 30 Lifeline Logs

LOG MESSAGE	DESCRIPTION
`PSTN Call Start`	A PSTN call has been initiated.
`PSTN Call End`	A PSTN call has terminated.
`PSTN Call Established`	A PSTN call has been set up.

CHAPTER 10
Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

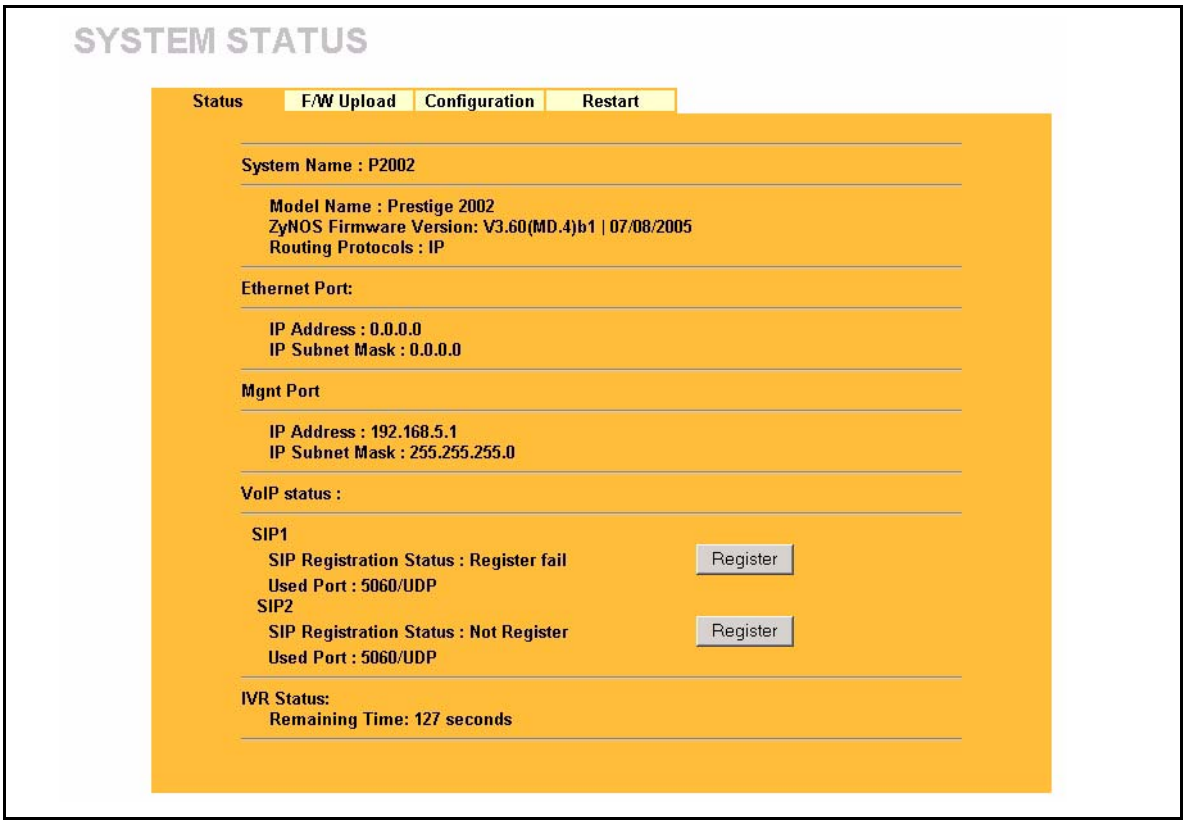
10.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your Prestige.

10.2 Status Screen

Click **MAINTENANCE** in the navigation panel to open the **Status** screen, where you can use to monitor your Prestige. Note that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

Figure 34 System Status



The following table describes the labels in this screen.

Table 31 System Status

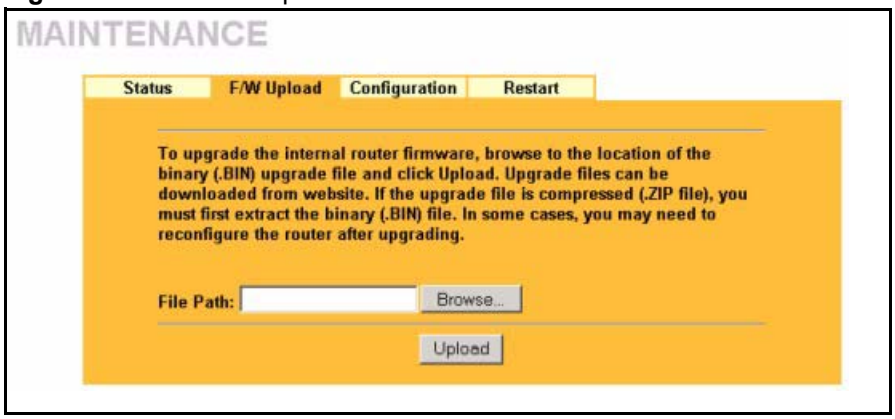
LABEL	DESCRIPTION
System Name	This is the **System Name** you chose in the **SYSTEM General** screen. It is for identification purposes
Model Name	The model name identifies your device type. The model name should also be on a sticker on your device. If you are uploading firmware, be sure to upload firmware for this exact model name.
ZyNOS Firmware Version:	This is the ZyNOS firmware version and the date the firmware was created. ZyNOS is ZyXEL's proprietary Network Operating System.
Ethernet Port	
IP Address	This is the Prestige's IP address. This applies to both of the Prestige's Ethernet ports.
IP Subnet Mask	This is the Prestige's subnet mask. This applies to both of the Prestige's Ethernet ports.
MGNT Port	
IP Address	This is the static IP address of the Prestige's logical Ethernet interface for management.
IP Subnet Mask	This is the subnet mask of the Prestige's logical Ethernet interface for management.
VoIP Status	
SIP1/SIP 2	This is the SIP account configured on the Prestige.
SIP Registration Status	This is the SIP registration status of the SIP account. This field displays **Registered** when the Prestige has successfully registered the SIP account with the SIP register server. This field displays **Not Registered** when the Prestige has not successfully registered the SIP account with the SIP register server.
Register/ Unregister	Click **Register** to have the Prestige attempt to register the SIP account with the SIP register server. Click **Unregister** to delete the SIP account's registration on the SIP register server. This removes the SIP registration server's SIP identity-to-IP address (or domain name) mapping for this SIP account, it does not cancel your SIP account.
Used Port	This field displays the Prestige's listening port for SIP traffic on this SIP account.
Custom Tone (IVR) Status	IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Prestige. You can use your phone to record custom tones for the caller ringing and on hold tone functions. This field displays the **Remaining Time** left for recording custom tones.

10.3 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "Prestige.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **MAINTENANCE** in the navigation panel and then the **F/W UPLOAD** tab. Follow the instructions in this screen to upload firmware to your Prestige.

Figure 35 Firmware Upload



The following table describes the labels in this screen.

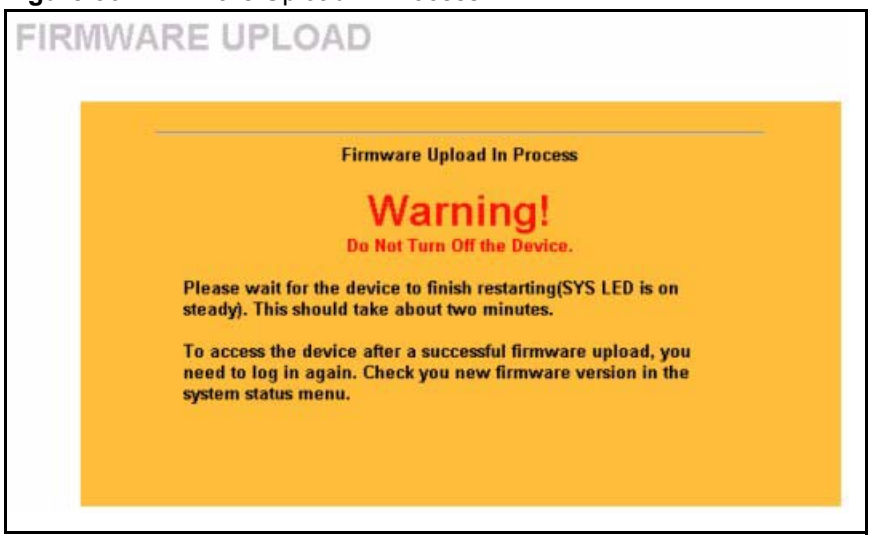
Table 32 Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the device while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the device again.

Figure 36 Firmware Upload In Process



The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 37 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **System Status** screen.

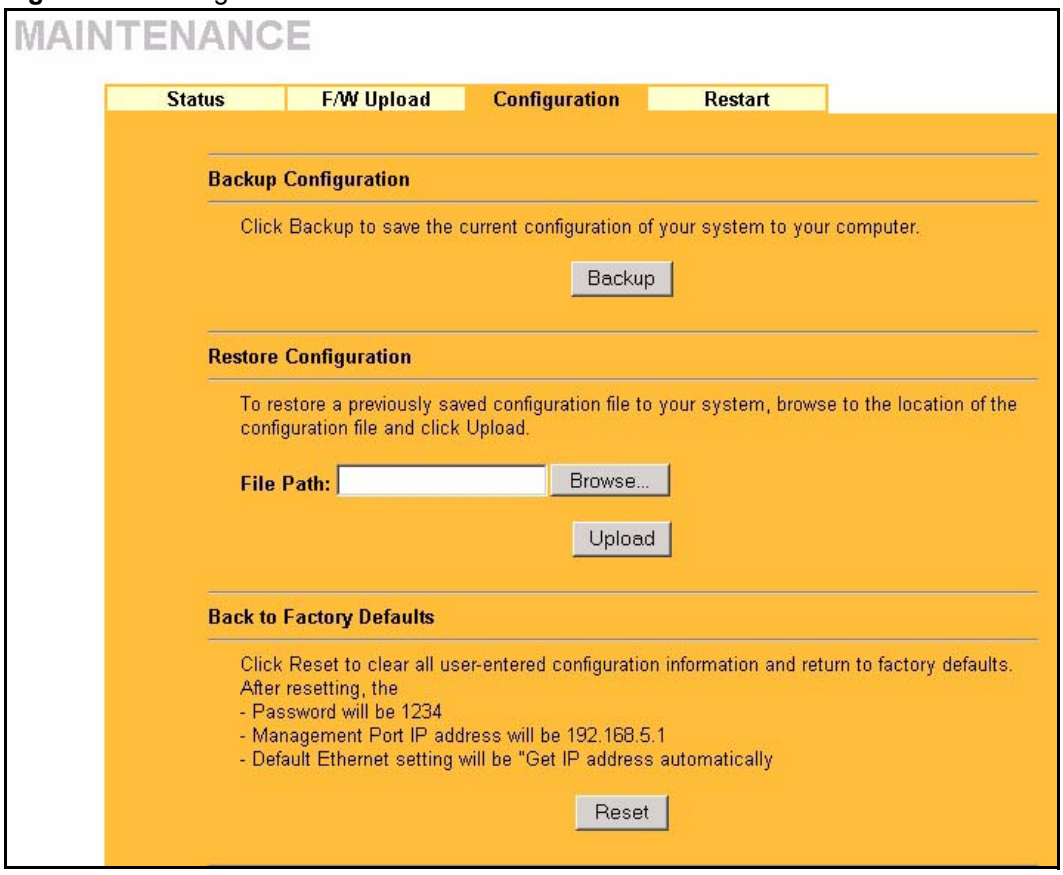
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 38 Firmware Upload Error

10.4 Configuration Screen

Click **MAINTENANCE** in the navigation panel and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 39 Configuration



10.4.1 Backup Configuration

Backup Configuration allows you to back up (save) the device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the device's current configuration to your computer.

