

P-3202HN-Ba

802.11N GPON VoIP IAD

User's Guide

DRAFT

Default Login Details

IP Address	192.168.1.1
User Name	admin
Password	1234

Version 1.0
Edition 1, 12/2009

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the IAD using the web configurator. .

Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get your IAD up and running right away. It contains information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

The embedded Web Help contains descriptions of individual screens and supplementary information.

- Support Disc

Refer to the included CD for support documents.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- 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.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.






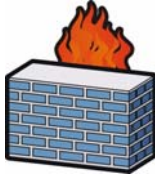



Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- This product may be referred to as the "IAD", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The IAD icon is not an exact representation of your device.

IAD 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- 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 should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

User's Guide	19
Introduction	21
The Web Configurator	29
Tutorials	35
Technical Reference	39
Status Screens	41
Device Mode Screen	51
WAN	55
LAN Setup	59
Wireless LAN	69
Network Address Translation (NAT)	101
Voice	117
Phone Usage	129
Firewalls	137
Static Route	159
Quality of Service (QoS)	163
Dynamic DNS Setup	179
Remote Management	183
Universal Plug-and-Play (UPnP)	197
System	211
Logs	215
Tools	219
Diagnostic	223
Troubleshooting	225
Product Specifications	231

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
Contents Overview	9
Table of Contents.....	11
Part I: User's Guide.....	19
Chapter 1	
Introduction	21
1.1 Overview	21
1.2 Managing the IAD	21
1.3 Good Habits for Managing the IAD	21
1.4 Applications for the IAD	22
1.4.1 Internet Access and Device Mode	22
1.4.2 Internet Calls (VoIP)	23
1.4.3 Wireless Connection	23
1.4.4 Triple Play	24
1.5 The Reset Button	25
1.5.1 Using the Reset Button	25
1.6 LEDs (Lights)	26
Chapter 2	
The Web Configurator	29
2.1 Overview	29
2.1.1 Accessing the Web Configurator	29
2.2 Web Configurator Main Screen	31
2.2.1 Title Bar	31
2.2.2 Navigation Panel	32
2.2.3 Main Window	34
2.2.4 Status Bar	34
Chapter 3	
Tutorials.....	35

3.1 Overview	35
3.2 Getting Starting with the IAD	35
3.3 Placing Phone Calls Over the Internet	36
Part II: Technical Reference	39
Chapter 4	
Status Screens	41
4.1 Overview	41
4.2 Status Screen	42
4.2.1 VoIP Status	47
4.2.2 WLAN Status	49
Chapter 5	
Device Mode Screen	51
5.1 Overview	51
5.1.1 Hybrid Mode (Router Mode)	51
5.1.2 Bridge Mode	51
5.2 Device Mode Screen	52
Chapter 6	
WAN	55
6.1 Overview	55
6.1.1 What You Need to Know	55
6.2 Internet Access Setup	56
Chapter 7	
LAN Setup	59
7.1 LAN Overview	59
7.1.1 LANs, WANs and the ZyXEL Device	59
7.1.2 DHCP Setup	59
7.2 DNS Server Addresses	60
7.3 LAN TCP/IP	60
7.3.1 IP Address and Subnet Mask	61
7.3.2 RIP Setup	62
7.3.3 Multicast	62
7.4 Configuring LAN IP and DHCP	63
7.5 LAN Client List	65
7.6 LAN IP Alias	66
Chapter 8	
Wireless LAN	69

8.1 Overview	69
8.1.1 What You Can Do in this Chapter	69
8.2 What You Need to Know	70
8.3 Before You Begin	72
8.4 The General Screen	73
8.4.1 No Security	75
8.4.2 WEP Encryption	76
8.4.3 WPA(2)-PSK	77
8.4.4 WPA(2) Authentication	78
8.4.5 MAC Filter	80
8.4.6 Adding a New MAC Filtering Rule	81
8.5 The More AP Screen	82
8.5.1 More AP Edit	83
8.6 The WPS Screen	83
8.7 The WPS Station Screen	85
8.8 The WDS Screen	86
8.9 The Advanced Setup Screen	88
8.10 Technical Reference	89
8.10.1 Wireless Network Overview	90
8.10.2 Additional Wireless Terms	91
8.10.3 Wireless Security Overview	91
8.10.4 WiFi Protected Setup	93
Chapter 9	
Network Address Translation (NAT).....	101
9.1 Overview	101
9.1.1 What You Can Do in this Chapter	101
9.1.2 What You Need To Know	101
9.2 The NAT General Screen	102
9.3 The Port Forwarding Screen	104
9.3.1 Configuring the Port Forwarding Screen	105
9.3.2 The Port Forwarding Rule Edit Screen	107
9.4 The Address Mapping Screen	108
9.4.1 The Address Mapping Rule Edit Screen	110
9.5 The ALG Screen	111
9.6 NAT Technical Reference	112
9.6.1 NAT Definitions	112
9.6.2 What NAT Does	112
9.6.3 How NAT Works	113
9.6.4 NAT Application	114
9.6.5 NAT Mapping Types	114
9.6.6 Port Translation	115

Chapter 10	
Voice	117
10.1 Introduction	117
10.1.1 What You Need to Know	117
10.2 SIP Service Provider	118
10.2.1 Advanced SIP Settings	120
10.3 SIP Account	122
10.3.1 Advanced Account Settings	123
10.4 Analog Phone	125
10.5 Speed Dial	126
Chapter 11	
Phone Usage	129
11.1 Overview	129
11.2 Dialing a Telephone Number	129
11.3 Using Speed Dial	129
11.4 Using Call Park and Pickup	129
11.5 Checking the IAD's IP Address	130
11.6 Auto Provisioning and Auto Firmware Upgrade	130
11.7 Phone Services Overview	131
11.7.1 The Flash Key	131
11.7.2 Europe Type Supplementary Phone Services	131
11.7.3 USA Type Supplementary Services	133
11.8 Phone Functions Summary	135
Chapter 12	
Firewalls	137
12.1 Overview	137
12.1.1 What You Can Do in this Chapter	138
12.1.2 What You Need to Know	138
12.1.3 Firewall Rule Setup Example	140
12.2 The Firewall General Screen	143
12.3 The Firewall Rules Screen	145
12.3.1 Configuring Firewall Rules	146
12.3.2 Customized Services	149
12.3.3 Configuring A Customized Service	150
12.4 The Firewall Threshold Screen	151
12.4.1 Threshold Values	151
12.4.2 Configuring Firewall Thresholds	152
12.5 Technical Reference	154
12.5.1 Guidelines For Enhancing Security With Your Firewall	154
12.5.2 Security Considerations	154
12.5.3 Triangle Route	155

Chapter 13	
Static Route	159
13.1 Overview	159
13.1.1 What You Can Do in this Chapter	159
13.2 The Static Route Screen	160
13.2.1 Static Route Edit	161
Chapter 14	
Quality of Service (QoS)	163
14.1 Overview	163
14.1.1 What You Can Do in this Chapter	163
14.1.2 What You Need to Know	164
14.2 The QoS General Screen	164
14.3 The Class Setup Screen	166
14.3.1 Class Configuration	168
14.3.2 QoS Example	171
14.4 The QoS Monitor Screen	175
14.5 Technical Reference	175
14.5.1 IEEE 802.1Q Tag	176
14.5.2 IP Precedence	176
14.5.3 DiffServ	176
14.5.4 Automatic Priority Queue Assignment	177
Chapter 15	
Dynamic DNS Setup	179
15.1 Overview	179
15.1.1 What You Can Do in this Chapter	179
15.1.2 What You Need To Know	179
15.2 The Dynamic DNS Screen	180
Chapter 16	
Remote Management	183
16.1 Overview	183
16.1.1 What You Can Do in this Chapter	184
16.1.2 What You Need to Know	184
16.2 The HTTP Screen	185
16.3 The Telnet Screen	186
16.4 The FTP Screen	187
16.5 SNMP	188
16.5.1 Supported MIBs	190
16.5.2 SNMP Traps	190
16.5.3 The SNMP Screen	190
16.6 The DNS Screen	191

16.7 The ICMP Screen	192
16.8 SSH	193
16.9 How SSH Works	194
16.10 SSH Implementation on the IAD	195
16.10.1 Requirements for Using SSH	195
16.11 The SSH Screen	195
Chapter 17	
Universal Plug-and-Play (UPnP).....	197
17.1 Overview	197
17.1.1 What You Can Do in this Chapter	197
17.1.2 What You Need to Know	197
17.2 The UPnP Screen	198
17.3 Installing UPnP in Windows Example	199
17.4 Using UPnP in Windows XP Example	203
Chapter 18	
System	211
18.1 Overview	211
18.1.1 What You Need to Know	211
18.2 General Setup	212
18.3 Time Setting	213
Chapter 19	
Logs	215
19.1 Overview	215
19.2 View Log	215
19.3 Log Settings	217
Chapter 20	
Tools.....	219
20.1 Overview	219
20.1.1 Some Warnings	219
20.2 Firmware Upgrade	220
20.3 Configuration	221
20.3.1 Backup Configuration	221
20.3.2 Restore Configuration	221
20.3.3 Reset to Factory Defaults	222
20.4 Restart	222
Chapter 21	
Diagnostic	223
21.1 Overview	223

21.2 General	223
Chapter 22	
Troubleshooting.....	225
22.1 Overview	225
22.2 Power, Hardware Connections, and LEDs	225
22.3 IAD Access and Login	226
22.4 Internet Access	227
22.5 Phone Calls and VoIP	228
Chapter 23	
Product Specifications	231
Appendix A Passive Optical Networks	239
Appendix B Setting Up Your Computer's IP Address	245
Appendix C Pop-up Windows, JavaScripts and Java Permissions	275
Appendix D IP Addresses and Subnetting	285
Appendix E Wireless LANs	297
Appendix F Common Services.....	313
Appendix G Legal Information.....	317
Index.....	321

PART I

User's Guide

Introduction

1.1 Overview

This device is an Integrated Access Device (IAD) which combines high-speed fiber optic (G-PON) Internet access, a built-in switch, wireless networking capability and Voice over IP (VoIP) technology to allow you to use an analog telephone to make phone calls over the Internet. The device also comes with one coaxial CATV connector to connect to a television or set-top-box.

Please refer to the following description of the product name format.

- "H" denotes an integrated 4-port hub (switch).
- "N" denotes IEEE 802.11n wireless functionality. There is an embedded mini-PCI module for IEEE 802.11b/g/n wireless LAN connectivity.

Only use firmware for your IAD's specific model. Refer to the label on the bottom of your IAD.

1.2 Managing the IAD

Use the IAD's built-in Web Configurator to manage it. You can connect to it using a web browser such as Firefox 2.0 (and higher) or Internet Explorer 6 (and higher). The web configurator gives you access to all the available settings for this product. For details on connecting to it, see the Quick Start Guide.

1.3 Good Habits for Managing the IAD

Do the following things regularly to make the IAD more secure and to manage the IAD more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the IAD to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the IAD. You could simply restore your last configuration.

1.4 Applications for the IAD

Here are some example uses for which the IAD is well suited.

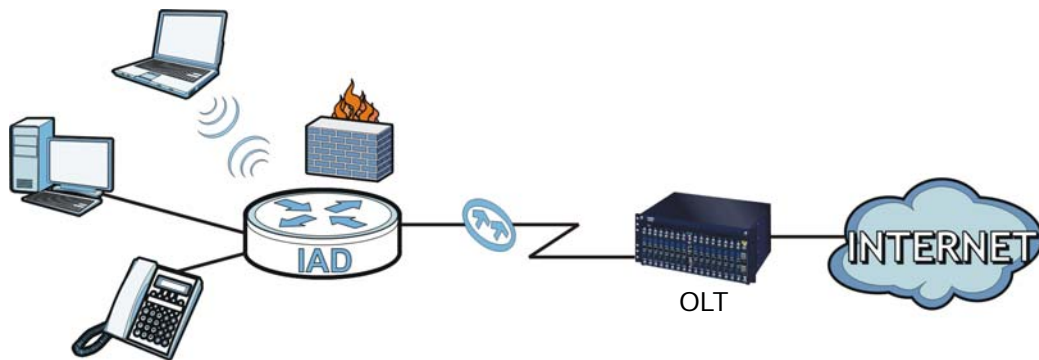
1.4.1 Internet Access and Device Mode

Your IAD provides shared Internet access by connecting a fiber optic line provided by your ISP to the PON port.

In hybrid mode, the IAD works as a router. You can enable NAT, firewall and use Quality of Service (QoS) to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers.

If you have a router deployed in your network already, set the IAD to act as a bridge. The routing features, such as NAT and static route are not available on the IAD in bridge mode and QoS configuration is done remotely by the ISP's OLT (Optical Line Terminal). This allows you put the IAD into an existing network that has a router with minimum configuration.

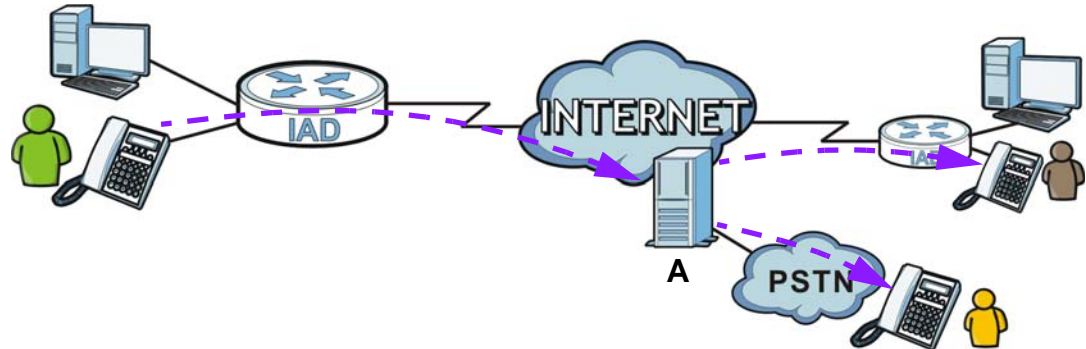
Figure 1 Internet Access Application (Router Mode)



1.4.2 Internet Calls (VoIP)

You can register up to 2 SIP (Session Initiation Protocol) accounts and use the IAD to make and receive VoIP telephone calls:

Figure 2 VoIP Application

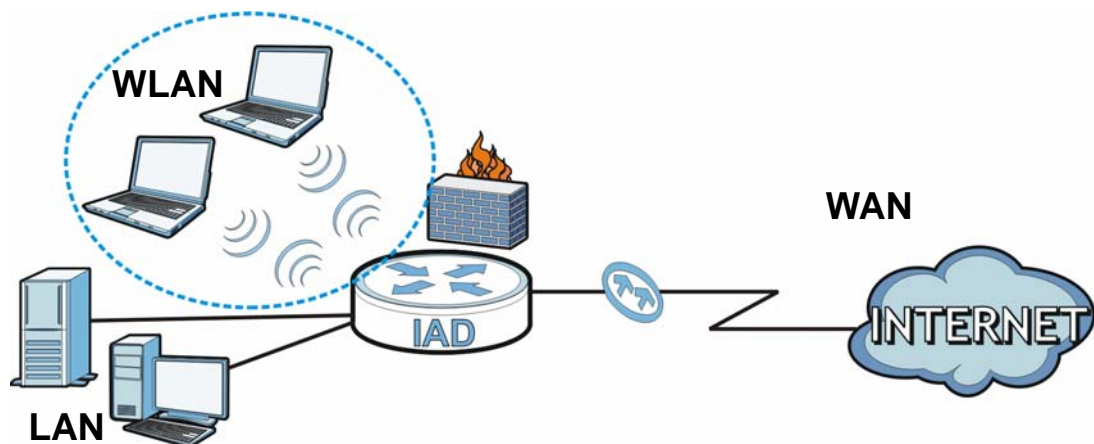


- ~~Peer-to-Peer calls (A) - Use the IAD to make a call to the recipient's IP address without using a SIP proxy server.~~
- Calls via a VoIP service provider (A) - The IAD sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

1.4.3 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the IAD. IEEE 802.11b/g compliant clients can wirelessly connect to the IAD to access network resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 3 Wireless Connection Application



1.4.3.1 The **WPS/WLAN** Button

You can use the **WPS/WLAN** button on the top of the device to turn the wireless LAN off or on. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

Turn the Wireless LAN Off or On

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **WPS/WLAN** button for one second and release it. The **WLAN/WPS** LED should change from on to off or vice versa.

Activate WPS

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **WPS/WLAN** button for more than five seconds and release it. Press the WPS button on another WPS -enabled device within range of the IAD. The **WLAN/WPS** LED should flash while the IAD sets up a WPS connection with the wireless device.

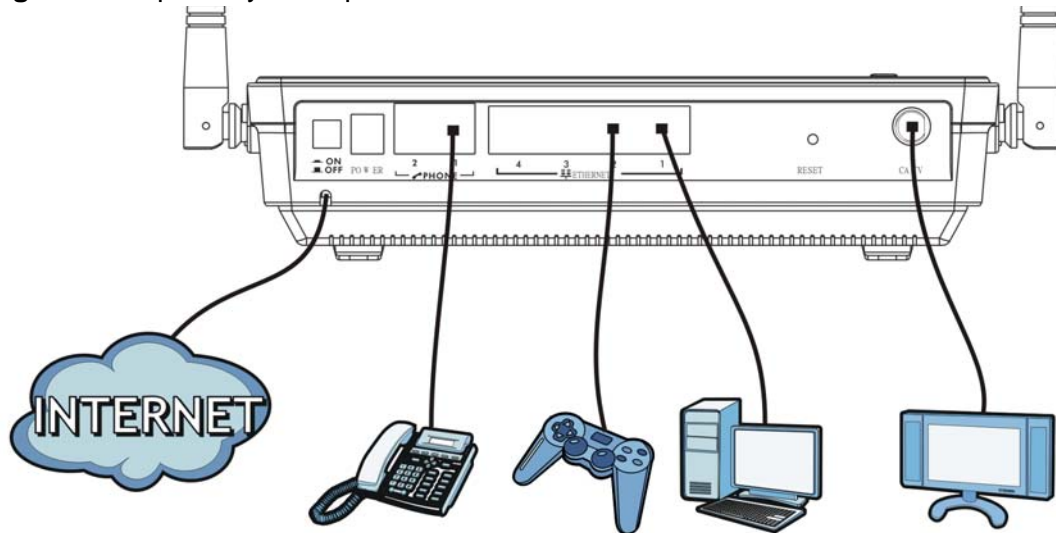
Note: You must activate WPS in the IAD and in another wireless device within two minutes of each other. See [Section 7.10.4 on page 151](#) for more information.