10.4.2 Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Prestige.

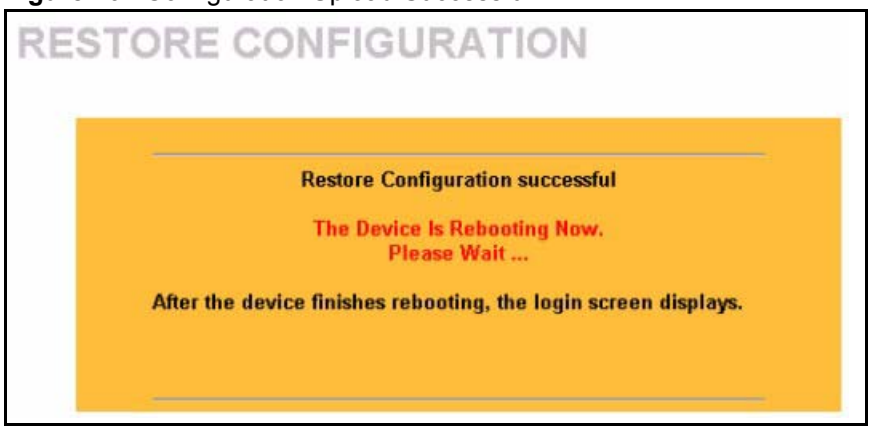
Table 33 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Note: Do not turn off the device while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the device again.

Figure 40 Configuration Upload Successful



The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 41 Network Temporarily Disconnected

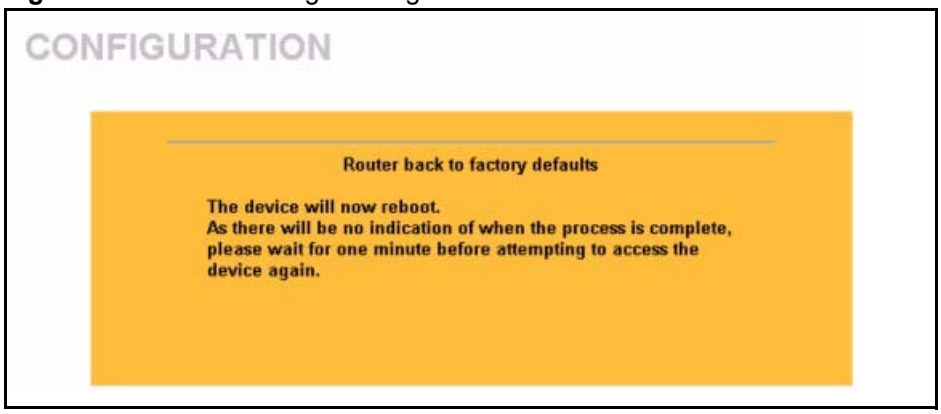
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See your *Quick Start Guide* or the appendices for details on how to set up your computer's IP address.

If the upload was not successful, a **Configuration Upload Error** screen will appear. Click **Return** to go back to the **Configuration** screen.

10.4.3 Back to Factory Defaults

Clicking the **Reset** button in this section clears all user-entered configuration information and returns the Prestige to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 42 Reset Warning Message



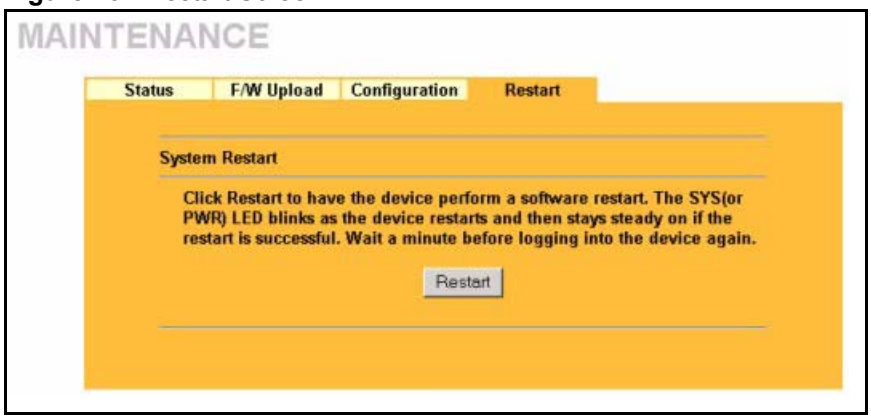
You can also press the **RESET** button on the rear panel to reset the factory defaults of your Prestige. For more information on the **RESET** button, see Section 2.3 on page 31.

10.5 Restart Screen

System restart allows you to reboot the Prestige without turning the power off.

Click **MAINTENANCE** in the navigation panel and then **Restart**. Click **Restart** to have the Prestige reboot. This does not affect the Prestige's configuration.

Figure 43 Restart Screen



CHAPTER 11
Phone Usage

This chapter describes how to use a phone connected to your Prestige for basic tasks.

11.1 Dialing a Telephone Number

The **VoIP/PWR** LED turns orange when your SIP account is registered. Dial a SIP number like "12345" on your phone's keypad.

Use speed dial entries (see Section 8.2 on page 75) for peer-to-peer calls or SIP numbers that use letters. Dial the speed dial entry on your telephone's keypad.

Use your voice service provider's dialing plan to call regular telephone numbers.

11.2 Using Speed Dial to Dial a Telephone Number

After configuring the speed dial entry and adding it to the phonebook, press the speed dial entry's key combination on your phone's keypad.

11.3 Internal Calls

Press "####" on your phone's keypad to call the Prestige's other phone port.

11.4 Checking the Prestige's IP Address

Do the following to listen to the Prestige's IP current address.

1. Pick up your phone's receiver.
2. Press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
3. Press "5" followed by the # key.
4. Listen to the IP address and make a note of it.
5. Hang up the receiver.

11.5 Auto Firmware Upgrade

During auto-provisioning, the Prestige checks to see if there is a newer firmware version. If newer firmware is available, the Prestige plays a recording when you pick up your phone's handset.

Press "*99#" to upgrade the Prestige's firmware.

Press "#99#" to not upgrade the Prestige's firmware.

CHAPTER 12
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

12.1 Problems Starting Up the Prestige

Table 34 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adaptor is connected to the Prestige and an appropriate power source. Check that the power source is turned on. Disconnect the Prestige's power and reconnect it. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

12.2 Problems with the LAN or PC LED

Table 35 Troubleshooting the LAN or PC LED

PROBLEM	CORRECTIVE ACTION
The LAN or PC LED does not turn on.	Check your Ethernet cable connections and type (refer to the *Quick Start Guide* for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet card is working properly.

12.3 Problems with the LAN Interface

Table 36 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN.	If the **LAN** or **PC** LED is off, see Table 35 on page 95. Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.
I cannot ping any computer on the LAN.	If the **LAN** and **PC** LEDs are both off, see Table 35 on page 95. Make sure that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.
The Prestige cannot get an IP address from the ISP.	The ISP provides the IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Verify your Ethernet settings, see Chapter 4 on page 41.

12.4 Problems with Internet Access

Table 37 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network. Verify your Ethernet settings, see Chapter 4 on page 41. Make sure you entered the correct user name and password.
Internet connection disconnects.	Contact your ISP.

12.5 Problems with the Web Configurator

Table 38 Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	If the Prestige's Ethernet IP address or management IP address has changed, then enter the new one as the URL. Your computer's IP address must be on the same subnet as the Prestige's Ethernet IP address or management IP address (whichever you use to access the Prestige). See Section 12.9 on page 99 to check that pop-up windows, JavaScripts and Java permissions are allowed. Ping the Prestige. In the computer, click **Start**, (**All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the Prestige's IP address (192.168.5.1 is the default management IP address) and then press [ENTER]. The Prestige should reply. Otherwise, make sure your computer's Ethernet adapter is installed and functioning properly. You may also need to clear your Internet browser's cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Option**s screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it. If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.
I access the wrong Prestige when using the management IP address for access.	This problem may occur if you have more than one Prestige on the same LAN. Disconnect your Prestige from the network and connect directly through the Prestige's **PC** port. You may also need to delete your computer's ARP table entry for the Prestige's IP address (see above).

12.6 Problems with the Password

Table 39 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The username is admin. The default password is 1234. The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to restore the default configuration file (see Section 2.3 on page 31). This restores all of the factory defaults including the password.

12.7 Problems with Telephone or Telephone Port

Table 40 Troubleshooting Telephone

PROBLEM	CORRECTIVE ACTION
There is no dial tone or I can't make or receive calls. or There is beeping instead of the dial tone.	Check the telephone connections and telephone wire. Beeping means that there is not a SIP account registered for the phone to use. You can check the Prestige's IP addresses and VoIP status in the **Maintenance Status** screen. Make sure you have the **VoIP** screen properly configured. If you configured a SIP account to receive calls on only one of the phone ports, make sure your phone is connected to that port. Make sure you have the **Phone Port** screen properly configured. If you configured a phone port to only use one of the SIP accounts for outgoing calls, make sure that SIP account is properly configured and active (see the **VoIP** and **Maintenance Status** screens).
There is a beep before the dial tone.	A single beep before the dial tone indicates that there is a voice message for SIP account 1. Two beeps before the dial tone indicate that there is a voice message for SIP account 2. Use your voice service provider's instructions to check your voice messages.

12.8 Problems with Voice Service

Table 41 Troubleshooting Voice Service

PROBLEM	CORRECTIVE ACTION
After the VoIP is configured and working, others are unable to call you or you lose your connection during a call. There is a NAT router between the Prestige and the SIP server.	This could be caused by a short NAT UDP session timeout on the NAT router. When the SIP session's entry in the NAT table times out, the NAT router does not have any record to use for forwarding VoIP traffic to the Prestige. If possible, set the NAT router to use a longer NAT UDP session timeout. Otherwise, try one of the following: • Shorten the registration expiration period (see the **Expiration Duration** field in the **VoIP Advanced** screen) in order to cause the Prestige to re-register with the SIP register server more frequently. Note that this will not help if the SIP register server enforces a long registration expiration period (since the Prestige will also use the period set by the SIP register server). • Use STUN. If your VoIP service provider does not have a STUN server, you can still enable STUN and enter the IP address and port number of the SIP server in the STUN server fields. This causes the Prestige to send STUN requests to the SIP server. While this will not make STUN work (since there won't be any responses to the STUN requests), it should keep the NAT UDP session in the NAT router.

12.9 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

12.9.1 Internet Explorer Pop-up Blockers

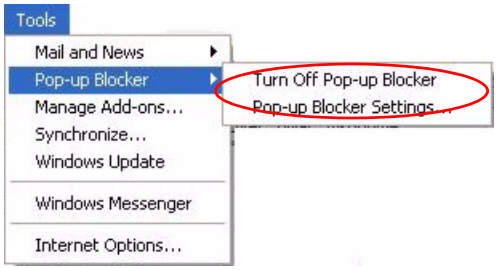
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

12.9.1.1 Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 44 Pop-up Blocker

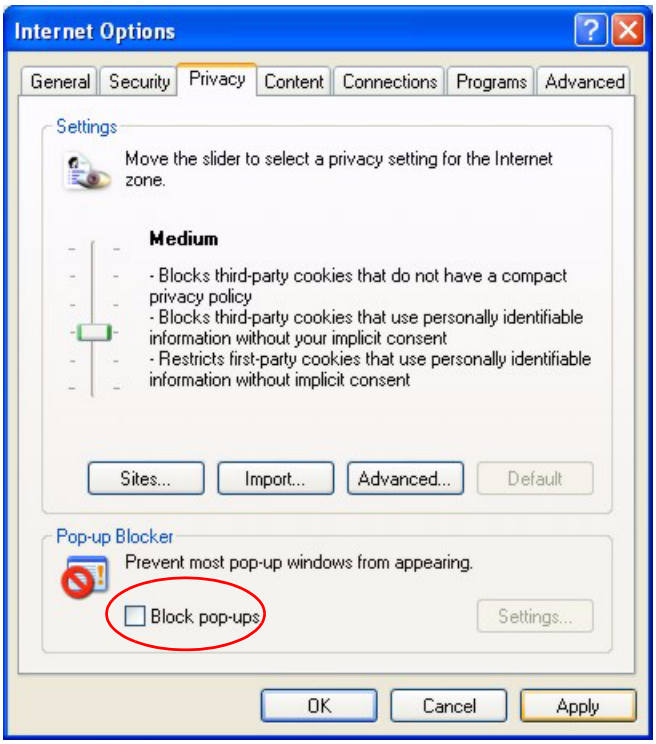


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 45 Internet Options



3 Click **Apply** to save this setting.

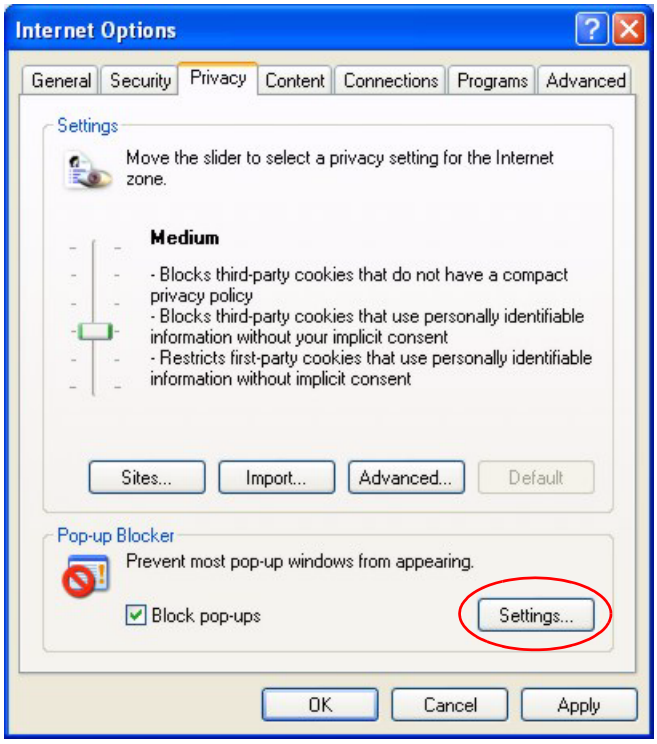
12.9.1.2 Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 46 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 47 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

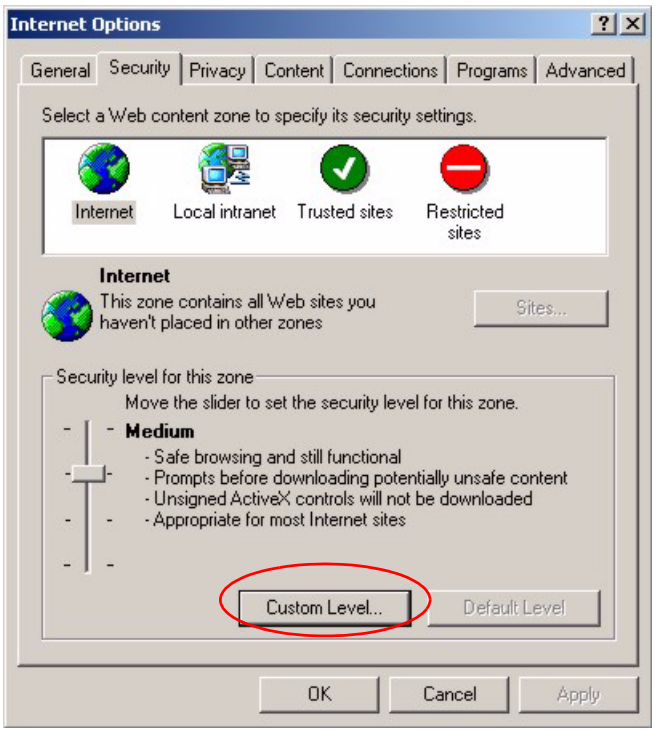
6 Click **Apply** to save this setting.

12.9.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 48 Internet Options



2 Click the **Custom Level...** button.

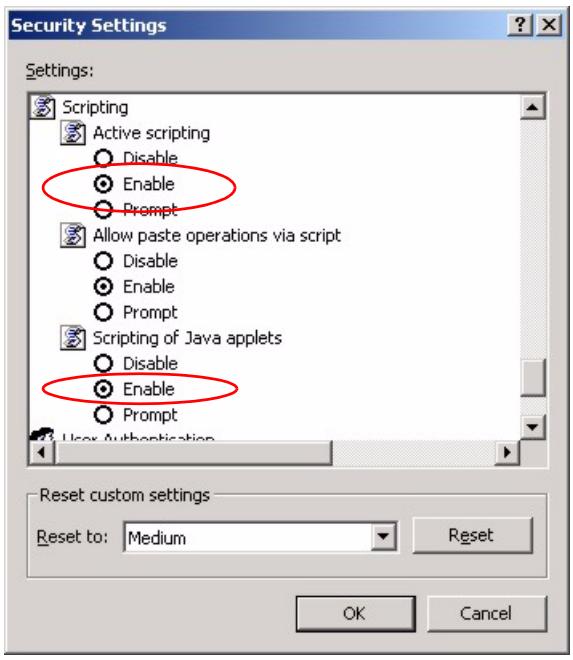
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 49 Security Settings - Java Scripting



12.9.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

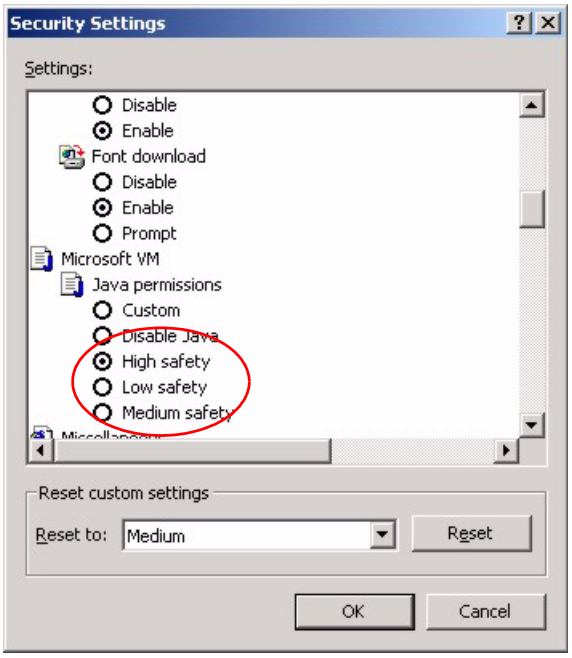
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 50 Security Settings - Java



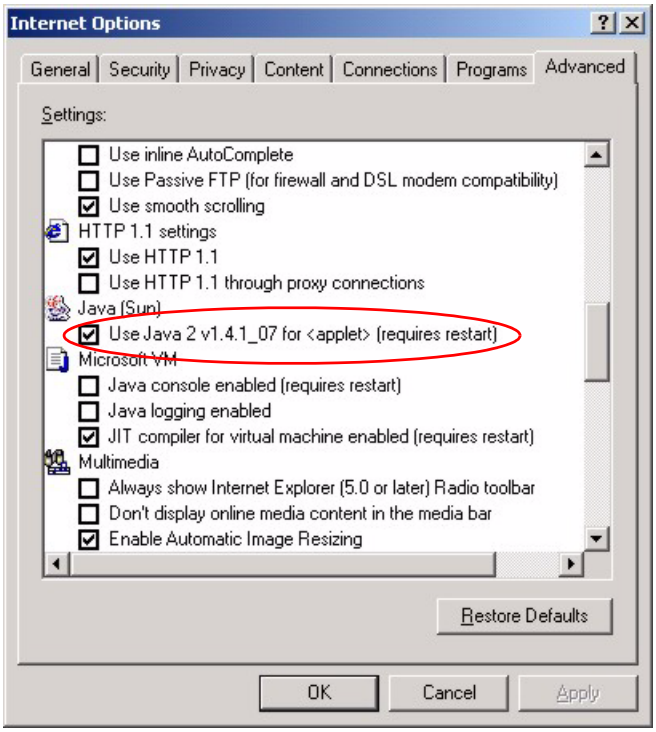
12.9.3.1 JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 51 Java (Sun)



APPENDIX A
Product Specifications

See also the introduction chapter for a general overview of the key features.

Specification Tables

Table 41 Device Specifications

Default Management IP Address	192.168.5.1
Default Management Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Dimensions	109 (Wide) x 105 (Deep) x 22 (High) mm
Weight	312 g
Ethernet Ports	Two auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
Phone Ports	2 RJ-11 Analog Telephone ports
Feeding Voltage	On hook: -48V; Minimum Voltage: -20V Off hook: -24V
Ringing Voltage	40V RMS at 3 REN
Line Ports (P2002L Only)	1 FXO (Foreign Exchange Office) port
Operation Temperature	0º C ~ 40º C
Storage Temperature	0º ~ 60º C
Operation Humidity	10% ~ 85% RH
Storage Humidity	10% ~ 90% RH
Network Features	PPPoE client DHCP client Friendly web-based configuration tool Telnet management FTP/TFTP firmware upgrade and configuration backup/restore IVR for IP address and FW upgrade Secure TFTP and HTTP auto-provisioning (3DES default encryption) Supports NAT Traversal (RFC 3489)

Table 42 Feature Specifications

Voice Functions	SIP (RFC 3261) version 2 SDP (RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) G.168 Echo Cancellation VAD (Voice Activity Detection) Silence Suppression CNG (Comfort Noise Generation) VLAN tag support QoS Supports TOS and Diffserv Tagging RTP Voice Highest Priority Codec: G.711 (PCM), G.729 (ADPCM) Loop Start Signaling Support Modem and Fax Tone Detection and Pass Through DTMF Detection Multiple SIP number supports Multiple Channel Supports T.38 Fax Relay Point to Point Calling (Direct IP to IP Calling) Speed Dial (Phonebook) Lifeline Support (P-2002L) Support NAT Traversal / RFC3489- IETF Simple Traversal of UDP Through NAT (STUN) Caller ID Dialing Type: Tone, Pulse (Auto detection) Ring cadence frequency can be tuned by firmware Tip/ring polarity reversal
Call Features	Call Waiting (CW) w/ caller ID Call Forwarding (unconditional/busy/no answer) Call Transferring (blind/consult/on hold/attendant) Three way conference call with local mixing CLIP (Calling Line Identification Presentation) CLIR (Calling Line Identification Restriction) Call Hold/Retrieve/Block Incoming Call Policy (Accept/Forward/Block) Second Call Internal Call Flash Hook Timer Caller Ringing Tone (Early Media) On Hold Tone Message Waiting Indicator (RFC 3824), Visualized MWI, MWI by e-mail IVR (Interactive Voice Response)