1.4.4 Triple Play

Your ISP may provide “triple play” service to your IAD. This allows you to take advantage of such features as broadband Internet access, Voice over IP telephony,

and streaming video/audio media, all at the same time with no noticeable loss in bandwidth.

Figure 4 Triple Play Example



1.5 The Reset Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

1.5.1 Using the Reset Button

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 5 LEDs on the Top Panel



None of the LEDs are on if the IAD is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The IAD is receiving power and ready for use.
		Blinking	The IAD is self-testing.
	Red	On	The IAD detected an error while self-testing, or there is a device malfunction.
		Off	The IAD is not receiving power.
PON	Green	On	The IAD has established a PON line connection with the ISP.
		Off	The IAD has not established a PON connection with the ISP or the fiber optic line is down.
		Blinking	The IAD is in the process of downloading firmware.
	Red	On	The IAD PON link has failed or has generated errors.
ETHERNET 1~4	Green	On	The IAD has an Ethernet connection with another device (such as a computer) on the Local Area Network (LAN) through this port.
		Blinking	The IAD is sending/receiving data to /from the LAN through this port.
		Off	The IAD does not have an Ethernet connection with the LAN through this port.
WPS/WLAN	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g/n mode.
		Blinking	The IAD is communicating with other wireless clients.
	Orange	Blinking	The IAD is setting up a WPS connection.
		Off	The wireless network is not activated.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The IAD has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The IAD is sending or receiving IP traffic.
	Red	On	The IAD attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The IAD does not have an IP connection, or the IAD is in bridge mode.
PHONE 1/2	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
		Off	The phone port does not have a SIP account registered.
CATV	Green	On	The IAD is receiving video signals.
		Off	The IAD is not receiving video signals.

Refer to the Quick Start Guide for information on hardware connections.

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Firefox 2.0 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.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See [Appendix C on page 275](#) if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

- 1 Make sure your IAD hardware is properly connected (refer to the Quick Start Guide for details on this).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.

- 4 A password screen displays. Enter your **user name and password**. The default user name is **admin** and the default password is **1234**. Click **Login**.

Figure 6 Password Screen



- 5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password of **up to 30 characters**, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 7 Change Password Screen

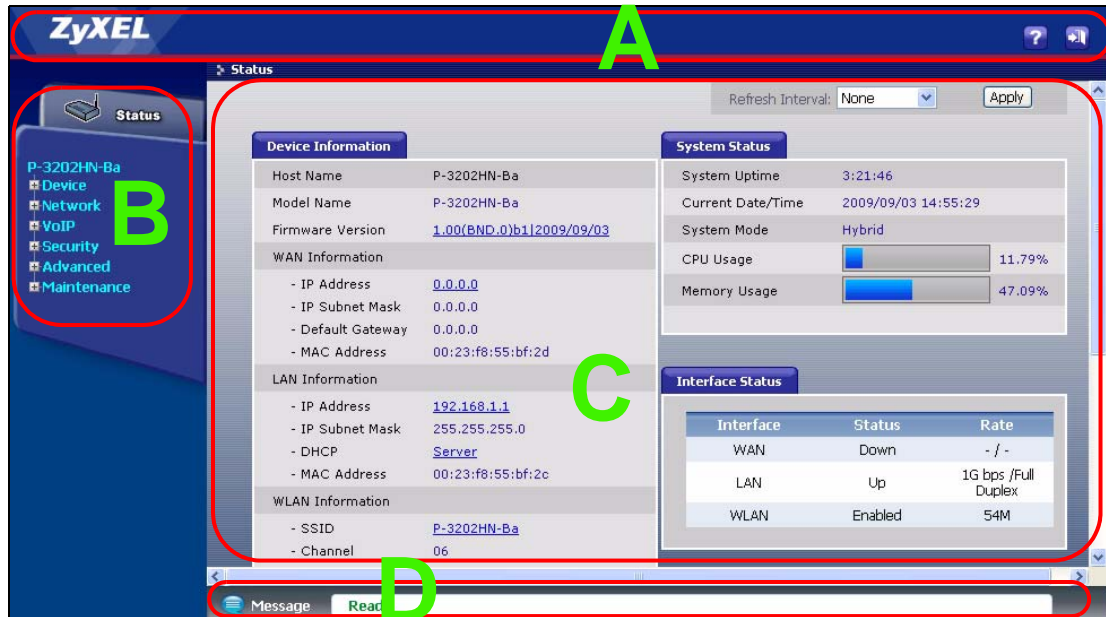


Note: For security reasons, the IAD automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

2.2 Web Configurator Main Screen

The main screen is divided into these parts:

Figure 8 Main Screen



- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar



2.2.1 Title Bar

The title bar allows you to change the language and provides some icons in the upper right corner.



The icons provide the following functions:

Table 2 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Help: Click this icon to open the online help.
	Logout: Click this icon to log out of the web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure IAD features. The following tables describe each menu item.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the IAD's general device and network status information. Use this screen to access the statistics and client list.
Device		
Device Mode		Use this screen to select whether the IAD acts as a router (Hybrid Mode) or a bridge (Bridge Mode).
Network		
WAN	Internet Access Setup	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
Wireless LAN	General	Use this screen to configure the wireless LAN settings, WLAN authentication/security settings.
	WPS	Use this screen to enable WPS (Wi-Fi Protected Setup) and view the WPS status.
	WPS Station	Use this screen to use WPS to set up your wireless network.
	MAC Filter	Use this screen to configure MAC filtering rules.
	QoS	Use this screen to enable WMM QoS (Wi-Fi MultiMedia Quality of Service). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
NAT	General	Use this screen to enable NAT on the IAD.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	ALG	Use this screen to allow certain applications to pass through the IAD.
VoIP		
SIP	SIP Service Provider	Use this screen to configure the SIP settings used by the IAD when you place calls over the Internet.
	SIP Account	Use this screen to configure your SIP account information.
Phone	Analog Phone	Use this screen to set which phone ports use which SIP accounts.
Phone Book	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Advanced		

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Static Route	Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Bandwidth MGMT	General	Use this screen to enable QoS and configure bandwidth management on the WAN.
	Rule Setup	Use this screen to define a classifier.
	QoS Monitor	Use this screen to view QoS packets statistics.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the IAD.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the IAD.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the IAD.
	SSH	Use this screen to configure Secure SHell (SSH) connections to and from the IAD.
	ICMP	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
	TR-069	Use this screen to enable remote management via TR-069 on the WAN.
Maintenance		
System	General	Use this screen to configure your device's name, management inactivity timeout and password.
	Time Setting	Use this screen to change your IAD's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the IAD without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.

2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See [Chapter 4 on page 41](#) for more information about the **Status** screen.

2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

3.1 Overview

This chapter introduces you to some basic networking and Voice over IP (VoIP) concepts as well as how to configure your IAD for specific functions.

3.2 Getting Starting with the IAD

This quick overview provides pointers on where in this User's Guide you can go to get started with configuring and using the IAD.

Your IAD may have come pre-configured from your ISP. If such is the case, changing any network settings may affect your ability to get online or connect to other computers on your network.

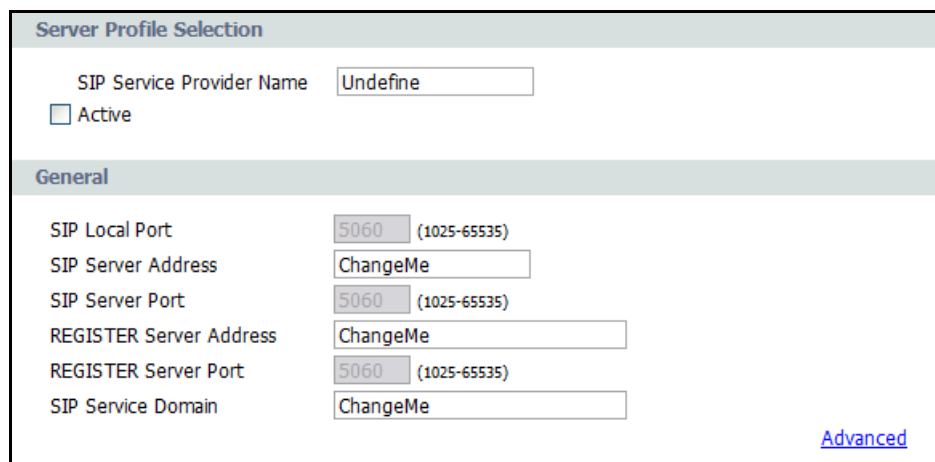
- 1 Install the device as described in the included Quick Start Guide.
- 2 Connect and login to the Web Configurator at its default IP address as described in [Section 2.2 on page 31](#). This is where you configure all available settings related to your device and its network connections. You will most likely need to connect to the IAD directly from your computer rather than over an existing network, since the device's default IP address won't match that network's existing topology.
- 3 Once you're in the Web Configurator, you can assign the IAD a new Local Area Network (LAN) IP address. This allows you to position in your LAN topology where **you** it is most beneficial to you. See [Section 7.4 on page 63](#) for details.
- 4 If you were given settings to configure the IAD's WAN connection, then you can do so in [Section 6.2 on page 56](#).
- 5 Finally, if you have a SIP account and want to place phone calls over the Internet, see [Section 3.3 on page 36](#).

3.3 Placing Phone Calls Over the Internet

The IAD allows you to plug an analog phone into it and place calls over the Internet as if you were using an IP Phone or a SIP phone. Making Internet phone calls requires that first have a SIP account set up with either your ISP (if they provide such a service) or **with** a third-party SIP provider.

To configure your SIP settings:

- 1 Connect to the Web Configurator (see the Quick Start Guide for details).
- 2 Open the **VoIP > SIP** screen, enter the following information, then click **Apply**:



The screenshot shows a web configuration page for SIP settings. It is divided into two sections: 'Server Profile Selection' and 'General'. In the 'Server Profile Selection' section, there is a text input field for 'SIP Service Provider Name' containing 'Undefine' and an unchecked checkbox for 'Active'. The 'General' section contains several configuration fields: 'SIP Local Port' (5060), 'SIP Server Address' (ChangeMe), 'SIP Server Port' (5060), 'REGISTER Server Address' (ChangeMe), 'REGISTER Server Port' (5060), and 'SIP Service Domain' (ChangeMe). Each port field has a small '(1025-65535)' range indicator. A blue 'Advanced' link is located at the bottom right of the form.

Active - Select this to enable these SIP service settings. If left unchecked, then any configuration you do here will be saved but left unused.

SIP Local Port, SIP Server Address, SIP Server Port, Register Server Address, Register Server Port, SIP Service Domain - These server settings are provided by the company that issues your VoIP account.

- 3 Click **VoIP > SIP > SIP Account** to enter your SIP account information:

SIP Account Selection

SIP Account Selection

General

Active SIP Account

Number

Authentication

User Name

Password

[Advanced](#)

SIP Account Selector - The IAD allows you to set up multiple SIP accounts. The first time you do this, you won't need to make a selection but in the future if you set up additional SIP accounts this is where you choose the one to configure.

Active SIP Account - Select this to make the current SIP account active. If you do not select this option, then you cannot use the settings configured here for the selected SIP account.

Number - Enter your SIP number. If you were given a SIP number that looked this – 1234567@sipaccount.com – then your number is the part before the “@”.

User Name -This is your SIP account user name.

Password - This is the password for your SIP account.

- 4 Next, you must configure your Phone settings to bind your newly configured SIP settings to a single phone. Click **VoIP > Phone** to display the following screen:

Phone Port Selection

Phone Port Selection

SIP Account to Make Outgoing Call

SIP Account Association	SIP Number
<input type="text" value="SIP1"/>	<input type="text" value="ChangeMe"/>

SIP Account(s) to Receive Incoming Call

SIP Account	SIP Number	SIP Account Status	SIP Account	SIP Number	SIP Account Status
<input checked="" type="checkbox"/> SIP1	<input type="text" value="ChangeMe"/>	Edit	<input type="checkbox"/> SIP2	<input type="text" value="ChangeMe"/>	Edit

- 5 Select a phone from the **Phone Port Settings** list, then select a **SIP Account** to use for all outgoing calls. The phone you choose corresponds to one of two phones physically connected to your IAD.

For **Incoming Calls**, you can assign multiple SIP accounts to a single phone. This means any call sent to the selected SIP account is forwarded to the phone chosen in **Phone Port Settings**.

Click **Apply** to save your settings.

- 6 Connect your analog phone to one of two phone ports on the IAD, as described in the Quick Start Guide. When you pick up the handset and hear a dial tone, enter the SIP phone number you want to call.

PART II

Technical Reference

Status Screens

4.1 Overview

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and unregister SIP accounts.

4.2 Status Screen

Click **Status** to open this screen. The screen varies slightly depending on the IAD's device mode. See Chapter 5 on page 51 for more information.

Figure 9 Status Screen (Bridge Mode)

The screenshot displays the Status Screen for a device in Bridge Mode. At the top right, there is a 'Refresh Interval' dropdown set to 'None' and an 'Apply' button. The screen is divided into several sections:

- Device Information:**
 - Host Name: P-3202HN-Ba
 - Model Name: P-3202HN-Ba
 - Firmware Version: [V1.00\(BND.0\)b3 3|2009/09/15](#)
 - WAN Information:**
 - IP Address: [0.0.0.0](#)
 - IP Subnet Mask: 0.0.0.0
 - Default Gateway: 0.0.0.0
 - MAC Address: 00:23:f8:55:bf:2d
 - LAN Information:**
 - IP Address: [192.168.1.1](#)
 - IP Subnet Mask: 255.255.255.0
 - MAC Address: 00:23:f8:55:bf:2c
 - WLAN Information:**
 - SSID: [P-3202HN-Ba](#)
 - Channel: 06
 - Security: WPA-PSK
- System Status:**
 - System Uptime: 0:03:44
 - Current Date/Time: 2009/09/15 12:48:27
 - System Mode: Bridge
 - CPU Usage: 26.56%
 - Memory Usage: 45.35%
- Interface Status:**

Interface	Status	Rate
WAN	Down	- / -
LAN	Up	1G bps/Full Duplex
WLAN	Enabled	54M
- Registration Status:**

Account	Action	Account Status	Associate Service Provider Name	URI
SIP 1	<input type="button" value="Register"/>	Not Registered	test	123456@isp.net
SIP 2	<input type="button" value="Register"/>	In-Active	test	ChangeMe@isp.net

Additional sections include a **Summary** section with links for [VoIP Status](#) and [WLAN Status](#).

Figure 10 Status Screen (Hybrid Mode)

The screenshot displays the Status Screen in Hybrid Mode. At the top right, there is a 'Refresh Interval' dropdown set to 'None' and an 'Apply' button. The screen is divided into several sections:

- Device Information:** Host Name (P-3202HN-Ba), Model Name (P-3202HN-Ba), Firmware Version (V1.00(BND.0)b3_3|2009/09/15).
- WAN Information:** IP Address (0.0.0.0), IP Subnet Mask (0.0.0.0), Default Gateway (0.0.0.0), MAC Address (00:23:f8:55:bf:2d).
- LAN Information:** IP Address (192.168.1.1), IP Subnet Mask (255.255.255.0), DHCP (Server), MAC Address (00:23:f8:55:bf:2c).
- WLAN Information:** SSID (P-3202HN-Ba), Channel (06), Security (WPA-PSK).
- Security:** Firewall (Disable).
- System Status:** System Uptime (5:38:39), Current Date/Time (2009/09/15 18:23:22), System Mode (Hybrid), CPU Usage (12.25%), Memory Usage (50.86%).
- Interface Status:** A table showing WAN (Down), LAN (Up, 1G bps /Full Duplex), and WLAN (Enabled, 54M).
- Summary:** Links for DHCP Client List, WLAN Status, VoIP Status, and Bandwidth Status.
- Registration Status:** A table with columns for Account, Action, Account Status, Associate Service Provider Name, and URI. It lists SIP 1 (Not Registered) and SIP 2 (In-Active).

Each field is described in the following table.

Table 4 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the IAD to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
Host Name	This field displays the IAD system name. It is used for identification. You can change this in the Maintenance > System > General screen's System Name field.
Model Number	This is the model name of your device.