Table 42 Feature Specifications (continued)

Custom Tones (IVR)	120 seconds total memory time 20 second maximum per tone You can record up to ten different custom tones but the total time must be 120 seconds or less. For example you could record up to ten 12-second tones or up to six 20-second tones.
Protocol Support	PPP over Ethernet (RFC 2516) Transparent bridging for unsupported network layer protocols DHCP Client
Management	Embedded Web Configurator CLI (Command Line Interpreter) Remote Management via Telnet or Web SNMP manageable FTP/TFTP for firmware downloading, configuration backup and restoration Syslog Built-in Diagnostic Tools for FLASH memory, RAM and LAN port
Static Routes	16 IP and 4 Bridge
Hardware Features	Restore Factory Defaults/Reboot Button Status LEDs • POWER/VoIP (Green/Orange) • Green blinking: self testing • Green on: power and system on • Orange on: VoIP SIP register ok • Off: power off • ETHERNET (Green) • Green solid: ethernet link successful • Green blinking: ethernet data is transmitting • PHONE (Green) • On: when voice port is off hook • Off: when voice port is connected • Blinking: telephone ringing
Other Features	Internal SPTGEN DNS Proxy UNIX syslog

Power Adaptor Specifications

Table 43 Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-1215A

Table 43 Power Adaptor Specifications (continued)

Input Power	AC120Volts/60Hz/30W
Output Power	AC12Volts/1.25A
Power Consumption	14 W
Safety Standards	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A25
Input Power	AC120Volts/60Hz/19W
Output Power	AC 12Volts/ 1.25A
Power Consumption	14W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A3BN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.3A
Power Consumption	14W
Safety Standards	ITS-GS, CE (EN 60950)
UNITED KINGDOM PLUG STANDARDS (P2002L ONLY)	
AC Power Adapter Model	AA-121A3D
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.3A
Power Consumption	14W
Safety Standards	ITS-GS, CE (EN 60950)

APPENDIX B
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

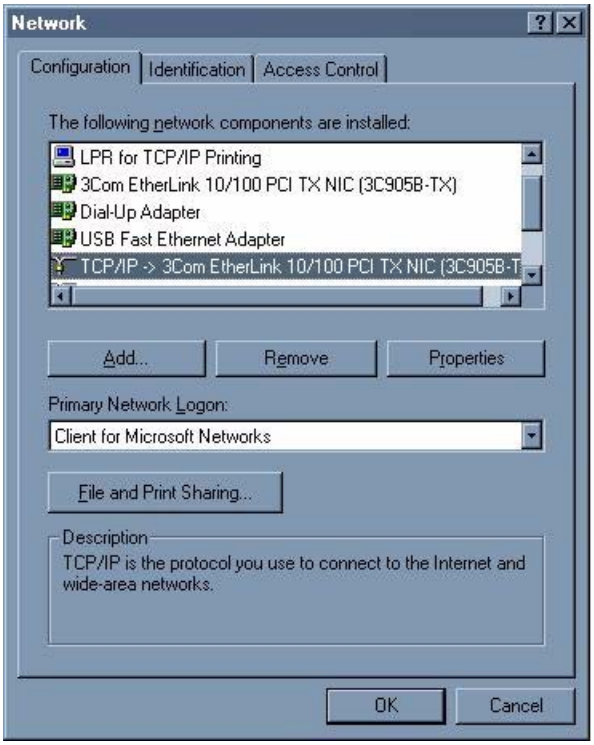
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 52 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

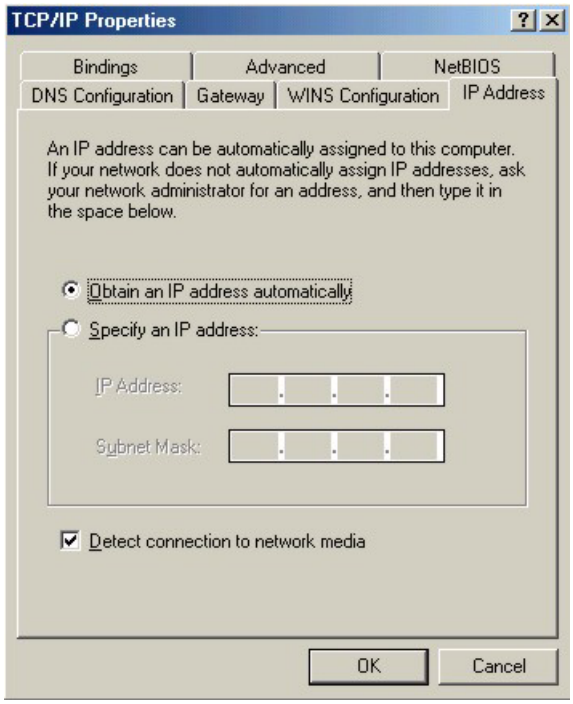
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

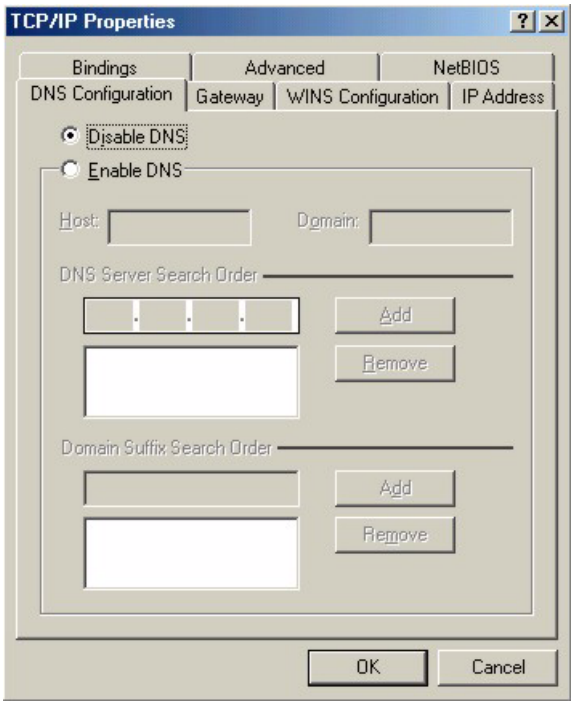
Figure 53 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 54 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

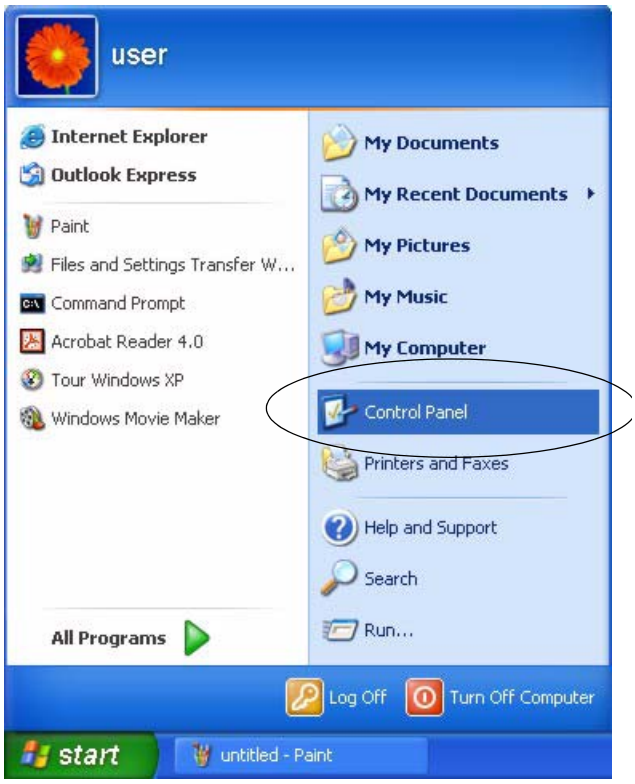
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

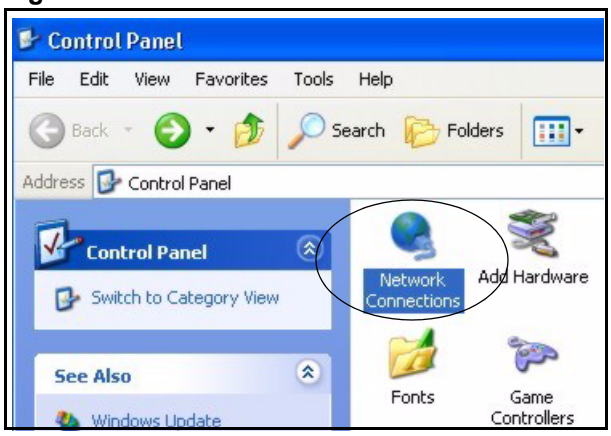
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 55 Windows XP: Start Menu



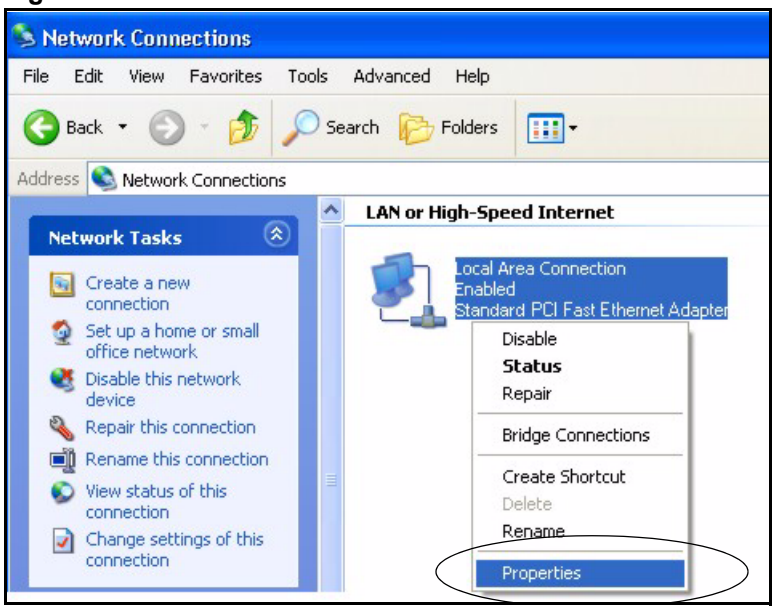
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 56 Windows XP: Control Panel



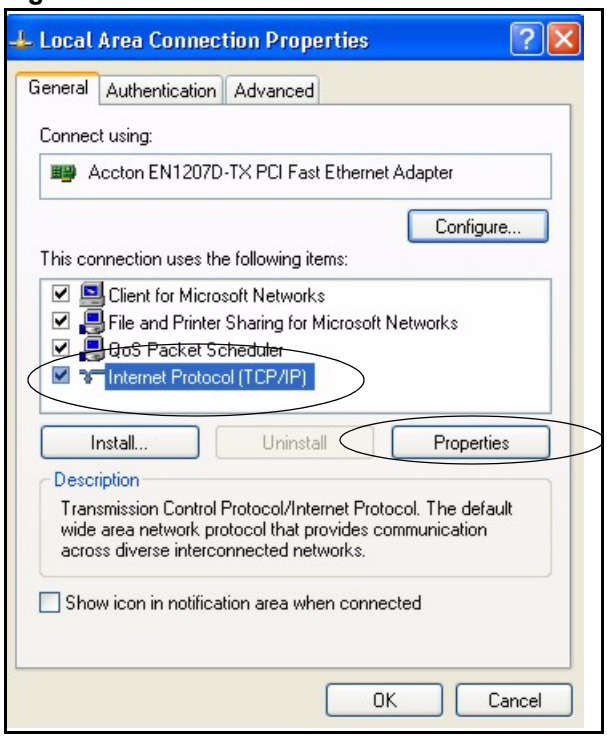
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 57 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 58 Windows XP: Local Area Connection Properties

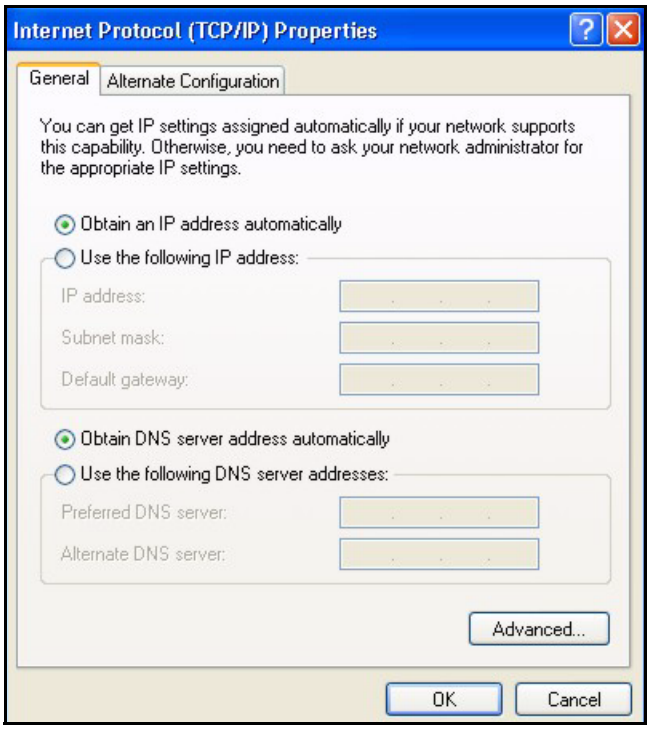


5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 59 Windows XP: Internet Protocol (TCP/IP) Properties

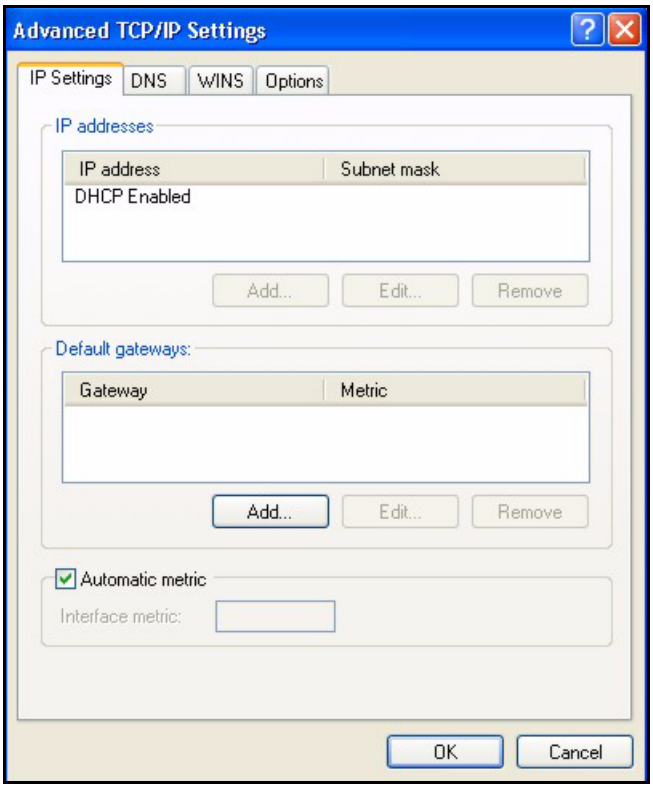


6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 60 Windows XP: Advanced TCP/IP Properties

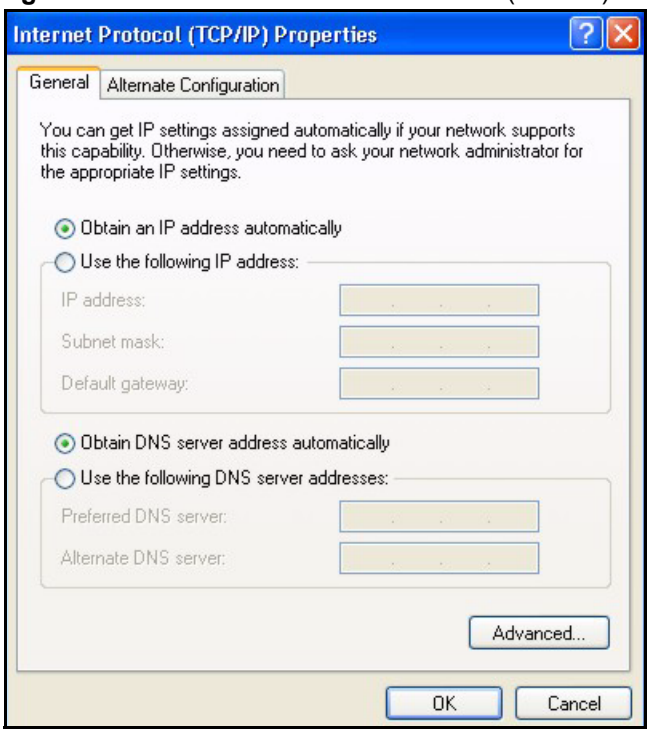


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 61 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

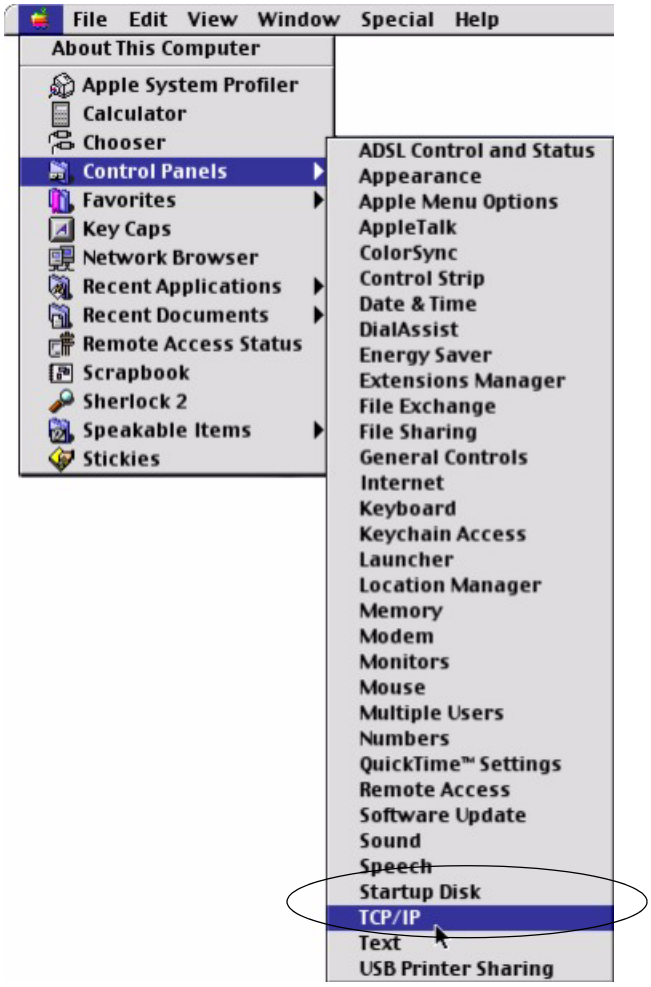
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

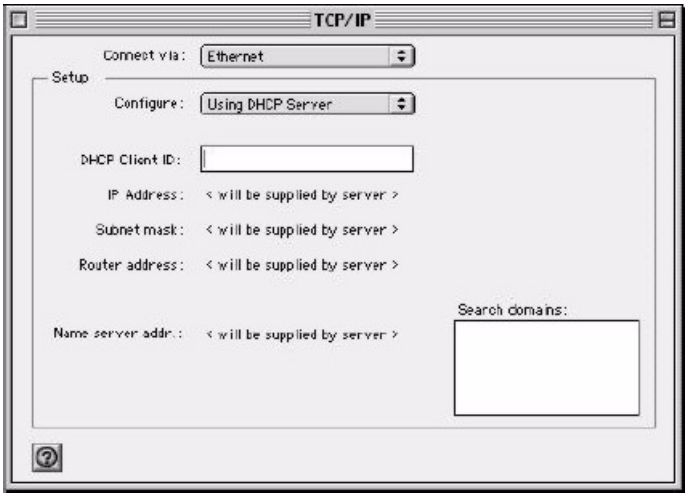
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 62 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 63 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Prestige and restart your computer (if prompted).

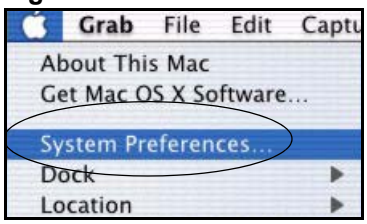
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 64 Macintosh OS X: Apple Menu

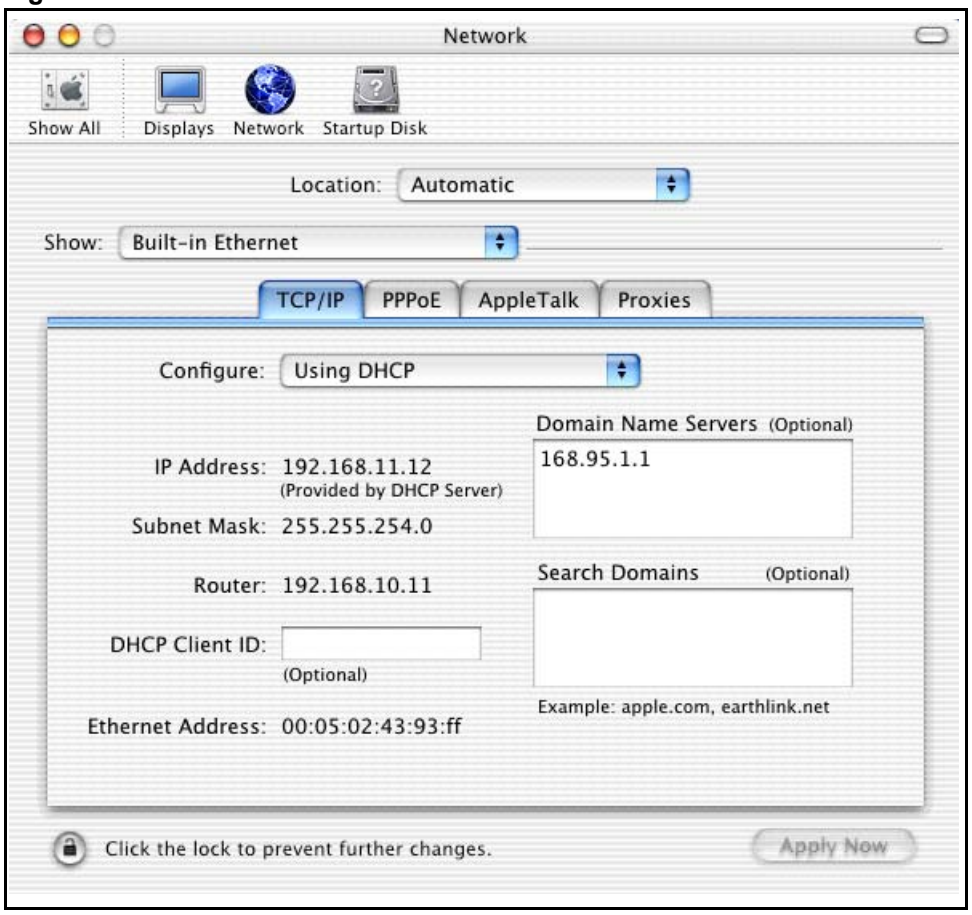


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 65 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

APPENDIX C
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Table 44 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.