Table 4 Status Screen

LABEL	DESCRIPTION
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
WAN Information	
IP Address	This field displays the current IP address of the IAD in the WAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Default Gateway	This field displays the IP address of the default gateway, if applicable.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your IAD. This MAC is used for VoIP connections made over the WAN and is different from the LAN MAC.
LAN Information	
IP Address	This field displays the current IP address of the IAD in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	<p>This field displays what DHCP services the IAD is providing to the LAN. Choices are:</p> <p>Server - The IAD is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p>Relay - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.</p> <p>None - The IAD is not providing any DHCP services to the LAN.</p> <p>Click this to go to the screen where you can change it.</p>
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your IAD. This MAC is used for LAN connections and differs from the WAN MAC.
WLAN Information	
SSID	This is the descriptive name used to identify the IAD in the wireless LAN. Click this to go to the screen where you can change it.
Channel	This is the channel number used by the IAD now.
Security	This displays the type of security mode the IAD is using in the wireless LAN.
Security	
Firewall	This displays whether or not the IAD's firewall is activated. Click this to go to the screen where you can change it.
System Status	

Table 4 Status Screen

LABEL	DESCRIPTION
System Uptime	This field displays how long the IAD has been running since it last started up. The IAD starts up when you plug it in, when you restart it (Maintenance > Tools > Restart), or when you reset it (see Section 1.5 on page 25).
Current Date/Time	This field displays the current date and time in the IAD. You can change this in Maintenance > System > Time Setting .
System Mode	This displays whether the IAD is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the IAD's processing ability is currently used. When this percentage is close to 100%, the IAD is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Memory Usage	This field displays what percentage of the IAD's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the IAD is probably becoming unstable, and you should restart the device. See Section 20.4 on page 222 , or turn it off (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the IAD has.
Status	This field indicates whether or not the IAD is using the interface. For the WAN interface, this field displays Up when the IAD is using the interface and Down when the IAD is not using the interface. For the LAN interface, this field displays Up when the IAD is using the interface and Down when the IAD is not using the interface. For the WLAN interface, it displays Enabled when WLAN is activated or Disabled when WLAN is not active.
Rate	For the LAN interface, this displays the port speed and duplex setting. For the WAN interface, this displays the port speed and duplex setting. For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or N/A when WLAN is disabled.
Summary	
DHCP Client List	Click this link to view current DHCP client information. See Section 7.5 on page 65 .
VoIP Status	Click this link to view statistics about your VoIP usage. See Section 4.2.1 on page 47 .
WLAN Status	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the IAD. See Section 4.2.2 on page 49 .
Bandwidth Status	Click this link to view QoS packets statistics on the IAD. See Section 4.2.2 on page 49 .
Registration Status	
Account	This column displays each SIP account in the IAD.

Table 4 Status Screen

LABEL	DESCRIPTION
Registration	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>If the SIP account is already registered with the SIP server,</p> <ul style="list-style-type: none"> Click Unregister to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address. The second field displays Registered. <p>If the SIP account is not registered with the SIP server,</p> <ul style="list-style-type: none"> Click Register to have the IAD attempt to register the SIP account with the SIP server. The second field displays the reason the account is not registered. <p>Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Settings.</p> <p>Register Fail - The last time the IAD tried to register the SIP account with the SIP server, the attempt failed. The IAD automatically tries to register the SIP account when you turn on the IAD or when you activate it.</p>
Action	<p>If the SIP account is already registered with the SIP server, the Account Status field displays Registered.</p> <ul style="list-style-type: none"> Click Unregister to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. <p>If the SIP account is not registered with the SIP server, the Account Status field displays Not Registered.</p> <ul style="list-style-type: none"> Click Register to have the IAD attempt to register the SIP account with the SIP server. The second field displays the reason the account is not registered. <p>The button is grayed out if the SIP account is disabled.</p>
Account Status	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>In-Active - The SIP account is not active. You can activate it in VoIP > SIP > SIP Account.</p> <p>Not Registered - The last time the IAD tried to register the SIP account with the SIP server, the attempt failed. Use the Register button to register the account again. The IAD automatically tries to register the SIP account when you turn on the IAD or when you activate it.</p> <p>Registered - The SIP account is already registered with the SIP server. You can use it to make a VoIP call.</p> <p>Register Fail - The last time the IAD tried to register the SIP account with the SIP server, the attempt failed. The IAD automatically tries to register the SIP account when you turn on the IAD or when you activate it.</p>

Table 4 Status Screen

LABEL	DESCRIPTION
Associate Service Provider Name	This field displays the VoIP service provider's name that you specified in the VoIP > SIP > SIP Service Provider screen.
URI	This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screens.

4.2.1 VoIP Status

Click **Status > VoIP Status** to access this screen.

Figure 11 VoIP Status

The screenshot shows the VoIP Status screen with three main sections:

- SIP Status:** A table with columns: Account, Registration, Last Registration, URI, Last Incoming Number, and Last Outgoing Number. It lists two accounts, SIP1 and SIP2, both with a 'Disabled' registration and 'Unregistered' status.
- Call Status:** A table with columns: Account, Duration, Status, Codec, and Peer Number. It lists two accounts, SIP1 and SIP2, both with a duration of '0 Day(s), 0 Hour(s), 0 Minute(s), 0 Second(s)' and a status of 'Idle'.
- Phone Status:** A table with columns: Phone, Outgoing Number, and Incoming Number. It lists two phones, Phone1 and Phone2, both with 'ChangeMe' for both outgoing and incoming numbers.

Each field is described in the following table.

Table 5 VoIP Status

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the IAD.

Table 5 VoIP Status

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You can change this in the Status screen. Registered - The SIP account is registered with a SIP server. Error - The last time the IAD tried to register the SIP account with the SIP server, the attempt failed. The IAD automatically tries to register the SIP account when you turn on the IAD or when you activate it. Disabled - The SIP account is not active. You can activate it in VoIP > SIP > SIP Account .
Last Registration	This field displays the last time you successfully registered the SIP account. It displays Unregistered if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screens.
Protocol	This field displays the transport protocol the SIP account uses. SIP accounts always use UDP.
Message-Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the IAD.
Hook	This field indicates whether the phone is on the hook or off the hook. On - The phone is hanging up or already hung up. Off - The phone is dialing, calling, or connected.
Duration	This field displays how long the current call has lasted. It displays 0 if no call has ever been made using the SIP account.
Status	This field displays the current state of the phone call. Idle - There are no current VoIP calls, incoming calls or outgoing calls being made. Dial - The callee's phone is ringing. Ring - The phone is ringing for an incoming VoIP call. Process - There is a VoIP call in progress. DISC - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	

Table 5 VoIP Status

LABEL	DESCRIPTION
Phone	This field displays each phone port in the IAD.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incomming Number	This field displays the SIP number that you use to receive calls on this phone port.
Poll Interval(s)	Enter how often you want the IAD to update this screen, and click Set Interval .
Set Interval	Click this to make the IAD update the screen based on the amount of time you specified in Poll Interval .
Stop	Click this to make the IAD stop updating the screen.

4.2.2 WLAN Status

Click **Status > WLAN Status** to access this screen. Use this screen to view the wireless stations that are currently associated to the IAD.

Figure 12 Status > WLAN Status

The following table describes the labels in this screen.

Table 6 Status > WLAN Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the IAD.
Refresh	Click Refresh to reload this screen.

Device Mode Screen

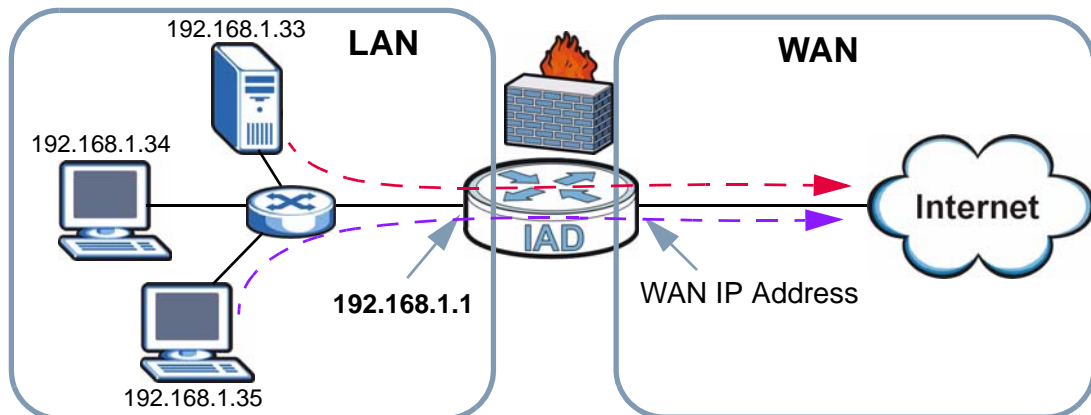
5.1 Overview

The **Status** screen lets you configure whether the IAD is a router or bridge. You can choose between **Hybride Mode** and **Bridge Mode** depending on your network topology and the features you require from your IAD. See [Section 1.4 on page 22](#) for more information on which mode to choose.

5.1.1 Hybrid Mode (Router Mode)

A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address. The router can use NAT to translate the packet's source IP address before forwarding it from the LAN to the WAN or from the LAN to the WAN.

Figure 13 LAN and WAN IP Addresses in Hybrid Mode (Router Mode)

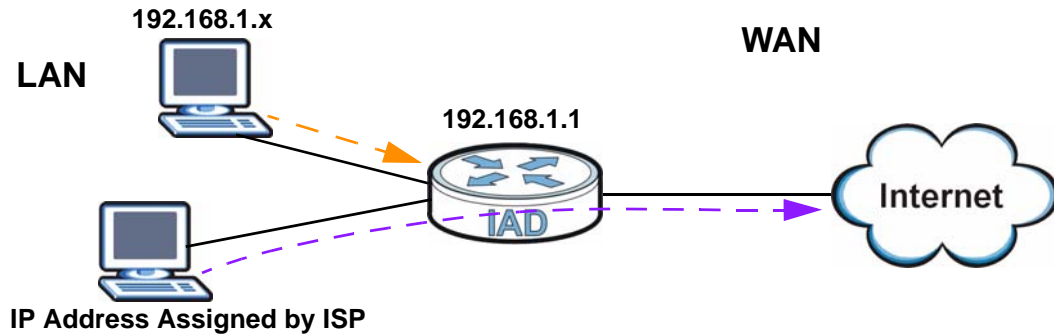


5.1.2 Bridge Mode

When the IAD acts as a bridge, the routing features will not be available. That means a bridge can not use NAT to translate the packet's source IP address before forwarding it. You need to set the client computer to receive an IP address automatically from the ISP. Computers behind the IAD cannot share the same Internet account. To configure the IAD, you need to manually set the computer's

IP address to be in the same subnet as the IAD since the DHCP server is also disabled on the IAD in bridge mode.

Figure 14 IP Addresses in Bridge Mode



5.2 Device Mode Screen

Click **Device > Device Mode** to open this screen. The IAD restarts automatically after you select a different device mode and click **Apply**.

Figure 15 Device Mode Screen



The following table lists the features available for each device mode.

Table 7 Hybrid and Bridge Modes Features Comparison

FEATURE	HYBRID MODE	BRIDGE MODE
DHCP Client List	Y	
WLAN Status	Y	Y
Bandwidth Status	Y	
Device Mode	Y	Y
WAN	Y	Y
LAN	Y	Y
Wireless LAN	Y	Y
NAT	Y	
SIP	Y	Y
Phone	Y	Y

Table 7 Hybrid and Bridge Modes Features Comparison

FEATURE	HYBRID MODE	BRIDGE MODE
Phone Book	Y	Y
VoIP Status	Y	Y
Firewall	Y	
Static Route	Y	
Bandwidth MGMT	Y	
Dynamic DNS	Y	
Remote MGMT	Y	Y
System	Y	Y
Logs	Y	Y
Tools	Y	Y
Diagnostic	Y	Y

Table Key: A Y in a mode's column shows that the device mode has the specified feature. The information in this table was correct at the time of writing, although it may be subject to change.

6.1 Overview

This chapter describes how to configure WAN settings. A WAN (Wide Area Network) is an outside connection to another network or the Internet.

6.1.1 What You Need to Know

The following terms and concepts may help as you read through the chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The IAD supports the following methods.

PPP over Ethernet

The IAD supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

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

One of the benefits of PPPoE is the ability to let you 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 individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the IAD (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the IAD does that part of the task.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

6.2 Internet Access Setup

Use this screen to change your IAD's WAN remote node settings. Click **Network > WAN > Internet Access Setup**. Although the screen differs by the encapsulation you select, all options are presented in the image below.

Figure 16 Internet Access Setup - PPPoE

Internet Access Setup

General

Encapsulation: PPPoE

User Name:

Password:

Service Name:

IP Address

Obtain an IP Address Automatically

Static IP Address

DNS Server

First DNS Server: FromISP

Second DNS Server: FromISP

Third DNS Server: FromISP

Connection

Nailed-Up Connection

Connection Demand Max Idle Timeout sec

Apply Cancel

Figure 17 Internet Access Setup - IP

The following table describes the labels in this screen.

Table 8 Internet Access Setup

LABEL	DESCRIPTION
General	
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Service Name	Type the name of your PPPoE service here.
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned information in the field below.
IP Address	Enter the IP address assigned by your ISP if you select Static IP Address .
Subnet Mask	Enter a subnet mask in dotted decimal notation when you select IP in the Encapsulation field.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you select IP in the Encapsulation field.
DNS Server	

Table 8 Internet Access Setup (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the IAD's WAN IP address) and you select Obtain an IP Address Automatically.</p> <p>Select UserDefined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose UserDefined, but leave the IP address set to 0.0.0.0, UserDefined changes to None after you click Apply. If you set a second choice to UserDefined, and enter the same IP address, the second UserDefined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Connection	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The IAD will try to bring up the connection automatically if it is disconnected.
Connection Demand	Select Connection Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connection Demand . The default setting is 0, which means the Internet session will not timeout.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

LAN Setup

This chapter describes how to configure LAN settings.

7.1 LAN Overview

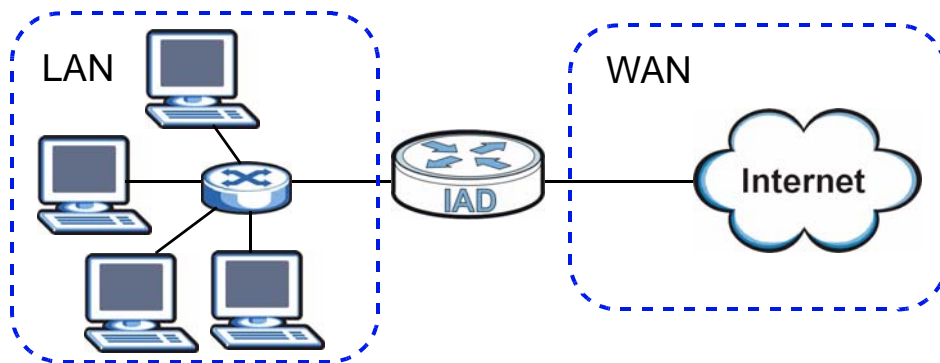
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 7.4 on page 63](#) to configure the **LAN** screens.

7.1.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the IAD ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 18 LAN and WAN IP Addresses



7.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can

configure the IAD as a DHCP server or disable it. When configured as a server, the IAD provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

7.1.2.1 IP Pool Setup

The IAD is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

7.2 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- 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 in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The IAD supports the IPCP DNS server extensions through the DNS proxy feature.

If the **DNS Server** fields in the **DHCP Setup** screen are set to **DNS Relay**, the IAD tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the IAD, the IAD acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

7.3 LAN TCP/IP

The IAD has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

7.3.1 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 most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the IAD. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 10.0.0.138, for your IAD, 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. Your IAD will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the IAD unless you are instructed to do otherwise.

7.3.1.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for

your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

7.3.2 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the IAD will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the IAD will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the IAD will send out RIP packets but will not accept any RIP packets received.
- **None** - the IAD will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the IAD sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

7.3.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not

assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The IAD supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the IAD queries all directly connected networks to gather group membership. After that, the IAD periodically updates this information. IP multicasting can be enabled/disabled on the IAD LAN ~~and/or WAN~~ interfaces in the Web Configurator (~~LAN, WAN~~). Select **None** to disable IP multicasting on these interfaces.

7.4 Configuring LAN IP and DHCP

Click **Network > LAN** to open the **IP & DHCP** screen. See [Section 7.1 on page 59](#) for background information. Use this screen to set the Local Area Network IP address and subnet mask of your IAD. You can also edit your IAD's RIP and multicast settings, and DNS server information that the IAD sends to the DHCP client devices on the LAN.

Figure 19 LAN IP & DHCP

The screenshot shows the 'IP & DHCP' configuration page with the following settings:

- LAN TCP/IP:** IP Address: 192.168.1.1; IP Subnet Mask: 255.255.255.0
- RIP & Multicast Setup:** RIP Direction: None; RIP Version: RIP-2M; Multicast: IGMP-v2
- DHCP Setup:** DHCP: Server; IP Pool Starting Address: 192.168.1.33; Pool Size: 32
- DNS Server:** First, Second, and Third DNS Servers: All set to 'FromISP' with IP address 0.0.0.0

Buttons for 'Apply' and 'Cancel' are located at the bottom of the form.

The following table describes the fields in this screen.

Table 9 LAN IP & DHCP

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the LAN IP address you want to assign to your IAD in dotted decimal notation, for example, 10.0.0.138 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your IAD automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
Advanced/Basic	Click Advanced to display and edit RIP and multicast settings. Otherwise, click Basic to hide them.
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The IAD supports both IGMP version 1 (IGMP-v1) and IGMP-v2 . Select None to disable it.
DHCP Setup	
DHCP	<p>If set to Server, your IAD can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to None, the DHCP server will be disabled.</p> <p>If set to Relay, the IAD acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Remote DHCP Server	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.
DNS Server	<p>This section displays only when you select Server in the DHCP field.</p> <p>The IAD passes a DNS (Domain Name System) server IP address to the DHCP clients.</p>

Table 9 LAN IP & DHCP (continued)

LABEL	DESCRIPTION
First DNS Server	Select FromISP if your ISP dynamically assigns DNS server information (and the IAD's WAN IP address).
Second DNS Server	Select UserDefined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose UserDefined, but leave the IP address set to 0.0.0.0, UserDefined changes to None after you click Apply. If you set a second choice to UserDefined, and enter the same IP address, the second UserDefined changes to None after you click Apply.
Third DNS Server	Select DNS Relay to have the IAD act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The IAD's LAN IP address displays in the field to the right (read-only). The IAD tells the DHCP clients on the LAN that the IAD itself is the DNS server. When a computer on the LAN sends a DNS query to the IAD, the IAD forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you click Apply. Select None if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

7.5 LAN Client List

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the IAD as a DHCP server or disable it. When configured as a server, the IAD provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Network > LAN > Client List** to open the following screen. **The read-only table shows current DHCP client information of all network clients using the IAD's**

DHCP server. Use this screen to view IP addresses on the LAN assigned to specific individual computers based on their MAC Addresses.

Figure 20 LAN Client List

The screenshot shows a web interface with three tabs: 'IP & DHCP', 'Client List' (selected), and 'IP Alias'. Below the tabs is a table titled 'DHCP Client Table' with the following data:

#	IP Address ▲	MAC Address	Expiration time
1	192.168.001.033	00:21:85:0c:44:4b	2009/09/15 - 15:35:52

The following table describes the labels in this screen.