A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Table 45 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Table 46 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Table 47 Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 48 Two Subnets Example

IP/SUBNET MASK	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Table 49 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 50 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Table 51 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 52 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 53 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 54 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 55 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class "C" subnet planning.

Table 56 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 44 on page 123) available for subnetting.

The following table is a summary for class "B" subnet planning.

Table 57 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

APPENDIX D
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see Figure 66 on page 132). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

It provides you with a familiar dial-up networking (DUN) user interface.

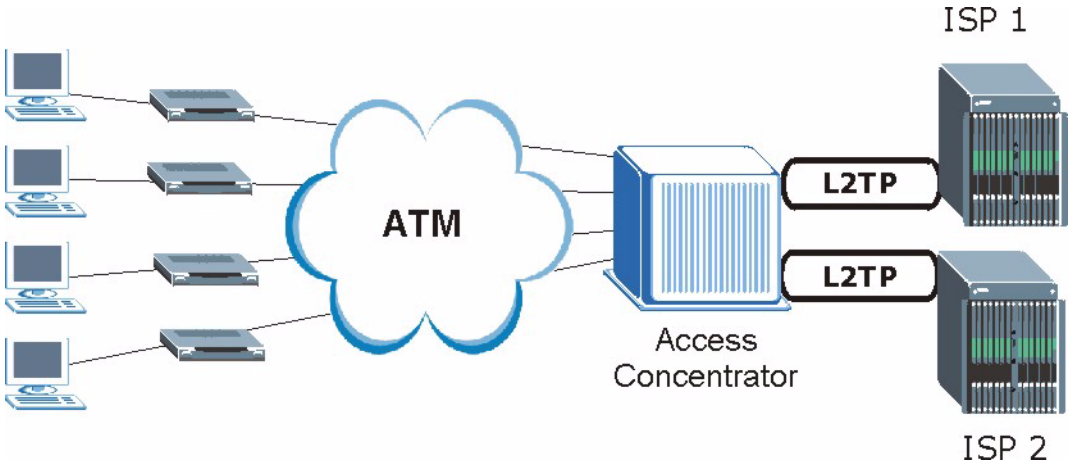
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

Figure 66 Single-Computer per Router Hardware Configuration



How PPPoE Works

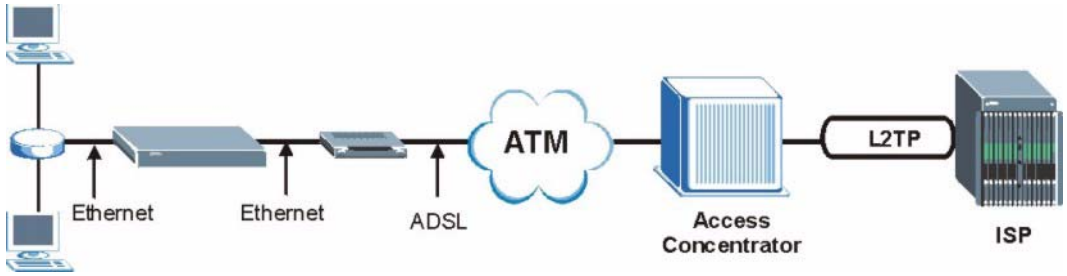
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

Figure 67 Prestige as a PPPoE Client



APPENDIX E
Internal SPTGEN

Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple Prestiges. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to configure each Prestige.

The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

```
<field identification number = field name = parameter values
allowed = input>,
```

where <input> is your input conforming to <parameter values allowed>.

The figure shown next is an example of an Internal SPTGEN text file.

Figure 68 Configuration Text File Format: Column Descriptions

```
/ Menu 1 General Setup
 10000000 = Configured                <0(No)| 1(Yes)>       = 1
 10000001 = System Name               <Str>                 = Prestige
 10000002 = Location                  <Str>                 =
 10000003 = Contact Person's Name     <Str>                 =
 10000004 = Route IP                  <0(No)| 1(Yes)>       = 1
 10000005 = Route IPX                <0(No)| 1(Yes)>       = 0
 10000006 = Bridge                   <0(No)| 1(Yes)>       = 0
```

Note: DO NOT alter or delete any field except parameters in the Input column.

Internal SPTGEN File Modification - Important Points to Remember

Each parameter you enter must be preceded by one "="sign and one space.

Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see Figure 68 on page 133), then you disable every field in this menu.

If you enter a parameter that is invalid in the **Input** column, the Prestige will not save the configuration and the command line will display the **Field Identification Number**. Figure 69 on page 134, shown next, is an example of what the Prestige displays if you enter a value other than "0" or "1" in the **Input** column of **Field Identification Number** 1000000 (refer to Figure 68 on page 133).

Figure 69 Invalid Parameter Entered: Command Line Example

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

The Prestige will display the following if you enter parameter(s) that *are* valid.

Figure 70 Valid Parameter Entered: Command Line Example

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Internal SPTGEN FTP Download Example

1. Launch your FTP application.
2. Enter "`bin`". The command "`bin`" sets the transfer mode to binary.
3. Get "`rom-t`" file. The command "`get`" transfers files from the Prestige to your computer. The name "`rom-t`" is the configuration filename on the Prestige.
4. Edit the "`rom-t`" file using a text editor (do not use a word processor). You must leave this FTP screen to edit.