Table 10 LAN Client List

LABEL	DESCRIPTION
#	This is the index number of the IP table entry (row).
IP Address	This field displays the IP address assigned to the client computer.
MAC Address	Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. This field displays the MAC address of the client computer.
Expiration Time	This field displays the date and time the IP address expires. The client computer then cannot use this IP address and needs to request information from the DHCP server again.

7.6 LAN IP Alias

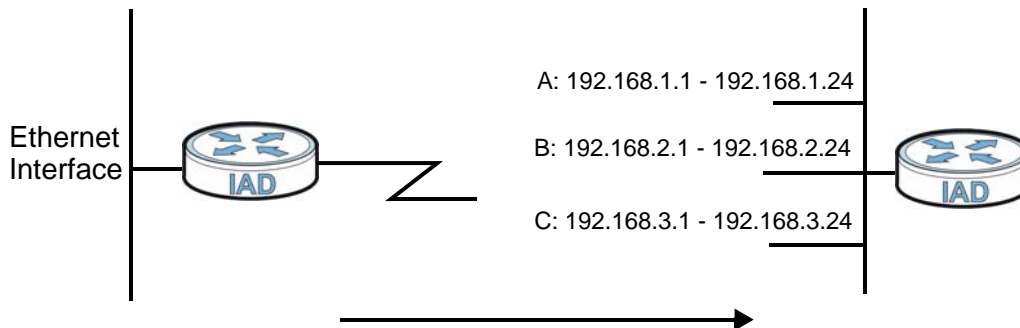
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The IAD supports three logical LAN interfaces via its single physical Ethernet interface with the IAD itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

Figure 21 Physical Network & Partitioned Logical Networks



Click **Network > LAN > IP Alias** to open the following screen. Use this screen to change your IAD's IP alias settings.

Figure 22 LAN IP Alias

The screenshot shows the 'LAN IP Alias' configuration screen. At the top, there are three tabs: 'IP & DHCP', 'Client List', and 'IP Alias', with 'IP Alias' selected. Below the tabs, there are two sections for configuring IP aliases. The first section is titled 'IP Alias 1' and contains a checkbox labeled 'IP Alias 1'. Below the checkbox are two input fields: 'IP Address' and 'IP Subnet Mask'. The second section is titled 'IP Alias 2' and contains a checkbox labeled 'IP Alias 2', followed by 'IP Address' and 'IP Subnet Mask' input fields. At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 11 LAN IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the IAD.
IP Address	Enter the IP address of your IAD in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your IAD will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the IAD.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

Wireless LAN

8.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.

See [Chapter 3 on page 35](#) for a tutorial showing how to set up your wireless connection in an example scenario.

See [Section 8.10 on page 89](#) for advanced technical information on wireless networks.

8.1.1 What You Can Do in this Chapter

This chapter describes the IAD's **Network > Wireless LAN** screens. Use these screens to set up your IAD's wireless connection.

- The **General** screen lets you turn the wireless connection on or off, set up wireless security and make other basic configuration changes ([Section 8.4 on page 73](#)). You can also configure the MAC filter to allow or block access to the IAD based on the MAC addresses of the wireless stations.
- The **More AP** screen lets you set up multiple wireless networks on your IAD ([Section 8.5 on page 82](#)).
- Use the **WPS** screen and the **WPS Station** screen to use WiFi Protected Setup (WPS). WPS lets you set up a secure network quickly, when connecting to other WPS-enabled devices.

Use the **WPS** screen (see [Section 8.6 on page 83](#)) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the IAD's WPS status.

Use the **WPS Station** (see [Section 8.7 on page 85](#)) screen to set up WPS by pressing a button or using a PIN.

- The **WDS** screen lets you set up a Wireless Distribution System, in which the IAD acts as a bridge with other ZyXEL access points ([Section 8.8 on page 86](#)).
- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes ([Section 8.9 on page 88](#)).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

8.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Wireless Network Construction

Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

Network Names

Each network must have a name, referred to as the SSID - "Service Set Identifier". The "service set" is the network, so the "service set identifier" is the network's name. This helps you identify your wireless network when wireless

networks' coverage areas overlap and you have a variety of networks to choose from.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

Wireless Security

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network she/he can either steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is perfectly secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use “70dodchal71vanpoi” as your security key.

Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

8.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See [Section 8.2 on page 70](#) if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

8.4 The General Screen

Note: If you are configuring the IAD from a computer connected to the wireless LAN and you change the IAD's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the IAD's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 23 Network > Wireless LAN > General

The following table describes the labels in this screen.

Table 12 Network > Wireless LAN > General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel or use Auto to have the IAD automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the IAD is currently using then displays next to this field.

Table 12 Network > Wireless LAN > General

LABEL	DESCRIPTION
Bandwidth	<p>Select whether the IAD uses a wireless channel width of 20MHz or 40MHz.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p> <p>This field is available only when you set the 802.11 Mode to 802.11n Only or 802.11b/g/n Mixed in the Advanced Setup screen.</p>
Control Sideband	<p>This is available for some regions when you select a specific channel and set the Bandwidth field to 40MHz. Set whether the control channel (set in the Channel field) should be in the Lower or Upper range of channel bands.</p> <p>This field is available only when you set the 802.11 Mode to 802.11n Only or 802.11b/g/n Mixed in the Advanced Setup screen.</p>
Network Name (SSID)	<p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <p>Note: If you are configuring the IAD from a computer connected to the wireless LAN and you change the IAD's SSID or wireless security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the IAD's new settings.</p>
Hide Network Name (SSID)	<p>Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.</p>
Enable Wireless Multicast Forwarding (WMF)	<p>Select this check box to allow the IAD to convert wireless multicast traffic into wireless unicast traffic.</p>
BSSID	<p>This shows the MAC address of the wireless interface on the IAD when wireless LAN is enabled.</p>
Security Mode	<p>See the following sections for more details about this field.</p>
MAC Filter	<p>Click this button to go to the MAC Filter screen to configure whether the wireless devices with the MAC addresses listed are allowed or denied to access the IAD using this SSID.</p>
Apply	<p>Click this to save your changes back to the IAD.</p>
Reset	<p>Click this to reload the previous configuration for this screen.</p>

8.4.1 No Security

Select **No Security** to allow wireless devices to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your IAD, your network is accessible to any wireless networking device that is within range.

Figure 24 Wireless LAN > General: No Security

The screenshot shows the configuration interface for the Wireless LAN > General settings. The 'Security Mode' dropdown menu is set to 'No Security'. Other visible settings include 'Enable Wireless LAN' (checked), 'Name (SSID)' (P-3202HN-Ba), 'Channel Selection' (Channel-06 2437MHz), and '802.11 Mode' (802.11 B/G/N). There are 'Apply' and 'Cancel' buttons at the bottom.

The following table describes the labels in this screen.

Table 13 Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.

8.4.2 WEP Encryption

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **WEP** from the **Security Mode** list.

Figure 25 Wireless LAN > General: Static WEP Encryption

The screenshot shows the 'General' tab of the Wireless LAN configuration interface. It is divided into three sections: 'Wireless Setup', 'Wireless Advanced Setup', and 'Security'. In the 'Security' section, 'Static WEP' is selected as the Security Mode. The WEP Key field contains the hexadecimal string '6456d36652220045192fb2b53d'. A 'Generate' button is located next to the Passphrase field. A note at the bottom explains that WEP key lengths of 5, 13, 10, or 26 characters correspond to 40/64-bit, 128-bit, 104-bit, and 152-bit security strengths, respectively. 'Apply' and 'Cancel' buttons are at the bottom.

The following table describes the wireless LAN security labels in this screen.

Table 14 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose WEP from the drop-down list box.

Table 14 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select 64-bit or 128-bit to enable data encryption.
Key 1 to Key 4	The WEP key is used to secure your data from eavesdropping by unauthorized wireless users. Both the IAD and the wireless stations must use the same WEP key for data transmission. Only one key can be activated at any one time. Select a default key to use for data encryption. If you chose 64-bit in the WEP Encryption field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose 128-bit in the WEP Encryption field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.

8.4.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 26 Wireless LAN > General: WPA(2)-PSK

The screenshot shows the 'General' tab of the Wireless LAN configuration interface. The 'Wireless Setup' section includes:

- Enable Wireless LAN
- Name(SSID): P-3202HN-Ba
- Hide SSID
- Auto Channel Selection
- Channel Selection: Channel-06 2437MHz

 The 'Wireless Advanced Setup' section includes:

- RTS/CTS Threshold: 2346 (range 256~2346)
- 802.11 Mode: 802.11 B/G/N
- [Basic](#) link

 The 'Security' section includes:

- Security Mode: WPA2-PSK
- WPA Compatible
- Pre-Shared Key: 00000000

 At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the wireless LAN security labels in this screen.

Table 15 Wireless LAN > General: WPA(2)-PSK

LABEL	DESCRIPTION
Auto Generate Key	This field is only available for WPA-PSK. Select this option to have the IAD automatically generate an SSID and pre-shared key. The SSID and Pre-Shared Key fields will not be configurable when you select this option.
Security Mode	Choose WPA-PSK or WPA2-PSK from the drop-down list box.
Active Compatible	This field is only available for WPA2-PSK. Select this if you want the IAD to support WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (TKIP , AES or TKIP+AES) for data encryption. Select TKIP if your wireless clients can all use TKIP. Select AES if your wireless clients can all use AES. Select TKIP+AES to allow the wireless clients to use either TKIP or AES.
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients.

8.4.4 WPA(2) Authentication

Use this screen to configure and enable WPA or WPA2 authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Note: WPA or WPA2 is not available if you enable WPS before you configure WPA or WPA2 in the **Wireless LAN > General** screen.

Note: If you select **WPA** or **WPA2** in the **Wireless LAN > General** screen, the **WDS** and **WPS** features are not available on the IAD.

Figure 27 Wireless LAN > General: WPA(2)

The screenshot shows the 'General' tab of the Wireless LAN configuration interface. It is divided into three sections: 'Wireless Setup', 'Wireless Advanced Setup', and 'Security'. In the 'Security' section, 'Security Mode' is set to 'WPA2'. Other settings include 'Enable Wireless LAN' checked, SSID 'P-3202HN-Ba', and an authentication server IP of '192.168.1.2' with port '1812' and shared secret 'ralink11'. 'Apply' and 'Cancel' buttons are at the bottom.

The following table describes the wireless LAN security labels in this screen.

Table 16 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose WPA or WPA2 from the drop-down list box.
Active Compatible	This field is only available for WPA2. Select this if you want the IAD to support WPA and WPA2 simultaneously.
Encryption	Select the encryption type (TKIP , AES or TKIP+AES) for data encryption. Select TKIP if your wireless clients can all use TKIP. Select AES if your wireless clients can all use AES. Select TKIP+AES to allow the wireless clients to use either TKIP or AES.

Table 16 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
WPA2 Preauthentication	This field is available only when you select WPA2 . Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select Enabled to turn on preauthentication in WAP2. Otherwise, select Disabled .
Network Re-auth Interval	This field is available only when you select WPA2 . Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 2147483647 seconds. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The Group Key Update Timer is the rate at which the RADIUS server sends a new group key out to all clients.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the IAD. The key must be the same on the external authentication server and your IAD. The key is not sent over the network.

8.4.5 MAC Filter

This screen allows you to configure the IAD to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the IAD (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to change your IAD's MAC filter settings. Click the **Edit** button in the **Wireless LAN > General** screen. The following screen displays.

Figure 28 Wireless LAN > MAC Filter



The following table describes the labels in this screen.

Table 17 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below. Select Disabled to turn off MAC address filtering. Select Allow to permit access to the IAD, MAC addresses not listed will be denied access to the IAD. Select Deny to block access to the IAD, MAC addresses not listed will be allowed to access the IAD
#	This is the index number of the MAC address.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the IAD.
Modify	Click the Remove icon to delete the entry.
Back	Click this to return to the previous screen without saving changes.
Add	Click this to create a new MAC filtering rule.

8.4.6 Adding a New MAC Filtering Rule

Click the **Add** button in the **MAC Filter** screen. The following screen displays.

Figure 29 Wireless LAN > MAC Filter > Add



The following table describes the labels in this screen.

Table 18 Wireless LAN > MAC Filter > Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the IAD in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Back	Click this to return to the previous screen without saving changes.
Apply	Click this to save your changes and go back to the previous screen.

8.5 The More AP Screen

This screen allows you to enable and configure multiple wireless networks on the IAD.

Click **Network > Wireless LAN > More AP**. The following screen displays.

Figure 30 Network > Wireless LAN > More AP



The following table describes the labels in this screen.

Table 19 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	Select the check box to activate an SSID profile.
SSID	An SSID profile is the set of parameters relating to one of the IAD's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the Edit icon to configure the SSID profile.

Table 19 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the IAD.
Reset	Click Reset to reload the previous configuration for this screen.

8.5.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 31 Network > Wireless LAN > More AP: Edit

See [Section 8.4 on page 73](#) for more details about the fields in this screen.

8.6 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your IAD.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

Click **Network > Wireless LAN > WPS**. The following screen displays.

Figure 32 Network > Wireless LAN > WPS

The screenshot shows a configuration window for WPS. At the top, there are tabs for 'General', 'WPS', 'WPS Station', 'MAC Filter', and 'QoS'. The 'WPS' tab is selected. Below the tabs, there are two main sections: 'WPS Setup' and 'WPS Status'. In the 'WPS Setup' section, the 'Enable WPS' checkbox is checked. Below it, the 'PIN Number' is displayed as '19341255' next to a 'Generate' button. The 'WPS Status' section shows the current status as 'Configured' with a 'Release_Configuration' button. Other status details include '802.11 Mode: 802.11 B/G/N', 'SSID: P-3202HN-Ba', 'Security: WPA-PSK', and 'Pre-Shared Key: 12345678'. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 20 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the IAD.
PIN Number	This shows the PIN (Personal Identification Number) of the IAD. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the IAD create a new PIN.
WPS Status	This displays Configured when the IAD has connected to a wireless network using WPS or Enable WPS is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays Unconfigured if WPS is disabled and there is no wireless or wireless security changes on the IAD or you click Release_Configuration to remove the configured wireless and wireless security settings.
Release_Configuration	This button is available when the WPS status is Configured but not configurable if you disable WPS. Click this button to remove all configured wireless and wireless security settings for WPS connections on the IAD.
Apply	Click Apply to save your changes back to the IAD.

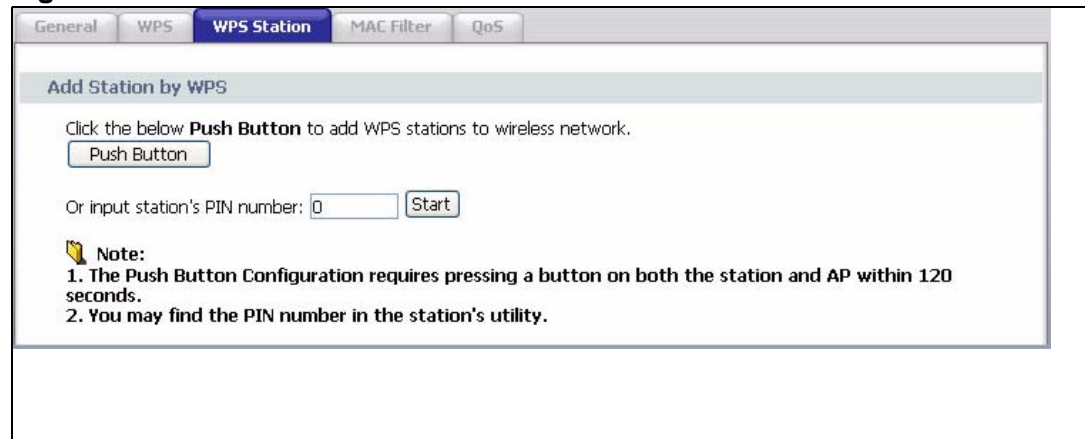
8.7 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Note: If you select **No Security** in the **Wireless LAN > General** screen and click **Push Button** in the **WPS Station** screen, the IAD automatically changes to use WPA-PSK/WPA2-PSK mixed mode and generates a pre-shared key.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

Figure 33 Network > Wireless LAN > WPS Station



The following table describes the labels in this screen.

Table 21 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	<p>Click this button to add another WPS-enabled wireless device (within wireless range of the IAD) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the Push Button on this screen.</p> <p>Note: You must press the other wireless device's WPS button within two minutes of pressing this button.</p>
Or input station's PIN number	<p>Enter the PIN of the device that you are setting up a WPS connection with and click Start to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the IAD.</p>

8.8 The WDS Screen

A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to set up your WDS links between the IADs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between the devices is made.

Note: You cannot use WDS when WPS is enabled or wireless security is set to "WPA" or "WPA2". The wireless security settings apply to both WDS links and the connections between the ZyXEL Device and any wireless clients.

Note: At the time of writing, WDS is only compatible with other ZyXEL Devices of the same model.

Click **Network > Wireless LAN > WDS**. The following screen displays. WDS is turned on and this screen is configurable when the ZyXEL Device's wireless security mode is **No Security**, **WEP** or **WPA(2)-PSK**.

Figure 34 Network > Wireless LAN > WDS



The following table describes the labels in this screen.

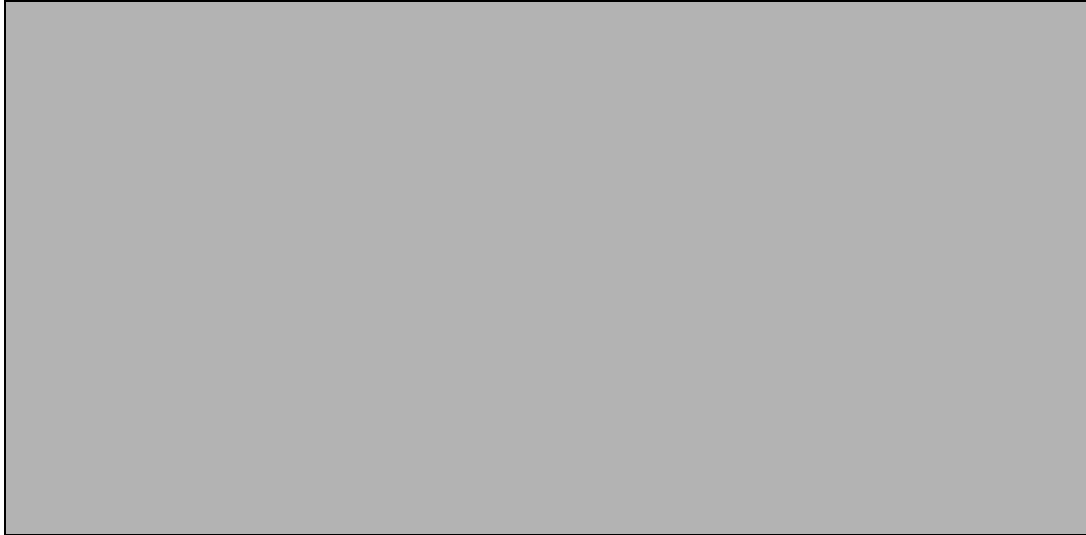
Table 22 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS	
Operating Mode	<p>Select the operating mode for your IAD.</p> <ul style="list-style-type: none"> • Access Point + Bridge - The IAD functions as a bridge and access point simultaneously. • Wireless Bridge - The IAD acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the IAD wirelessly. <p>You need to know the MAC address of the peer device, which must be of the same model and also WDS-enabled. The IAD can establish up to four wireless links with other APs.</p>
Bridge Restrict	<p>This field is available only when you set operating mode to Access Point + Bridge.</p> <p>Select Enabled to turn on WDS and enter the peer device's MAC address manually in the table below.</p> <p>Select Enabled(Scan) to turn on WDS, search and display the available APs within range in the table below.</p>
Remote Bridges MAC Address	<p>Enter the MAC address of the peer device that your IAD wants to make a bridge connection with.</p> <p>You can connect to up to 4 peer devices.</p>
	<p>This field is available only when you select Enabled(Scan) in the Bridge Restrict field.</p> <p>Select the check box and click Apply to have the IAD establish a wireless link with the selected wireless device.</p>
SSID	<p>This field is available only when you select Enabled(Scan) in the Bridge Restrict field.</p> <p>This shows the SSID of the available wireless device within range.</p>
BSSID	<p>This field is available only when you select Enabled(Scan) in the Bridge Restrict field.</p> <p>This shows the MAC address of the available wireless device within range.</p>
Refresh	<p>Click Refresh to update the Remote Bridges MAC Address table when Bridge Restrict is set to Enabled(Scan).</p>
Apply	<p>Click Apply to save your changes to IAD.</p>

8.9 The Advanced Setup Screen

To configure advanced wireless settings, click **Network > Wireless LAN > Advanced Setup**. The screen appears as shown.

Figure 35 Wireless LAN > Advanced Setup



The following table describes the labels in this screen.

Table 23 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Number of Wireless Stations Allowed	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the IAD.
Output Power	Set the output power of the IAD. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following 20% , 40% , 60% , 80% or 100% .
Multicast Rate	Select a data rate at which the IAD transmits wireless multicast traffic. If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion.

Table 23 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
802.11 Mode	<p>Select 802.11b Only to only allow IEEE 802.11b compliant WLAN devices to associate with the IAD.</p> <p>Select 802.11g Only to allow IEEE 802.11g compliant WLAN devices to associate with the IAD. IEEE 802.11b compliant WLAN devices can associate with the IAD only when they use the short preamble type.</p> <p>Select 802.11n Only to only allow IEEE 802.11n compliant WLAN devices to associate with the IAD. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the IAD.</p> <p>Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the IAD. The IAD adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices.</p> <p>Select 802.11 b/g/n mixed mode to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the IAD. The transmission rate of your IAD might be reduced.</p>
802.11 Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select Off to disable 802.11 protection. The transmission rate of your IAD might be reduced in a mixed-mode network.</p> <p>This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.</p>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are Long or Short. The default setting is Long. See the appendix for more information.</p> <p>This field is not configurable and the IAD uses Short when you set 802.11 Mode to 802.11g Only or 802.11n Only.</p>
Apply	Click this to save your changes back to the IAD.
Reset	Click this to reload the previous configuration for this screen.

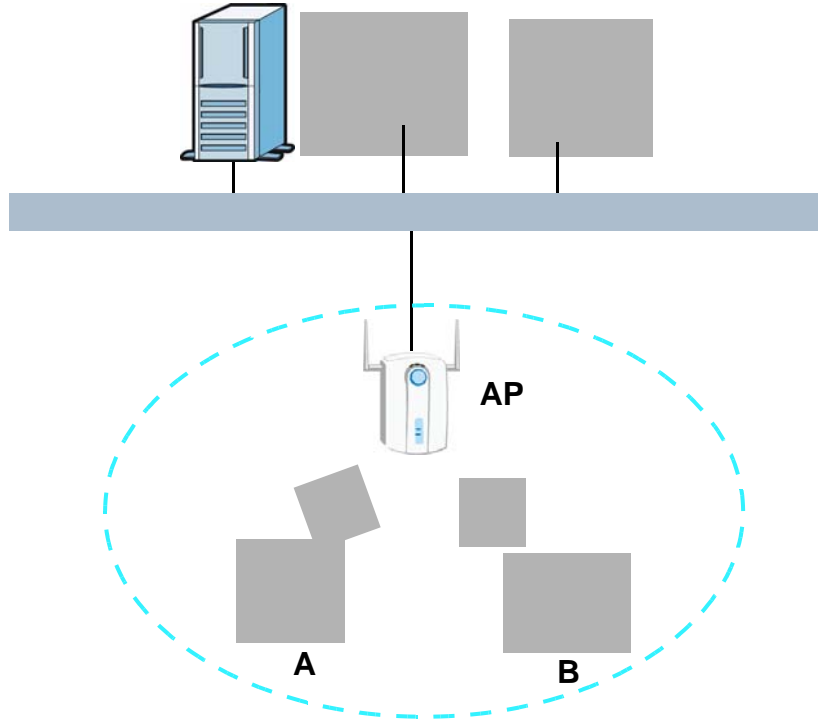
8.10 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

8.10.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 36 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your IAD is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

8.10.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the IAD's Web Configurator.

Table 24 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the IAD. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the IAD.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the IAD does, it cannot communicate with the IAD.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

8.10.3 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

8.10.3.1 SSID

Normally, the IAD acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the IAD does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

8.10.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal

characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the IAD which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

8.10.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

8.10.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

-
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of authentication. (See [Section 8.10.3.3 on page 92](#) for information about this.)

Table 25 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the IAD and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your IAD, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the IAD.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

8.10.4 WiFi Protected Setup

Your IAD supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works

between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

8.10.4.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the IAD, see [Section 8.7 on page 85](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the IAD you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

8.10.4.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the IAD, see [Section 8.6 on page 83](#)).
- 4 Enter the client's PIN in the AP's configuration interface.

Note: If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

- 5 Start WPS on both devices within two minutes.

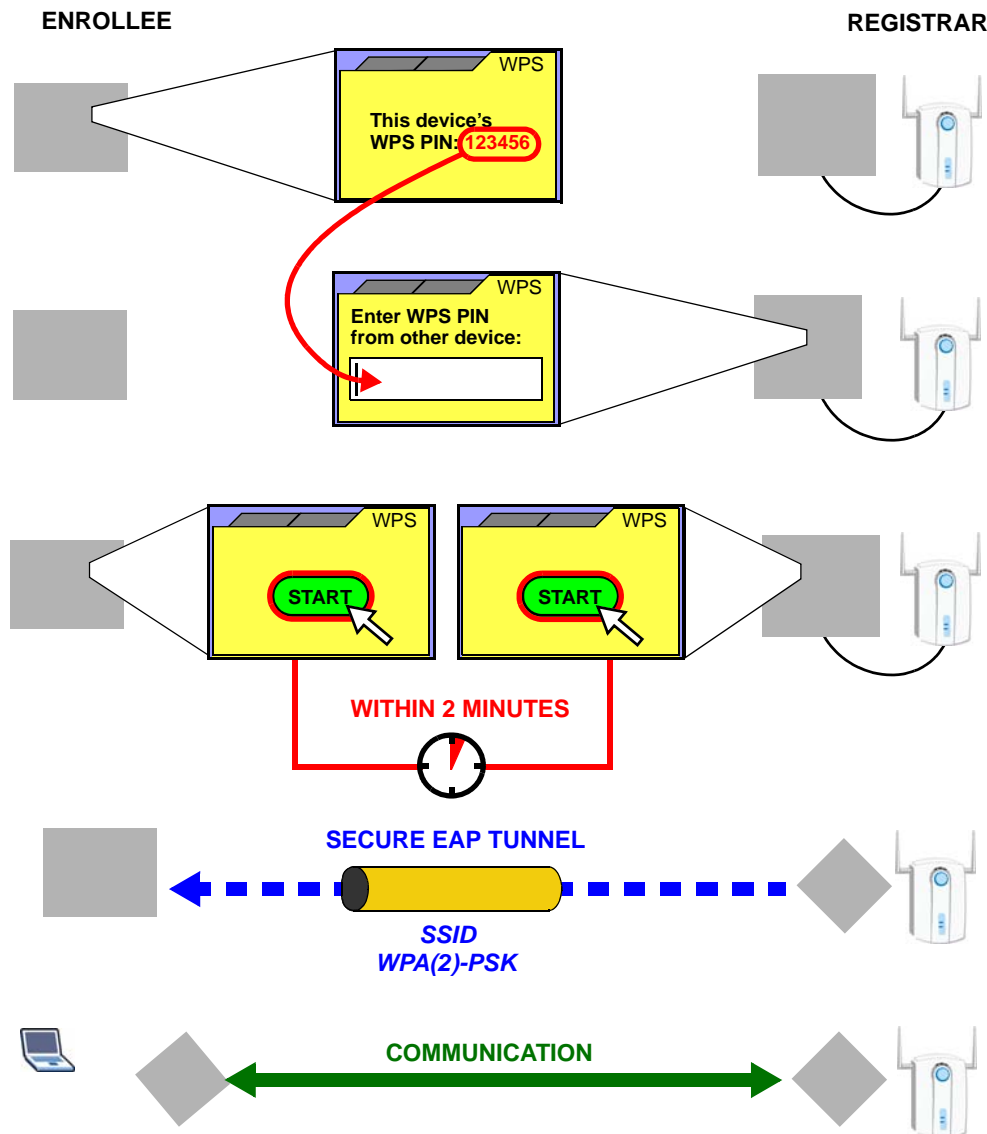
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

- 6 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 37 Example WPS Process: PIN Method

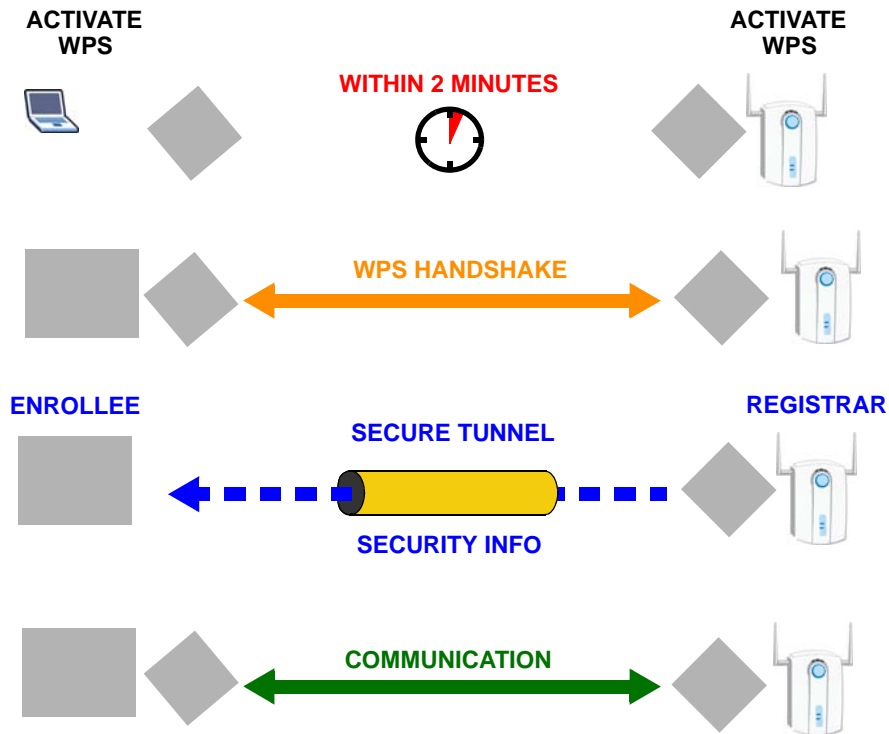


8.10.4.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 38 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

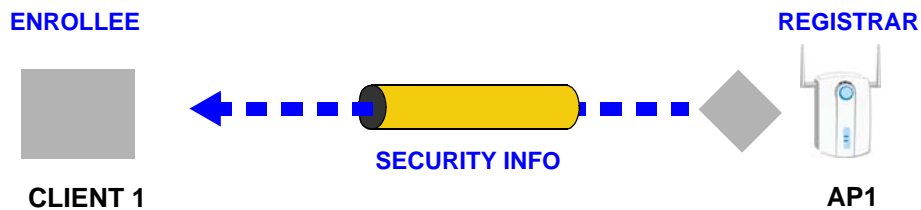
By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

8.10.4.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

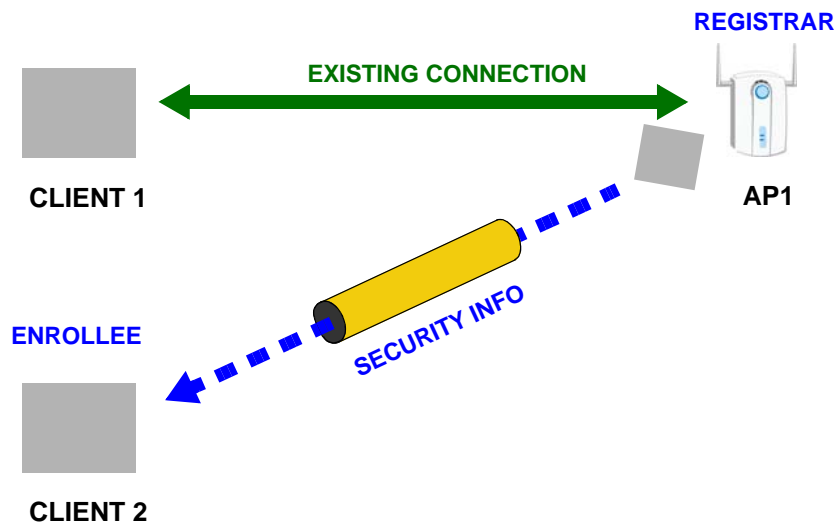
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 39 WPS: Example Network Step 1



In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

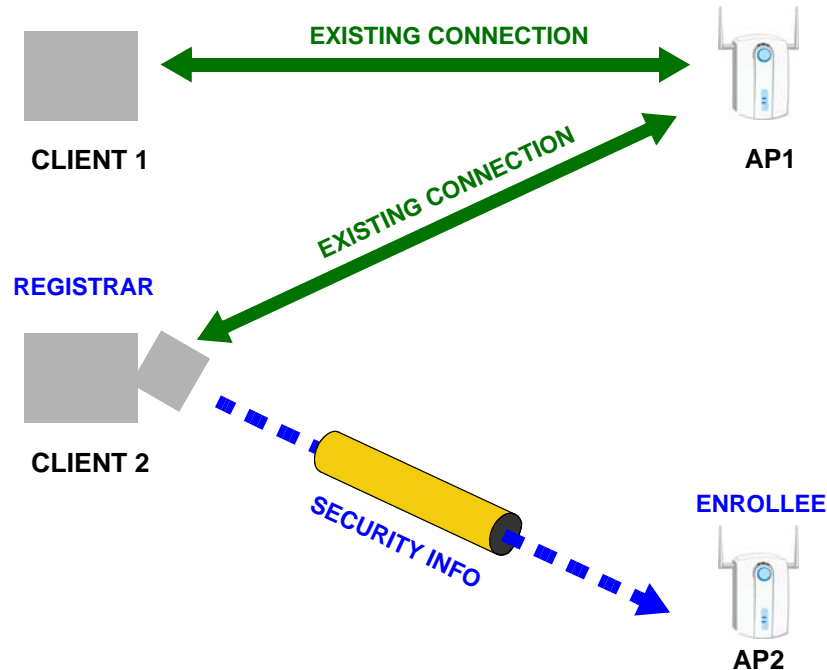
Figure 40 WPS: Example Network Step 2



In step **3**, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access

point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 41 WPS: Example Network Step 3



8.10.4.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

Network Address Translation (NAT)

9.1 Overview

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 to a different IP address known within another network.

This chapter discusses how to configure NAT on the IAD.

See [Section 9.6 on page 112](#) for advanced technical information on NAT.

9.1.1 What You Can Do in this Chapter

- Use the **General** screen ([Section 9.2 on page 102](#)) to configure the NAT setup settings.
- Use the **Port Forwarding** screen ([Section 9.3 on page 104](#)) to configure forward incoming service requests to the server(s) on your local network.
- Use the **Address Mapping** screen ([Section 9.4 on page 108](#)) to change your IAD's address mapping settings.
- Use the **ALG** screen ([Section 9.5 on page 111](#)) to enable and disable the SIP (VoIP) ALG in the IAD.

9.1.2 What You Need To Know

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the IAD, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the

packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The IAD also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 33 on page 115](#).

- Choose **SUA Only** if you have just one public WAN IP address for your IAD.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your IAD.

9.2 The NAT General Screen

Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the IAD.

Click **Network > NAT** to open the following screen.