Figure 71 Internal SPTGEN FTP Download Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)
```

Note: You can rename your "`rom-t`" file when you save it to your computer but it must be named "`rom-t`" when you upload it to your Prestige.

Internal SPTGEN FTP Upload Example

1. Launch your FTP application.
2. Enter "`bin`". The command "`bin`" sets the transfer mode to binary.
3. Upload your "`rom-t`" file from your computer to the Prestige using the "`put`" command. computer to the Prestige.
4. Exit this FTP application.

Figure 72 Internal SPTGEN FTP Upload Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

Example Internal SPTGEN Screens

This appendix introduces Internal SPTGEN. All menus shown in this appendix are example menus meant to show Internal SPTGEN usage. Actual menus for your product may differ.

Table 58 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number (not seen in SMT screens)
FN	Field Name
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the Prestige.

The following are Internal SPTGEN screens associated with the SMT screens of your Prestige.

Table 59 Menu 1 General Setup

/ Menu 1 General Setup			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0(No) | 1(Yes)>	= 0
10000001 =	System Name	<Str>	= Prestige
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0(No) | 1(Yes)>	= 1
10000006 =	Bridge	<0(No) | 1(Yes)>	= 0
10000007 =	First System DNS Server Type	<0(From ISP) | 1(User Defined) | 2(None)>	= 0
10000008 =	First System DNS Server IP address		= 0.0.0.0
10000009 =	Second System DNS Server Type	<0(From ISP) | 1(User Defined) | 2(None)>	= 0
10000010 =	Second System DNS Server IP address		= 0.0.0.0
10000011 =	Third System DNS Server Type	<0(From ISP) | 1(User Defined) | 2(None)>	= 0
10000012 =	Third System DNS Server IP address		= 0.0.0.0

Table 60 Menu 4 Internet Access Setup

/ Menu 4 Internet Access Setup			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0(No) | 1(Yes)>	= 1
40000001 =	ISP	<0(No) | 1(Yes)>	= 1

Table 60 Menu 4 Internet Access Setup (continued)

40000002 =	Active	<0(No) | 1(Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@pqa
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0(No) | 1(Yes)>	= 1
40000012 =	IP Address Assignment	<0(Static)|1(Dynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0(No) | 1(Yes)>	= 1
40000031=	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
40000032=	RIP Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0(No) |1(Yes)>	= 0
40000034=	LAN IP Address		= 0.0.0.0
40000035=	LAN IP subnet mask Bits		= 0
40000036=	LAN Gateway		= 0.0.0.0

Table 61 Menu 12

/ Menu 12.1.1 IP Static Route Setup			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0(No) |1(Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.2 IP Static Route Setup			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0(No) |1(Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.3 IP Static Route Setup			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=
120103002 =	IP Static Route set #3, Active	<0(No) |1(Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.4 IP Static Route Setup			
FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0(No) |1(Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0

Table 61 Menu 12 (continued)

120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.5 IP Static Route Setup			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0(No) |1(Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.6 IP Static Route Setup			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0(No) |1(Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.7 IP Static Route Setup			
FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0(No) |1(Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0
120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.8 IP Static Route Setup			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=

Table 61 Menu 12 (continued)

120108002 =	IP Static Route set #8, Active	<0(No) |1(Yes)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(No) |1(Yes)>	= 0

Table 62 Menu 15 SUA Server Setup

/ Menu 15 SUA Server Setup			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0(No) | 1(Yes)>	= 0
150000003 =	SUA Server #2 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0
150000007 =	SUA Server #3 Active	<0(No) | 1(Yes)>	= 0
150000008 =	SUA Server #3 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0(No) | 1(Yes)>	= 0
150000013 =	SUA Server #4 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0(No) | 1(Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0
150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0(No) | 1(Yes)> = 0	= 0

Table 62 Menu 15 SUA Server Setup (continued)

150000023 =	SUA Server #6 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0(No) | 1(Yes)>	= 0
150000028 =	SUA Server #7 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0
150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0(No) | 1(Yes)>	= 0
150000033 =	SUA Server #8 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0(No) | 1(Yes)>	= 0
150000038 =	SUA Server #9 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0
150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042 =	SUA Server #10 Active	<0(No) | 1(Yes)>	= 0
150000043 =	SUA Server #10 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0
150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0(No) | 1(Yes)>	= 0
150000048 =	SUA Server #11 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0(No) | 1(Yes)>	= 0
150000053 =	SUA Server #12 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0

Table 63 Menu 21.1 Filter Set #1

/ Menu 21 Filter set #1			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=
/ Menu 21.1.1.1 set #1, rule #1			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type	<2(TCP/IP)>	= 2
210101002 =	IP Filter Set 1,Rule 1 Active	<0(No)|1(Yes)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.1.2 set #1, rule #2			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0(No)|1(Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0

Table 63 Menu 21.1 Filter Set #1 (continued)

210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.1.3 set #1, rule #3			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type	<2(TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0(No)|1(Yes)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210103013 =	IP Filter Set 1,Rule 3 Act Match	<1(check next)|2(forward)|3(drop)	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.4 set #1, rule #4			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2(TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0(No)|1(Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0

Table 63 Menu 21.1 Filter Set #1 (continued)

210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1(check next)|2(forward) |3(drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.5 set #1, rule #5			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2(TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0(No)|1(Yes)>	= 1
210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0
210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1(Check Next)|2(Forward)|3(Drop)>	= 1
/ Menu 21.1.1.6 set #1, rule #6			
FIN	FN	PVA	INPUT

Table 63 Menu 21.1 Filter Set #1 (continued)

210106001 =	IP Filter Set 1,Rule 6 Type	<2(TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0(No)|1(Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2

Table 64 Menu 21.1 Filer Set #2

/ Menu 21.1 Filter set #2			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Name	<Str>	= NetBIOS_WAN
/ Menu 21.1.2.1 Filter set #2, rule #1			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2, Rule 1 Type	<0(none)|2(TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0(No)|1(Yes)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137

Table 64 Menu 21.1 Filer Set #2 (continued)

210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0
210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.2 Filter set #2, rule #2			
FIN	FN	PVA	INPUT
210202001 =	IP Filter Set 2, Rule 2 Type	<0(none)|2(TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0(No)|1(Yes)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0
210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2,Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1(check next)|2(forward)|3(drop)>	= 3

Table 64 Menu 21.1 Filer Set #2 (continued)

210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.3 Filter set #2, rule #3			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type	<0(none)|2(TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0(No)|1(Yes)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2,Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210203014 =	IP Filter Set 2,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.4 Filter set #2, rule #4			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0(none)|2(TCP/IP)>	= 2
210204002 =	IP Filter Set 2, Rule 4 Active		<0(No)|1(Yes)> = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137

Table 64 Menu 21.1 Filer Set #2 (continued)

210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.5 Filter set #2, rule #5			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type	<0(none)|2(TCP/IP)>	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0(No)|1(Yes)>	= 1
210205003 =	IP Filter Set 2,Rule 5 Protocol		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0
210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3

Table 64 Menu 21.1 Filer Set #2 (continued)

210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.6 Filter set #2, rule #6			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type	<0(none)|2(TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0(No)|1(Yes)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210206013 =	IP Filter Set 2,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210206014 =	IP Filter Set 2,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2
241100005 =	FTP Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0(all)|1(none)|2(Lan) |3(Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

Table 65 Menu 23 System Menus

*/ Menu 23.1 System Password Setup

Table 65 Menu 23 System Menus (continued)

FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234

Table 66 Menu 24.10 Time and Date Setting

/ Menu 24.10 Time and Date Setting			
FIN	FN	PVA	INPUT
241000001 =	Time Protocol		= 0
241000002 =	Time Server Address		=
241000003 =	Time Zone		= 12
241000004 =	Daylight Saving	<0(No) | 1(Yes)>	= 0
241000005 =	Start Date (month)		= 1
241000006 =	Start Date (day)		= 0
241000007 =	End Date (month)		= 1
241000008 =	End Date (day)		= 0

Table 67 Menu 24.11 Remote Management Control

/ Menu 24.11 Remote Management Control			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port		= 23
241100002 =	TELNET Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21
241100005 =	FTP Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0(all)|1(none)|2(Lan) |3(Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0
241100010 =	SNMP Service Port		= 161
241100011 =	SNMP Service Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100012 =	SNMP Service Secured IP address		= 0.0.0.0
241100013 =	DNS Service Port		= 53

Table 67 Menu 24.11 Remote Management Control (continued)

241100014 =	DNS Service Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100015 =	DNS Service Secured IP address		= 0.0.0.0

Table 68 Menu 98 VoIP and Auto Upgrade Menus

/ Menu 98.1.1 VoIP SIP #1 Setup			
FIN	FN	PVA	INPUT
980101001 =	SIP #1 Active	<0(No) | 1(Yes)>	= 1
980101002 =	SIP #1 Server Address		= sipserver.net
980101003 =	SIP #1 Server Port	<1024~65535>	= 5060
980101004 =	SIP #1 Registartion Server IP		= sipserver.net
980101005 =	SIP #1 Registartion Server Port	<1024~65535>	= 5060
980101006 =	SIP #1 Registartion Expiration Time	<2~65535>	= 3600
980101007 =	SIP #1 Register ReSend Time	<1~65535>	= 180
980101008 =	SIP #1 Session Expire Time	<30~3600>	= 180
980101009 =	SIP #1 Local signaling Port	<1024~65535>	= 5060
980101010 =	SIP #1 RTP Port Range Start	<1024~65535>	= 50000
980101011 =	SIP #1 RTP Port Range End <1024~65535>		= 65535
980101012 =	SIP #1 UserId		= changeme
980101013 =	SIP #1 Password		= changeme
980101014 =	SIP #1 Phone Number		= changeme
980101015 =	SIP #1 Minimun Session Expire Time	<20~1800>	= 30
980101017 =	SIP #1 Domain Name		= sipserver.net
980101018 =	SIP #1 Mapping to POTS Phone1	<0(No) | 1(Yes)>	= 1
980101019 =	SIP #1 Mapping to POTS Phone2	<0(No) | 1(Yes)>	= 1
980101020 =	SIP #1 CODEC Type 1	<0(G711mu) |8(G711A) |18(G729)>	= 18
980101021 =	SIP #1 CODEC Type 2	<0(G711mu) |8(G711A) |18(G729)>	= 0

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

980101022 =	SIP #1 DTMF Key Type	<0(RFC_2833) |1(PCM) |2(SIP_INFO) |3(RFC_2833_LIKE_SIP_INFO)>	= 0
980101023 =	SIP #1 Transport Type	<0(UDP) |1(TCP)>	= 0