Figure 42 Network > NAT > General

The screenshot shows a window titled "NAT Setup". At the top, there is a checked checkbox labeled "Active Network Address Translation(NAT)". Below this, there is a text input field labeled "Max NAT/Firewall Session Per User" containing the number "6000". At the bottom of the window, there are two buttons: "Apply" and "Cancel".

The following table describes the labels in this screen.

Table 26 Network > NAT > General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your IAD.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your IAD.
Max NAT/ Firewall Session Per User	<p>When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the IAD.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions.</p>
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.3 The Port Forwarding Screen

Note: This screen is available only when you select **SUA only** in the **NAT > General** screen.

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

The most often used port numbers and services are shown in [Appendix F on page 313](#). Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

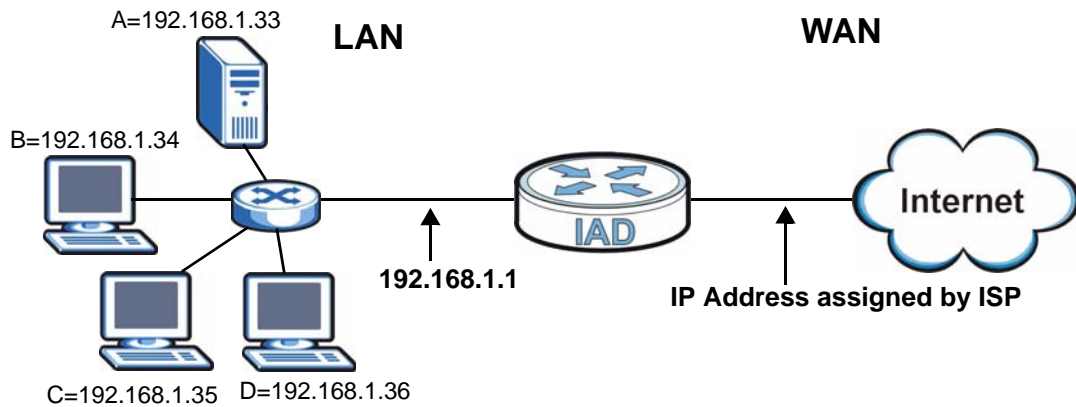
Note: If you do not assign a **Default Server** IP address, the IAD discards all packets received for ports that are not specified here or in the remote management setup.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP

addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 43 Multiple Servers Behind NAT Example



9.3.1 Configuring the Port Forwarding Screen

Click **Network > NAT > Port Forwarding** to open the following screen.

See [Appendix F on page 313](#) for port numbers commonly used for particular services.

Figure 44 Network > NAT > Port Forwarding

#	Active	Service Name	Start Port	End Port	Server IP Address	Modify
1	<input checked="" type="checkbox"/>	HTTPS	443	443	1. 2. 3. 4	

The following table describes the fields in this screen.

Table 27 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a Default Server IP address, the IAD discards all packets received for ports that are not specified here or in the remote management setup.

Table 27 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is a service's name.
Protocol	This is the transport layer protocol used for the service.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Port Translation	
Start Port	This is the first internal port number that identifies a service.
End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to return to the previous configuration.

9.3.2 The Port Forwarding Rule Edit Screen

Use this screen to edit a port forwarding rule. Select **User define** in the **Service Name** field of the **Port Forwarding** screen or click an existing rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

Figure 45 Network > NAT > Port Forwarding: Edit

The screenshot shows a 'Rule Setup' window with the following fields and values:

- Active:**
- Service Name:** www
- Start Port:** 80
- End Port:** 80
- Server IP Address:** 10.10.1.2

At the bottom of the window are three buttons: **Back**, **Apply**, and **Cancel**.

The following table describes the fields in this screen.

Table 28 Network > NAT > Port Forwarding: Edit

LABEL	DESCRIPTION
Rule Setup	
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are TCP , UDP , or ALL .
Start Port	<p>Enter the original destination port for the packets.</p> <p>To forward only one port, enter the port number again in the End Port field.</p> <p>To forward a series of ports, enter the start port number here and the end port number in the End Port field.</p>
End Port	<p>Enter the last port of the original destination port range.</p> <p>To forward only one port, enter the port number again in the Start Port field above and then enter it again in this field.</p> <p>To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above.</p>
Server IP Address	Enter the inside IP address of the server here.

Table 28 Network > NAT > Port Forwarding: Edit (continued)

LABEL	DESCRIPTION
Port Translation	Enter the port number here to which you want the IAD to translate the incoming port.
Start Port	For a range of ports, enter the first number of the range to which you want the incoming ports translated.
End Port	Enter the last port of the translated port range.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

9.4 The Address Mapping Screen

Note: The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

Ordering your rules is important because the IAD applies the rules in the order that you specify. When a rule matches the current packet, the IAD takes the corresponding action and the remaining rules are ignored.

To change your IAD's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

Figure 46 Network > NAT > Address Mapping

The screenshot shows the 'Address Mapping' tab selected in a configuration interface. Below the tab is a table titled 'Address Mapping Rules' with 10 rows and 7 columns. The columns are: #, Local Start IP, Local End IP, Global Start IP, Global End IP, Type, and Modify. Each row contains dashes for the IP and Type fields, and edit/delete icons for the Modify field.

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	-	-	-	-	-	
2	-	-	-	-	-	
3	-	-	-	-	-	
4	-	-	-	-	-	
5	-	-	-	-	-	
6	-	-	-	-	-	
7	-	-	-	-	-	
8	-	-	-	-	-	
9	-	-	-	-	-	
10	-	-	-	-	-	

The following table describes the fields in this screen.

Table 29 Network > NAT > Address Mapping

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are - for Server port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is - for One-to-one and Server mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). This field is - here if you have a dynamic IP address (0.0.0.0) from your ISP. You can only do this for Many-to-One, one-to-one and Server mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is - for One-to-one, Many-to-One and Server mapping types.
Type	<p>1-1: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p>M-1: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p>M-M Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p>MM No (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p>Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Modify	<p>Click the edit icon to go to the screen where you can edit the address mapping rule.</p> <p>Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.</p>

9.4.1 The Address Mapping Rule Edit Screen

To edit an address mapping rule, click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 47 Network > NAT > Address Mapping: Edit

The screenshot shows a web-based configuration interface titled "Edit Address Mapping Rule1". It contains several input fields and a dropdown menu. The "Type" field is a dropdown menu currently set to "One-to-One". Below it are four text input fields: "Local Start IP" (0.0.0.0), "Local End IP" (N/A), "Global Start IP" (0.0.0.0), and "Global End IP" (N/A). The "Server Mapping Set" field is a dropdown menu set to "2" with a link "Edit Details" next to it. At the bottom of the form are three buttons: "Back", "Apply", and "Cancel".

The following table describes the fields in this screen.

Table 30 Network > NAT > Address Mapping: Edit

LABEL	DESCRIPTION
Type	<p>Choose the port mapping type from one of the following.</p> <p>One-to-One: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.</p> <p>Many-to-One: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p>Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p>Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p>Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	<p>This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address.</p> <p>This field is N/A for One-to-One and Server mapping types.</p>
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.

Table 30 Network > NAT > Address Mapping: Edit (continued)

LABEL	DESCRIPTION
Server Mapping Set	Only available when Type is set to Server . Select a number from the drop-down menu to choose a port forwarding set.
Edit Details	Click this link to go to the Port Forwarding screen to edit a port forwarding set that you have selected in the Server Mapping Set field.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

9.5 The ALG Screen

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 IAD registers with the SIP register server, the SIP ALG translates the IAD'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 IAD is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the IAD. To access this screen, click **Network > NAT > ALG**.

Figure 48 Network > NAT > ALG

Each field is described in the following table.

Table 31 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click this to save your changes and to apply them to the IAD.
Reset	Click this to return to previously saved configuration.

9.6 NAT Technical Reference

This chapter contains more information regarding NAT.

9.6.1 NAT Definitions

Inside/outside denotes where a host is located relative to the IAD, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 32 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

9.6.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

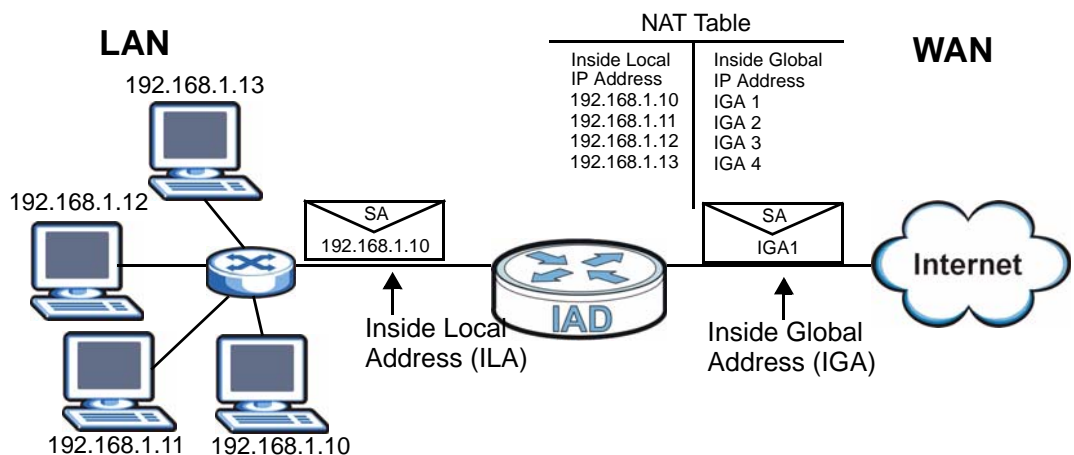
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the

outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 33 on page 115](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your IAD filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

9.6.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The IAD keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

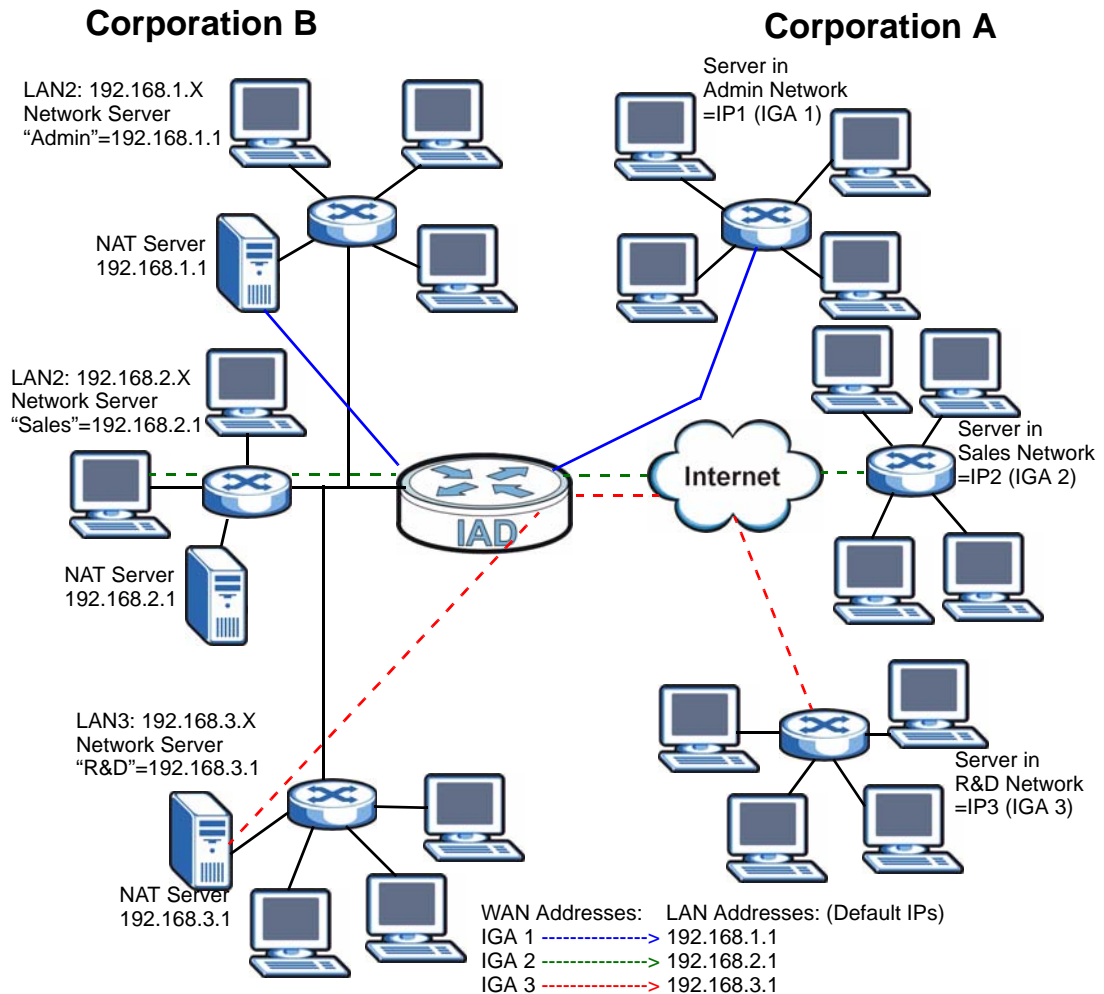
Figure 49 How NAT Works



9.6.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the IAD can communicate with three distinct WAN networks.

Figure 50 NAT Application With IP Alias



9.6.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the IAD maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the IAD maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).

- **Many to Many Overload:** In Many-to-Many Overload mode, the IAD maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the IAD maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 33 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1 ↔ IGA1
Many-to-One (SUA/PAT)	ILA1 ↔ IGA1
	ILA2 ↔ IGA1 ...
Many-to-Many Overload	ILA1 ↔ IGA1
	ILA2 ↔ IGA2
	ILA3 ↔ IGA1
	ILA4 ↔ IGA2 ...
Many-to-Many No Overload	ILA1 ↔ IGA1
	ILA2 ↔ IGA2
	ILA3 ↔ IGA3
	...
Server	Server 1 IP ↔ IGA1
	Server 2 IP ↔ IGA1
	Server 3 IP ↔ IGA1

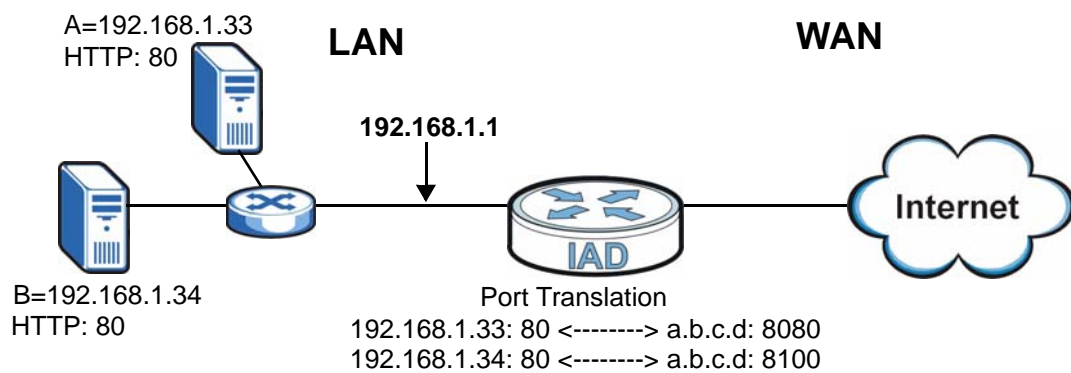
9.6.6 Port Translation

The IAD can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the local network. When you use port forwarding without port translation, a single server on the local network can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the local network can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port's IP address. The IAD translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The IAD also translates port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

Note: In this example, anyone wanting to access server A from the Internet must use port 8080. Anyone wanting to access server B from the Internet must use port 8100.

Figure 51 Port Translation Example



10.1 Introduction

This chapter provides background information on VoIP and SIP and explains how to configure your device's voice settings.

VoIP is the sending of voice signals over 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.

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.

10.1.1 What You Need to Know

The following terms and concepts may help as you read through this chapter.

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.

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.

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).

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.

10.2 SIP Service Provider

Use this screen to maintain basic information about each SIP account. Your VoIP service provider (the company that lets you make phone calls over the Internet) should provide this. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP**.

Figure 52 VoIP > SIP > SIP Service Provider

Server Profile Selection	
SIP Service Provider Name	Undefine
<input type="checkbox"/> Active	
General	
SIP Local Port	5060 (1025-65535)
SIP Server Address	ChangeMe
SIP Server Port	5060 (1025-65535)
REGISTER Server Address	ChangeMe
REGISTER Server Port	5060 (1025-65535)
SIP Service Domain	ChangeMe
Advanced	

Each field is described in the following table.

Table 34 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
Server Profile Selection	
SIP Service Provider Name	Enter your SIP service provider's name, using up to 256 printable English-keyboard characters.
Active	Select this to make use these settings for all SIP phone calls.
General	
SIP Local Port	Enter the IAD's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 32 printable English keyboard characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 32 printable English keyboard characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 32 printable English keyboard characters.
Apply	Click this to save your changes.
Cancel	Click this to exit the screen without saving any changes.
Advanced Setup	Click this to edit the advanced settings for this SIP account. The Advanced SIP Settings screen appears.

10.2.1 Advanced SIP Settings

Use this screen to maintain advanced settings for each SIP account. Click **Advanced** in **VoIP > SIP > SIP Service Provider**. The following screen displays.

Figure 53 SIP Service Provider > Advanced

Timer Setting		
Registration Period	<input type="text" value="3600"/>	(20-65535) second
Register Expires	<input type="text" value="3600"/>	(90-65535) second
Register Re-send Timer	<input type="text" value="180"/>	(1-65535) second
Session Expires	<input type="text" value="180"/>	(90-3600) second
Min-SE	<input type="text" value="90"/>	(90-1800) second
RTP Port Range		
Start Port	<input type="text" value="50000"/>	(1025-65535)
End Port	<input type="text" value="65535"/>	(1025-65535)
Dialing Interval Selection		
Dialing Interval Selection	<input type="text" value="3"/> <input type="button" value="v"/>	Second

[Basic](#)

Each field is described in the following table.

Table 35 SIP Service Provider > Advanced

LABEL	DESCRIPTION
Timer Settings	
Registration Period	Enter the number of seconds allocated for the IAD to register with a SIP service.
Register Expires	Enter the number of seconds your SIP account is registered with the SIP register server before the registration is downgraded to 'inactive' and all SIP functions for the account are blocked. The IAD automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration, which takes priority over this setting.)
Register Re-send timer	Enter the number of seconds the IAD waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the SIP server waits for a 'keep alive' signal from the IAD before disconnecting the call. The keep alive signal is periodically sent from the IAD during a call as long as the connection between it and the server remains constant. If interference happens somewhere along the line, or the connection is unexpectedly terminated, then the SIP server uses this setting as a timer to automatically disconnect the call.

Table 35 SIP Service Provider > Advanced (continued)

LABEL	DESCRIPTION
Min-SE	Enter the minimum number of seconds the IAD accepts for a session expiration time when it receives a request to start a SIP session. If the request has a shorter time, the IAD rejects it.
RTP Port Range	
Start Port End Port	<p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the Start Port and End Port fields.</p> <p>To enter a range of ports,</p> <ul style="list-style-type: none"> • enter the port number at the beginning of the range in the Start Port field • enter the port number at the end of the range in the End Port field.
Dialing Interval Selection	
Dialing Interval Selection	Select the number of seconds the IAD waits before placing a dialed call.
Apply	Click this to save your changes.
Cancel	Click this to exit the screen without saving any changes.
Basic	Click this to return to the basic SIP Settings screen without saving your changes.

10.3 SIP Account

Use this screen to set up your basic SIP account information. Click **VoIP > SIP > SIP Account** to display this screen.

Figure 54 VoIP > SIP > SIP Account

The screenshot shows the 'SIP Account Selection' screen. It has a title bar 'SIP Account Selection'. Below it, there's a label 'SIP Account Selection' and a dropdown menu showing 'SIP1'. The next section is 'General', containing a checkbox 'Active SIP Account' and a text field 'Number' with the value 'ChangeMe'. The 'Authentication' section has a 'User Name' field with 'ChangeMe' and a 'Password' field with masked characters. An 'Advanced' link is located in the bottom right corner.

Each field is described in the following table.

Table 36 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
SIP Account Selection	
SIP Account	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
General	
Active SIP Account	Select this if you want the IAD to use this account. Clear it if you do not want the IAD to use this account.
Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 50 printable English keyboard characters.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 20 printable English keyboard characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 20 printable English keyboard characters.
Apply	Click this to save your changes.
Cancel	Click this to exit the screen without saving any changes.
Advanced	Click this to edit the advanced settings for this SIP account. The Advanced SIP Account Settings screen appears.

10.3.1 Advanced Account Settings

Use this screen to maintain advanced settings for each SIP account. Click **Advanced** in **VoIP > SIP > SIP Account**. The following screen displays.

Figure 55 SIP Account > Advanced

Voice Feature

Primary Compression Type

Secondary Compression Type

Third Compression Type

Speaking Volume

Listening Volume

Active G.168 (Echo Cancellation)

Active VAD

Call Feature

Active Call Transfer

Active Call Waiting
Call Waiting Reject Timer (0-65535)Second

Active Unconditional Forward

Active Busy Forward

Active No Answer Forward
No Answer Ring Count (0-65535)second(s)

⚠ CAUTION:
If you enable [Unconditional Forward], [Busy Forward] and [No Answer] will be ignored.

Active Do Not Disturb

⚠ WARNING:
If you enable this item, you will not get indication when somebody call you.

[Basic](#)

Each field is described in the following table.

Table 37 SIP Account > Advanced

LABEL	DESCRIPTION
Voice Feature	
Primary Compression Type	<p>Select the type of voice coder/decoder (codec) that you want the IAD to use.</p> <p>G.711 provides high voice quality but requires more bandwidth (64 kbps).</p> <ul style="list-style-type: none"> • G.711A is typically used in Europe. • G.711u is typically used in North America and Japan. • G.729 operates at 8 kbps and is often the codec of choice for VoIP because of its low bandwidth requirements. <p>The IAD must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.</p>
Secondary Compression Type	Select the IAD's second choice for voice coder/decoder.
Third Compression Type	Select the IAD's third choice for voice coder/decoder.
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD	Select this if the IAD should transmit smaller packets when you are not speaking. This reduces the bandwidth used.
Call Feature	Call features are described in detail in Chapter 11 on page 129 .
Active Call Transfer	Select this to enable the call transfer feature.
Active Call Waiting	Select this to enable the call waiting feature.
Call Waiting Reject Timer	Enter the number of seconds for call waiting to stay engaged before disconnecting the caller.
Active Unconditional Forward	Select this, then enter a phone number to which incoming calls are forwarded.
Active Busy Forward	Select this, then enter a phone number to which calls are forwarded when your phone is off the hook.
Active No Answer Forward	Select this, then enter a phone number to which calls are forwarded when the phone is not answered.
No Answer Ring Count	Enter the number of rings the IAD waits before forwarding unanswered calls.
Active Do Not Disturb	Select this to enable the DND feature.
Apply	Click this to save your changes.
Cancel	Click this to exit the screen without saving any changes.
Basic	Click this to return to the basic SIP Account screen without saving your changes.

10.4 Analog Phone

Use this screen to link the IAD's analog phone ports with one or more SIP accounts to handle outgoing and incoming calls. Click **VoIP > Phone**. The following screen displays.

Figure 56 Phone > Analog Phone

Phone Port Selection

Phone Port Selection

SIP Account to Make Outgoing Call

SIP Account Association	SIP Number
<input type="text" value="SIP1"/>	ChangeMe

SIP Account(s) to Receive Incoming Call

SIP Account	SIP Number	SIP Account Status	SIP Account	SIP Number	SIP Account Status
<input checked="" type="checkbox"/> SIP1	ChangeMe	Edit	<input type="checkbox"/> SIP2	ChangeMe	Edit

Each field is described in the following table.

Table 38 Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Selection	
Phone Port Selection	Select a phone port to configure on this screen.
SIP Account to Make Outgoing Call	
SIP Account Association	Select a SIP account for all outgoing calls on this port to use.
SIP Number	Indicates the SIP number associated with this account. Click it to open the SIP Account screen, where you can enter a new number.
SIP Account(s) to Receive Incoming Calls	
SIP Account	This indicates the SIP account.
SIP Number	This indicates the SIP account's number. You can click it to open the SIP Account screen, where you can change it.
SIP Account Status	This indicates whether the account is active or not. Click it to open the SIP Account screen, where you can change the status.
Apply	Click this to save your changes.
Cancel	Click this to exit the screen without saving any changes.

10.5 Speed Dial

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. You also have to create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. To access this screen, click **VoIP > Phone Book > Speed Dial**.

Figure 57 Phone Book > Speed Dial

#	Number	Description	Modify
#01			
#02			
#03			
#04			
#05			
#06			
#07			
#08			
#09			
#10			

Each field is described in the following table.

Table 39 Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the IAD to call when you dial the speed-dial number.
Description	Enter a description for this speed dial number. You can use up to 127 alphanumeric characters.
Add	Click this to use the information in the Speed Dial section to update the Speed Dial Phone Book section.
Speed Dial Phone Book	Use this section to look at all the speed-dial entries and to erase them.

Table 39 Phone Book > Speed Dial (continued)

LABEL	DESCRIPTION
#	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the IAD calls when you dial the speed-dial number.
Destination	This field is blank, if the speed-dial entry uses one of your SIP accounts. Otherwise, this field shows the IP address or domain name of the SIP server or other party. (This field corresponds with the Type field in the Speed Dial section.)
Modify	Use this field to edit or erase the speed-dial entry. Click the Edit icon to copy the information for this speed-dial entry into the Speed Dial section, where you can change it. Click the Remove icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

Phone Usage

11.1 Overview

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

Note: Not all service providers support all features.

11.2 Dialing a Telephone Number

The **PHONE** LED turns green when your SIP account is registered. Dial a SIP number like "12345" on your phone's keypad.

Use speed dial entries (see [Section 10.5 on page 126](#)) for peer-to-peer calls or SIP numbers that use letters. Dial the speed dial entry on your telephone's keypad.

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

11.3 Using Speed Dial

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.

11.4 Using Call Park and Pickup

Do the following to put a call on hold on one phone and continue it on another (connected to the IAD). This feature may not be supported by all service providers.

- 1 During the call, press "***97#**" and then any number (up to 8 digits long). You need to remember this number in order to pick up the call on another phone. Hang up the receiver.

- 2 Pick up another phone's receiver. Press "#97#" followed by the same number you entered before to continue the call.

11.5 Checking the IAD's IP Address

Do the following to listen to the IAD's current IP 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.

11.6 Auto Provisioning and Auto Firmware Upgrade

If your service provider uses an auto-provisioning server to set up your device, you must first authenticate your IAD with the auto provisioning server, allowing you to use the service.

- On a phone connected to the device, enter "*99*", your SIP number, "*", then "#".
- For example, if your SIP number is 0123456, you would enter "*99*0123456#".

During auto-provisioning, the IAD checks to see if there is a newer firmware version (if your service provider activates this feature). If newer firmware is available, the IAD plays a recording when you pick up your phone's handset.

- Press "*99#" to upgrade the IAD's firmware.
- Press "#99#" to not upgrade the IAD's firmware.

11.7 Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The IAD supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb

Note: To take full advantage of the supplementary phone services available through the IAD's phone port, you may need to subscribe to the services from your VoIP service provider.

11.7.1 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 IAD.

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

11.7.2 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 40 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.

11.7.2.1 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.

11.7.2.2 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”.

11.7.2.3 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.

11.7.2.4 European Three-Way Conference

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

- 1 When you are on the phone talking to someone, press 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”.

11.7.3 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 41 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.

11.7.3.1 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.

11.7.3.2 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.

11.7.3.3 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.

11.7.3.4 USA Three-Way Conference

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

- 1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call (to party B).
- 3 When party B answers the second call, press the flash key 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 (with party A on-line and party B on hold), press the flash key.
- 6 If you want to go back to the three-way conversation, press the flash key again.
- 7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

11.8 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

Table 42 Phone Functions Summary

ACTI ON	FUNCTION	DESCRIPTION
*99#	Enable firmware update	Use these to upload or not upload new firmware to the IAD, if requested by your service provider. See Section 11.6 on page 130 .
#99#	Disable firmware update	
*98#	Call transfer	Transfer a call to another phone. See Section 11.7.2 on page 131 (Europe type) and Section 11.7.3 on page 133 (USA type).
*97#	Call park	Use these to place a call on hold on one phone and then continue it on another (if supported by your service provider). See Chapter 23 on page 231 .
#97#	Call pickup	
*66#	Call return	Place a call to the last person who called you. See Chapter 23 on page 231 .
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off. Chapter 23 on page 231
#95#	Disable Do Not Disturb	

Table 42 Phone Functions Summary

ACTI ON	FUNCTION	DESCRIPTION
*41#	Enable call waiting	Use these to allow you to put a call on hold while answering another, or to turn this function off. See Section 11.7.2 on page 131 (Europe type) and Section 11.7.3 on page 133 (USA type).
#41#	Disable call waiting	
*21#	Enable call forward	Use these to allow you to use the call forwarding tables you set in the IAD, or to turn this function off.
#21#	Disable call forward	
22	Uncondition forward	Forward all incoming calls.
23	No answer forward	Forward incoming calls if you do not answer.
24	Busy forward	Forward calls if you are already making a call.

Firewalls

12.1 Overview

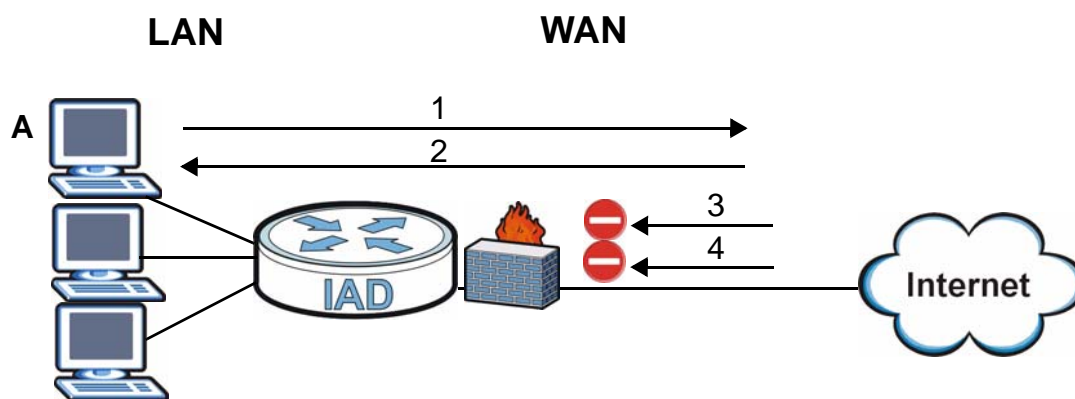
Use these screens to enable and configure the firewall that protects your IAD and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 58 Default Firewall Action



- See [Section 12.1.3 on page 140](#) for an example of setting up a firewall.
- See [Section 12.5 on page 154](#) for advanced technical information on firewall.

12.1.1 What You Can Do in this Chapter

- Use the **General** screen ([Section 12.2 on page 143](#)) to enable firewall and/or triangle route on the IAD, and set the default action that the firewall takes on packets that do not match any of the firewall rules.
- Use the **Rules** screen ([Section 12.3 on page 145](#)) to view the configured firewall rules and add, edit or remove a firewall rule.
- Use the **Threshold** screen ([Section 12.4 on page 151](#)) to set the thresholds that the IAD uses to determine when to start dropping sessions that do not become fully established (half-open sessions).

12.1.2 What You Need to Know

Firewall

The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It is generally a mechanism used to protect a trusted network from an untrusted network.

The IAD firewall is a stateful inspection firewall and restricts access by screening data packets against defined access rules. The IAD physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks. The IAD protects against Denial of Service (DoS) attacks, prevents theft, destruction and modification of data, and logs events.

Firewall Rules

Your customized rules take precedence and override the IAD's default settings. The IAD checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the IAD takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ Router
- LAN to WAN
- WAN to LAN
- WAN to WAN/ Router

Note: The LAN includes both the LAN port and the WLAN.

By default, the IAD's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router

These rules specify which computers on the LAN can manage the IAD (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

Note: You can also configure the remote management settings to allow only a specific computer to manage the IAD.

- LAN to WAN

These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the IAD's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN

These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to WAN/ Router

By default the IAD stops computers on the WAN from managing the IAD or using the IAD as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the IAD.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the IAD.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

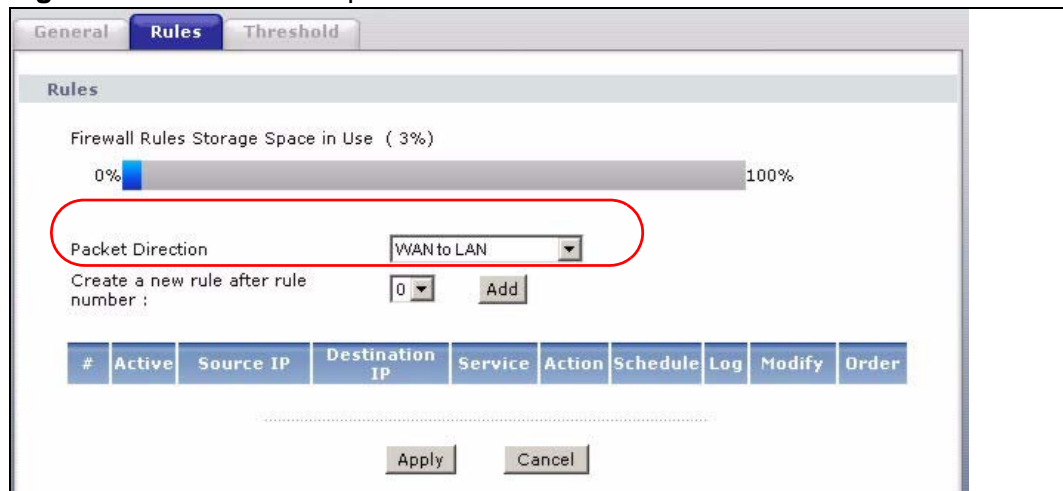
These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the IAD's default rules.

12.1.3 Firewall Rule Setup Example

The following Internet firewall rule example allows a “Doom” connection from the Internet.

- 1 Click **Security > Firewall > Rules**.
- 2 Select **WAN to LAN** in the **Packet Direction** field.
- 3 Select the index number after that you want to add the rule. For example, if you select “6”, your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
- 4 Click **Add** to display the firewall rule configuration screen.

Figure 59 Firewall Example: Rules



- 5 In the **Edit Rule** screen, click the **Edit Customized Services** link to open the **Customized Service** screen.

- Click an index number to display the **Customized Services Config** screen and configure the screen as follows and click **Apply**.

Figure 60 Edit Custom Port Example

The screenshot shows a web interface for configuring a service. It is divided into two main sections: 'Config' and 'Port Configuration'.
 In the 'Config' section, there is a text input field for 'Service Name' containing 'MyService' and a dropdown menu for 'Service Type' set to 'TCP/UDP'.
 In the 'Port Configuration' section, there are two radio buttons: 'Single' (which is selected) and 'Port Range'. Below them, there are two text input fields for 'Port Number', both containing '123', with 'From' and 'To' labels.
 At the bottom of the form, there are four buttons: 'Back', 'Apply', 'Cancel', and 'Delete'.

- Select **Any** in the **Destination Address List** box and then click **Delete**.
- Configure the destination address screen as follows and click **Add**.