980101024 =	SIP #1 Hide Caller ID	<0(No) |1(Yes)>	= 0
980101025 =	SIP #1 Auto Redial	<0(No) |1(Yes)>	= 0
980101026 =	SIP #1 STUN Server Active	<0(No) | 1(Yes)>	= 0
980101027 =	SIP #1 STUN Server Address		=
980101028 =	SIP #1 STUN Server Port	<1024~65535>	= 0
980101029 =	SIP #1 Call Forward Index	<1~2>	= 1
980101030 =	SIP #1 Outbound Proxy Active	<0(No) | 1(Yes)>	= 0
980101031 =	SIP #1 Outbound Proxy Address		=
980101032 =	SIP #1 Outbound Proxy Port	<1024~65535>	= 0
980101033 =	SIP #1 Outbound Proxy KA Active	<0(No) | 1(Yes)>	= 0
980101034 =	SIP #1 Outbound Proxy KA Interval		= 0
980101035 =	SIP #1 Session Timer Active	<0(No) | 1(Yes)>	= 0
/ Menu 98.1.2 VoIP SIP #2 Setup			
FIN	FN	PVA	INPUT
980102001 =	SIP #2 Active	<0(No) | 1(Yes)>	= 1
980102002 =	SIP #2 Server Address		= sipserver.net
980102003 =	SIP #2 Server Port	<1024~65535>	= 5060
980102004 =	SIP #2 Registartion Server IP		= sipserver.net
980102005 =	SIP #2 Registartion Server Port	<1024~65535>	= 5060
980102006 =	SIP #2 Registartion Expiration Time	<2~65535>	= 3600
980102007 =	SIP #2 Register ReSend Time	<1~65535>	= 180
980102008 =	SIP #2 Session Expire Time	<30~3600>	= 180
980102009 =	SIP #2 Local signaling Port	<1024~65535>	= 5060
980102010 =	SIP #2 RTP Port Range Start	<1024~65535>	= 50000
980102011 =	SIP #2 RTP Port Range End <1024~65535>		= 65535
980102012 =	SIP #2 UserId		= changeme
980102013 =	SIP #2 Password		= changeme
980102014 =	SIP #2 Phone Number		= changeme
980102015 =	SIP #2 Minimun Session Expire Time	<20~1800>	= 30

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

980102017 =	SIP #2 Domain Name		= sipserver.net
980102018 =	SIP #2 Mapping to POTS Phone1	<0(No) | 1(Yes)>	= 1
980102019 =	SIP #2 Mapping to POTS Phone2	<0(No) | 1(Yes)>	= 1
980102020 =	SIP #2 CODEC Type 1	<0(G711mu) |8(G711A) |18(G729)>	= 18
980102021 =	SIP #2 CODEC Type 2	<0(G711mu) |8(G711A) |18(G729)>	= 0
980102022 =	SIP #2 DTMF Key Type	<0(RFC_2833) |1(PCM) |2(SIP_INFO) |3(RFC_2833_LIKE_SIP_INFO)>	= 0
980102023 =	SIP #2 Transport Type	<0(UDP) |1(TCP)>	= 0
980102024 =	SIP #2 Hide Caller ID	<0(No) |1(Yes)>	= 0
980102025 =	SIP #2 Auto Redial	<0(No) |1(Yes)>	= 0
980102026 =	SIP #2 STUN Server Active	<0(No) | 1(Yes)>	= 0
980102027 =	SIP #2 STUN Server Address		=
980102028 =	SIP #2 STUN Server Port	<1024~65535>	= 0
980102029 =	SIP #2 Call Forward Index	<1~2>	= 1
980102030 =	SIP #2 Outbound Proxy Active	<0(No) | 1(Yes)>	= 0
980102031 =	SIP #2 Outbound Proxy Address		=
980102032 =	SIP #2 Outbound Proxy Port	<1024~65535>	= 0
980102033 =	SIP #2 Outbound Proxy KA Active	<0(No) | 1(Yes)>	= 0
980102034 =	SIP #2 Outbound Proxy KA Interval		= 0
980102035 =	SIP #2 Session Timer Active	<0(No) | 1(Yes)>	= 0
/ Menu 98.2 VoIP QoS Setup			
FIN	FN	PVA	INPUT
980200001 =	SIP TOS Priority Setting	<0~7>	= 5
980200002 =	RTP TOS Priority Setting	<0~7>	= 5
980200003 =	VLAN Taging	<0(No) |1(Active)>	= 0
980200004 =	Voice VLAN ID	<0~4095>	= 0
/ Menu 98.3.1 Phone #1 Setup			
FIN	FN	PVA	INPUT
980301001 =	Phone #1 Speaking Volume	<-14~14>	= 0
980301002 =	Phone #1 Listening Volume	<-14~14>	= 0
980301003 =	Phone #1 Outgoing Call use SIP #1	<0(No) |1(Yes)>	= 1
980301004 =	Phone #1 Outgoing Call use SIP #2	<0(No) |1(Yes)>	= 1
980301005 =	Phone #1 G.168 Echo Cancellation	<0(No) |1(Yes)>	= 1

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

980301006 =	Phone #1 Voice Active Detection Support	<0(No) |1(Yes)>	= 0
980301007 =	Phone #1 Dialing Short Interval		= 3
980301008 =	Phone #1 Dialing Long Interval		= 8
980301009 =	Phone #1 Flash Max Interval		= 1000
980301010 =	Phone #1 Flash Min Interval		= 100
/ Menu 98.3.2 Phone #2 Setup			
FIN	FN	PVA	INPUT
980302001 =	Phone #2 Speaking Volume	<-14~14>	= 0
980302002 =	Phone #2 Listening Volume	<-14~14>	= 0
980302003 =	Phone #2 Outgoing Call use SIP #1	<0(No) |1(Yes)>	= 1
980302004 =	Phone #2 Outgoing Call use SIP #2	<0(No) |1(Yes)>	= 1
980302005 =	Phone #2 G.168 Echo Cancellation	<0(No) |1(Yes)>	= 1
980302006 =	Phone #2 Voice Active Detection Support	<0(No) |1(Yes)>	= 0
980302007 =	Phone #2 Dialing Short Interval		= 3
980302008 =	Phone #2 Dialing Long Interval		= 8
980302009 =	Phone #2 Flash Max Interval		= 1000
980302010 =	Phone #2 Flash Min Interval		= 100
/ Menu 98.5 VoIP RTP Setup			
FIN	FN	PVA	INPUT
980500001 =	Sort Buffer Size ms	<0(0ms)| 1(10ms) |2(20ms)>	= 1
980500002 =	RTCP Interval ms		= 40
980500004 =	G711 voice Packet Length ms	<0(10ms)| 1(20ms) |2(30ms)>	= 1
980500005 =	G729 voice Packet Length ms	<0(10ms)| 1(20ms) |2(30ms) .. |7(80ms)>	= 1
/ Menu 98.6 Auto Provision Setup			
FIN	FN	PVA	INPUT
980600001 =	Auto Provision Active	<0(No) |1(Yes)>	= 0
980600002 =	Auto Provision Server Address		= autoproserver.net
980600003 =	Auto Provision Expire Time (Second)	<1~2600000>	= 180
980600004 =	Auto Provision Retry Expire Time (Second)	<180~65535>	= 180
980600005 =	Auto Provision Protocol	<0(TFTP)| 1(HTTP) |2(HTTPS)>	= 0
980600006 =	Auto Provision Method	<0(Common)| 1(Bluewin)>	= 0

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

/ Menu 98.7.1 Phone Book (Speed Dial) #1 Setup			
FIN	FN	PVA	INPUT
980701001 =	Phone Book #1 Active	<0(No) |1(Yes)>	= 0
980701002 =	Phone Book #1 SIP Number		=
980701003 =	Phone Book #1 SIP IP/URL		=
980701004 =	Phone Book #1 Name		=
980701005 =	Phone Book #1 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980701006 =	Phone Book #1 Speed Number		=
/ Menu 98.7.2 Phone Book (Speed Dial) #2 Setup			
FIN	FN	PVA	INPUT
980702001 =	Phone Book #2 Active	<0(No) |1(Yes)>	= 0
980702002 =	Phone Book #2 SIP Number		=
980702003 =	Phone Book #2 SIP IP/URL		=
980702004 =	Phone Book #2 Name		=
980702005 =	Phone Book #2 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980702006 =	Phone Book #2 Speed Number		=
/ Menu 98.7.3 Phone Book (Speed Dial) #3 Setup			
FIN	FN	PVA	INPUT
980703001 =	Phone Book #3 Active	<0(No) |1(Yes)>	= 0
980703002 =	Phone Book #3 SIP Number		=
980703003 =	Phone Book #3 SIP IP/URL		=
980703004 =	Phone Book #3 Name		=
980703005 =	Phone Book #3 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980703006 =	Phone Book #3 Speed Number		=
/ Menu 98.7.4 Phone Book (Speed Dial) #4 Setup			
FIN	FN	PVA	INPUT
980704001 =	Phone Book #4 Active	<0(No) |1(Yes)>	= 0
980704002 =	Phone Book #4 SIP Number		=
980704003 =	Phone Book #4 SIP IP/URL		=
980704004 =	Phone Book #4 Name		=
980704005 =	Phone Book #4 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980704006 =	Phone Book #4 Speed Number		=
/ Menu 98.7.5 Phone Book (Speed Dial) #5 Setup			
FIN	FN	PVA	INPUT
980705001 =	Phone Book #5 Active	<0(No) |1(Yes)>	= 0
980705002 =	Phone Book #5 SIP Number		=

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

980705003 =	Phone Book #5 SIP IP/URL		=
980705004 =	Phone Book #5 Name		=
980705005 =	Phone Book #5 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980705006 =	Phone Book #5 Speed Number		=
/ Menu 98.7.6 Phone Book (Speed Dial) #6 Setup			
FIN	FN	PVA	INPUT
980706001 =	Phone Book #6 Active	<0(No) |1(Yes)>	= 0
980706002 =	Phone Book #6 SIP Number		=
980706003 =	Phone Book #6 SIP IP/URL		=
980706004 =	Phone Book #6 Name		=
980706005 =	Phone Book #6 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980706006 =	Phone Book #6 Speed Number		=
/ Menu 98.7.7 Phone Book (Speed Dial) #7 Setup			
FIN	FN	PVA	INPUT
980707001 =	Phone Book #7 Active	<0(No) |1(Yes)>	= 0
980707002 =	Phone Book #7 SIP Number		=
980707003 =	Phone Book #7 SIP IP/URL		=
980707004 =	Phone Book #7 Name		=
980707005 =	Phone Book #7 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980707006 =	Phone Book #7 Speed Number		=
/ Menu 98.7.8 Phone Book (Speed Dial) #8 Setup			
FIN	FN	PVA	INPUT
980708001 =	Phone Book #8 Active	<0(No) |1(Yes)>	= 0
980708002 =	Phone Book #8 SIP Number		=
980708003 =	Phone Book #8 SIP IP/URL		=
980708004 =	Phone Book #8 Name		=
980708005 =	Phone Book #8 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980708006 =	Phone Book #8 Speed Number		=
/ Menu 98.7.9 Phone Book (Speed Dial) #9 Setup			
FIN	FN	PVA	INPUT
980709001 =	Phone Book #9 Active	<0(No) |1(Yes)>	= 0
980709002 =	Phone Book #9 SIP Number		=
980709003 =	Phone Book #9 SIP IP/URL		=
980709004 =	Phone Book #9 Name		=
980709005 =	Phone Book #9 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980709006 =	Phone Book #9 Speed Number		=

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

/ Menu 98.7.10 Phone Book (Speed Dial) #10 Setup			
FIN	FN	PVA	INPUT
980710001 =	Phone Book #10 Active	<0(No) |1(Yes)>	= 0
980710002 =	Phone Book #10 SIP Number		=
980710003 =	Phone Book #10 SIP IP/URL		=
980710004 =	Phone Book #10 Name		=
980710005 =	Phone Book #10 Type	<0(Proxy) |1(Non-Proxy)>	= 0
980710006 =	Phone Book #10 Speed Number		=
/ Menu 98.8 VoIP Common Setup			
FIN	FN	PVA	INPUT
980800001 =	VoIP Country Code		= 0
980800002 =	VoIP Immediate Dial Active	<0(No) |1(Yes)>	= 0
980800003 =	PSTN FallBack	<0(No) |1(Force SIP if PSTN unplugged)>	= 0
980800004 =	VoIP RTP send after receive ACK	<0(No) |1(Yes)>	= 0
980800005 =	VoIP Follow RFC3265	<0(No) |1(Yes)>	= 0
980800006 =	SIP FallBack	<0(No) |1(Force FXO LifeLine if SIP failed)>	= 0
/ Menu 98.9 Auto Upgrade Common Setup			
FIN	FN	PVA	INPUT
980900001 =	Target_Firmware_Version		= 360md3b5
980900002 =	Firmware_Download_Addr		= ftp://firmwareserver.net/
980900003 =	Fw_Notify_Voice_Type		= de
980900004 =	Target_Firmware_Username		=
980900005 =	Target_Firmware_Password		=
/ Menu 98.11.1 Call Forwarding #1 Setup			
FIN	FN	PVA	INPUT
981101001 =	Call Forward #1 for unconditional		=
981101002 =	Call Forward #1 for busy		=
981101003 =	Call Forward #1 for no answer		=
981101004 =	Call Forward #1 for no answer time	<5~179>	= 0
981101005 =	Call Forward #1 Table[1] caller		=
981101006 =	Call Forward #1 Table[1] dest		=
981101007 =	Call Forward #1 Table[1] flag		= 0
981101008 =	Call Forward #1 Table[2] caller		=
981101009 =	Call Forward #1 Table[2] dest		=
981101010 =	Call Forward #1 Table[2] flag		= 0

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

981101011 =	Call Forward #1 Table[3] caller		=
981101012 =	Call Forward #1 Table[3] dest		=
981101013 =	Call Forward #1 Table[3] flag		= 0
981101014 =	Call Forward #1 Table[4] caller		=
981101015 =	Call Forward #1 Table[4] dest		=
981101016 =	Call Forward #1 Table[4] flag		= 0
981101017 =	Call Forward #1 Table[5] caller		=
981101018 =	Call Forward #1 Table[5] dest		=
981101019 =	Call Forward #1 Table[5] flag		= 0
981101020 =	Call Forward #1 Table[6] caller		=
981101021 =	Call Forward #1 Table[6] dest		=
981101022 =	Call Forward #1 Table[6] flag		= 0
981101023 =	Call Forward #1 Table[7] caller		=
981101024 =	Call Forward #1 Table[7] dest		=
981101025 =	Call Forward #1 Table[7] flag		= 0
981101026 =	Call Forward #1 Table[8] caller		=
981101027 =	Call Forward #1 Table[8] dest		=
981101028 =	Call Forward #1 Table[8] flag		= 0
981101029 =	Call Forward #1 Table[9] caller		=
981101030 =	Call Forward #1 Table[9] dest		=
981101031 =	Call Forward #1 Table[9] flag		= 0
981101032 =	Call Forward #1 Table[10] caller		=
981101033 =	Call Forward #1 Table[10] dest		=
981101034 =	Call Forward #1 Table[10] flag		= 0
/ Menu 98.11.2 Call Forwarding #2 Setup			
FIN	FN	PVA	INPUT
981102001 =	Call Forward #2 for unconditional		=
981102002 =	Call Forward #2 for busy		=
981102003 =	Call Forward #2 for no answer		=
981102004 =	Call Forward #2 for no answer time	<5~179>	= 0
981102005 =	Call Forward #2 Table[1] caller		=
981102006 =	Call Forward #2 Table[1] dest		=
981102007 =	Call Forward #2 Table[1] flag		= 0
981102008 =	Call Forward #2 Table[2] caller		=
981102009 =	Call Forward #2 Table[2] dest		=
981102010 =	Call Forward #2 Table[2] flag		= 0
981102011 =	Call Forward #2 Table[3] caller		=
981102012 =	Call Forward #2 Table[3] dest		=
981102013 =	Call Forward #2 Table[3] flag		= 0

Table 68 Menu 98 VoIP and Auto Upgrade Menus (continued)

981102014 =	Call Forward #2 Table[4] caller		=
981102015 =	Call Forward #2 Table[4] dest		=
981102016 =	Call Forward #2 Table[4] flag		= 0
981102017 =	Call Forward #2 Table[5] caller		=
981102018 =	Call Forward #2 Table[5] dest		=
981102019 =	Call Forward #2 Table[5] flag		= 0
981102020 =	Call Forward #2 Table[6] caller		=
981102021 =	Call Forward #2 Table[6] dest		=
981102022 =	Call Forward #2 Table[6] flag		= 0
981102023 =	Call Forward #2 Table[7] caller		=
981102024 =	Call Forward #2 Table[7] dest		=
981102025 =	Call Forward #2 Table[7] flag		= 0
981102026 =	Call Forward #2 Table[8] caller		=
981102027 =	Call Forward #2 Table[8] dest		=
981102028 =	Call Forward #2 Table[8] flag		= 0
981102029 =	Call Forward #2 Table[9] caller		=
981102030 =	Call Forward #2 Table[9] dest		=
981102031 =	Call Forward #2 Table[9] flag		= 0
981102032 =	Call Forward #2 Table[10] caller		=
981102033 =	Call Forward #2 Table[10] dest		=
981102034 =	Call Forward #2 Table[10] flag		= 0

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z