Figure 61 Firewall Example: Edit Rule: Destination Address

The screenshot shows a web interface for editing a firewall rule. It is titled 'Edit Rule 2'.
 At the top, there is a checked checkbox for 'Active' and a dropdown menu for 'Action for Matched Packets' set to 'Permit'.
 The 'Source Address' section has a dropdown menu for 'Address Type' set to 'Any Address'. Below it are four text input fields: 'Start IP Address' (0.0.0.0), 'End IP Address' (0.0.0.0), and 'Subnet Mask' (0.0.0.0). To the right of these fields are three buttons: 'Add >>', 'Edit <<', and 'Delete'. To the right of these buttons is a list box containing 'Any'.
 The 'Destination Address' section has a dropdown menu for 'Address Type' set to 'Range Address'. Below it are four text input fields: 'Start IP Address' (10.0.0.10), 'End IP Address' (10.0.0.15), and 'Subnet Mask' (0.0.0.0). To the right of these fields are three buttons: 'Add >>', 'Edit <<', and 'Delete'. To the right of these buttons is a list box containing '10.0.0.10 - 10.0.0.15'.

- Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.

Note: Custom services show up with an “*” before their names in the **Services** list box and the **Rules** list box.

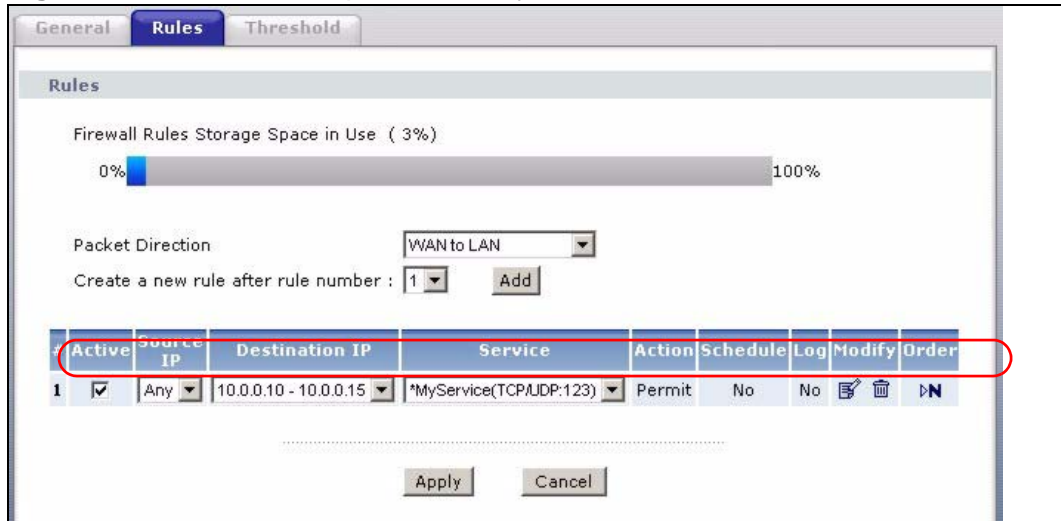
Figure 62 Firewall Example: Edit Rule: Select Customized Services

The screenshot shows the 'Edit Rule 2' configuration window. The 'Service' section is highlighted with a red circle, showing the 'Available Services' list with 'MyService(TCP:UDP:123)' selected in the 'Selected Services' list. The 'Schedule' section is also visible, showing 'Day to Apply' set to 'Everyday' and 'Time of Day to Apply' set to 'All day'. The 'Apply' button is circled in red.

On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.

Rule 1 allows a “Doom” connection from the WAN to IP addresses 10.1.1.10 through 10.1.1.15 on the LAN.

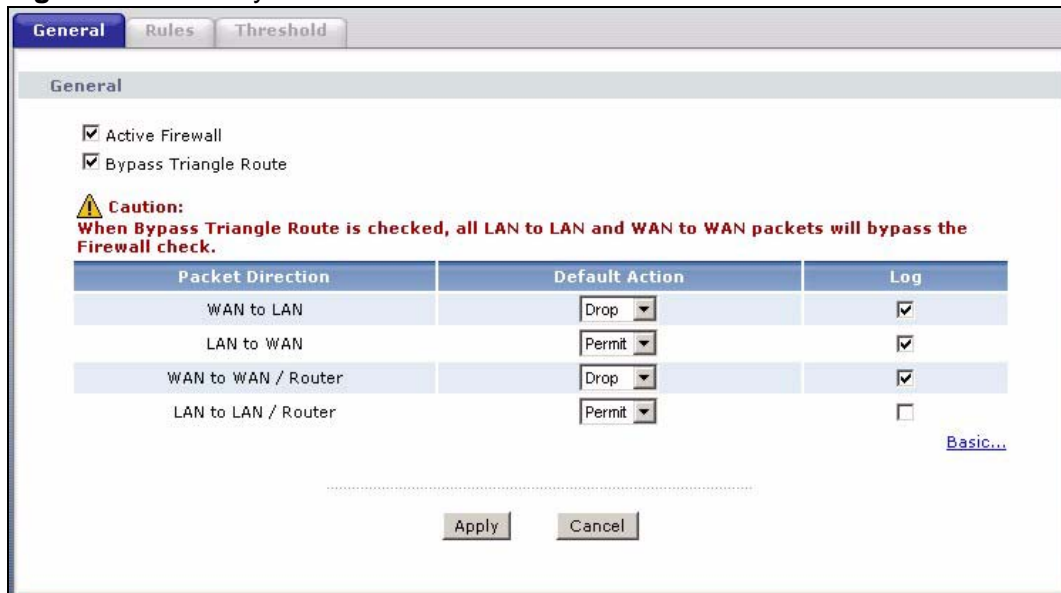
Figure 63 Firewall Example: Rules: MyService



12.2 The Firewall General Screen

Click **Security > Firewall** to display the following screen. Activate the firewall by selecting the **Active Firewall** check box as seen in the following screen.

Figure 64 Security > Firewall > General



The following table describes the labels in this screen.

Table 43 Security > Firewall > General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The IAD performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	<p>If an alternate gateway on the LAN has an IP address in the same subnet as the IAD's LAN IP address, return traffic may not go through the IAD. This is called an asymmetrical or "triangle" route. This causes the IAD to reset the connection, as the connection has not been acknowledged.</p> <p>Select this check box to have the IAD permit the use of asymmetrical route topology on the network (not reset the connection).</p> <p>Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the IAD. A better solution is to use IP alias to put the IAD and the backup gateway on separate subnets. See Section 12.5.3.1 on page 155 for an example.</p>
Packet Direction	<p>This is the direction of travel of packets (LAN to LAN / Router, LAN to WAN, WAN to WAN / Router, WAN to LAN).</p> <p>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, LAN to LAN / Router means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the IAD or the IAD itself.</p>
Default Action	<p>Use the drop-down list boxes to select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules.</p> <p>Select Drop to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select Reject to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select Permit to allow the passage of the packets.</p>
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

12.3 The Firewall Rules Screen

Note: The ordering of your rules is very important as rules are applied in turn.

Refer to [Section 12.5 on page 154](#) for more information.

Click **Security > Firewall > Rules** to bring up the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

Figure 65 Security > Firewall > Rules

The following table describes the labels in this screen.

Table 44 Security > Firewall > Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the IAD's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click Add to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the General screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.

Table 44 Security > Firewall > Rules (continued)

LABEL	DESCRIPTION
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Service	This drop-down list box displays the services to which this firewall rule applies. See Appendix F on page 313 for more information.
Action	This field displays whether the firewall silently discards packets (Drop), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (Reject) or allows the passage of packets (Permit).
Schedule	This field tells you whether a schedule is specified (Yes) or not (No).
Log	This field shows you whether a log is created when packets match this rule (Yes) or not (No).
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the Move the rule to field. Type a number in the Move the rule to field and click the Move button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

12.3.1 Configuring Firewall Rules

Refer to [Section 12.1.2 on page 138](#) for more information.

In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 66 Security > Firewall > Rules: Edit

Edit Rule 2

Active
Action for Matched Packets: Permit

Source Address

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Source Address List

Any

Add >>
Edit <<
Delete

Destination Address

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Destination Address List

Any

Add >>
Edit <<
Delete

Service

Available Services

Any(All)
 Any(ICMP)
 AIMNEW-ICQ(TCP:5190)
 AUTH(TCP:113)
 BGP(TCP:179)

[Edit Customized Services](#)

Selected Services

Any(UDP)
 Any(TCP)

Add >>
Remove

Schedule

Day to Apply

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Apply : (24-Hour Format)

All day

Start hour minute End hour minute

Log

Log Packet Detail Information.

Alert

Send Alert Message to Administrator When Matched.

Back
Apply
Cancel

The following table describes the labels in this screen.

Table 45 Security > Firewall > Rules: Edit

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select whether to discard (Drop), deny and send an ICMP destination-unreachable message to the sender of (Reject) or allow the passage of (Permit) packets that match this rule.
Source/ Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: Single Address , Range Address , Subnet Address and Any Address .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click Add >> to add a new address to the Source or Destination Address box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click Edit << .
Delete	Highlight an existing source or destination address from the Source or Destination Address box above and click Delete to remove it.
Services	
Available/ Selected Services	Please see Appendix F on page 313 for more information on services available. Highlight a service from the Available Services box on the left, then click Add >> to add it to the Selected Services box on the right. To remove a service, highlight it in the Selected Services box on the right, then click Remove . Custom services are prefixed with an asterisk.
Edit Customized Service	Click the Edit Customized Services link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select All Day or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the Log Settings page and select the Access Control logs category to have the IAD record these logs.
Alert	

Table 45 Security > Firewall > Rules: Edit (continued)

LABEL	DESCRIPTION
Send Alert Message to Administrator When Matched	Select the check box to have the IAD generate an alert when the rule is matched.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

12.3.2 Customized Services

Configure customized services and port numbers not predefined by the IAD. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix F on page 313](#) for some examples. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Figure 67 Security > Firewall > Rules: Edit: Edit Customized Services

No.	Name	Protocol	Port
1			
2			
3			
4			
5			
6			
7			
8			
9			

Back

The following table describes the labels in this screen.

Table 46 Security > Firewall > Rules: Edit: Edit Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the Firewall Customized Services Config screen to configure or edit a customized service.
Name	This is the name of your customized service.

Table 46 Security > Firewall > Rules: Edit: Edit Customized Services

LABEL	DESCRIPTION
Protocol	This shows the IP protocol (TCP , UDP or TCP/UDP) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click Back to return to the Firewall Edit Rule screen.

12.3.3 Configuring A Customized Service

Click a rule number in the **Firewall Customized Services** screen to create a new custom port or edit an existing one. This action displays the following screen.

Figure 68 Security > Firewall > Rules: Edit: Edit Customized Services: Config

The following table describes the labels in this screen.

Table 47 Security > Firewall > Rules: Edit: Edit Customized Services: Config

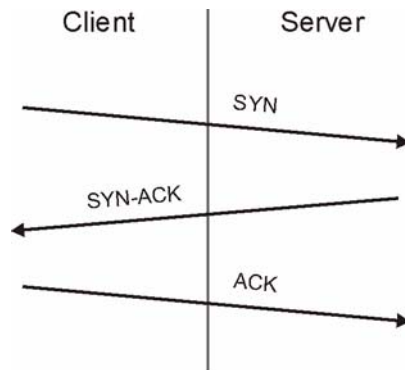
LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (TCP , UDP or TCP/UDP) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click Single to specify one port only or Range to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.
Delete	Click Delete to delete the current rule.

12.4 The Firewall Threshold Screen

For DoS attacks, the IAD uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state—the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 69 Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

12.4.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the IAD has been receiving DoS attacks that are not recorded in the logs or the logs show that the IAD is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

- 1 The maximum number of opened sessions.
- 2 The minimum capacity of server backlog in your LAN network.
- 3 The CPU power of servers in your LAN network.
- 4 Network bandwidth.

5 Type of traffic for certain servers.

Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

- If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the IAD may classify them as DoS attacks.

12.4.2 Configuring Firewall Thresholds

The IAD also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall > Threshold** to bring up the next screen.

Figure 70 Security > Firewall > Threshold

The following table describes the labels in this screen.

Table 48 Security > Firewall > Threshold

LABEL	DESCRIPTION
Denial of Service Thresholds	The IAD measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The IAD continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.

Table 48 Security > Firewall > Threshold (continued)

LABEL	DESCRIPTION
One Minute High	<p>This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the IAD deletes half-open sessions as required to accommodate new connection attempts.</p> <p>For example, if you set the one minute high to 100, the IAD starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.</p>
Maximum Incomplete Low	<p>This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The IAD continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.</p>
Maximum Incomplete High	<p>This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the IAD deletes half-open sessions as required to accommodate new connection requests. Do not set Maximum Incomplete High to lower than the current Maximum Incomplete Low number.</p> <p>For example, if you set the maximum incomplete high to 100, the IAD starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.</p>
TCP Maximum Incomplete	<p>An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.</p> <p>Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The IAD sends alerts whenever the TCP Maximum Incomplete is exceeded.</p>
Action taken when TCP Maximum Incomplete reached threshold	<p>Select the action that IAD should take when the TCP maximum incomplete threshold is reached. You can have the IAD either:</p> <p>Delete the oldest half open session when a new connection request comes.</p> <p>or</p> <p>Deny new connection requests for the number of minutes that you specify (between 1 and 255).</p>
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

12.5 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

12.5.1 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via web configurator.
- 2 Think about access control before you connect to the network in any way.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

12.5.2 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the IAD and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

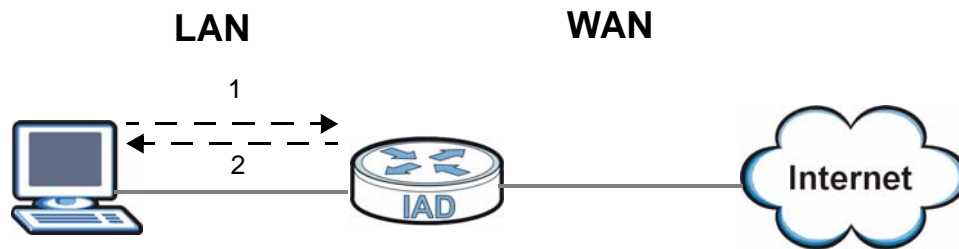
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

12.5.3 Triangle Route

When the firewall is on, your IAD acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the IAD to protect your LAN against attacks.

Figure 71 Ideal Firewall Setup



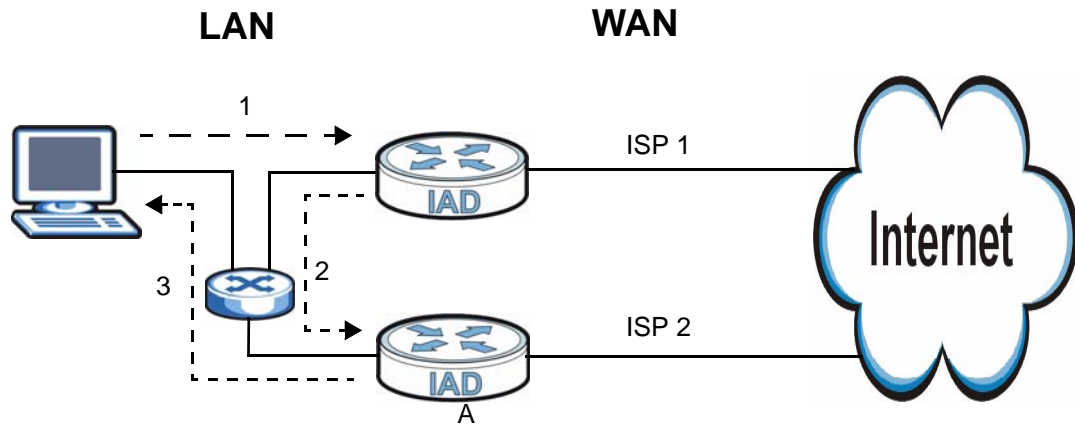
12.5.3.1 The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the IAD’s LAN IP address), the “triangle route” (also called asymmetrical route) problem may occur. The steps below describe the “triangle route” problem.

- 1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2 The IAD reroutes the SYN packet through Gateway **A** on the LAN to the WAN.
- 3 The reply from the WAN goes directly to the computer on the LAN without going through the IAD.

As a result, the IAD resets the connection, as the connection has not been acknowledged.

Figure 72 “Triangle Route” Problem



12.5.3.2 Solving the “Triangle Route” Problem

If you have the IAD allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the IAD and its firewall protection.

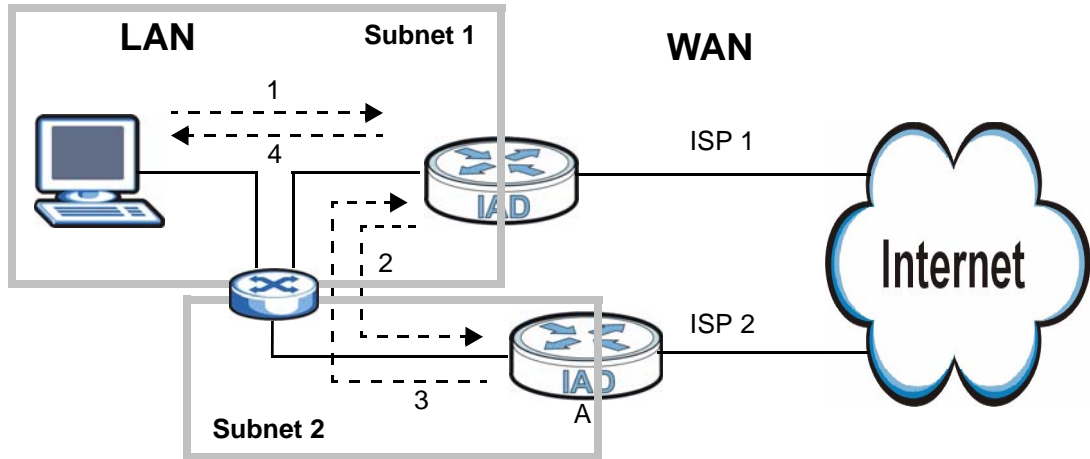
Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your IAD supports up to three logical LAN interfaces with the IAD being the gateway for each logical network.

It's like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the IAD to your LAN. The following steps describe such a scenario.

- 1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The IAD reroutes the packet to Gateway A, which is in Subnet 2.
- 3 The reply from the WAN goes to the IAD.

- The IAD then sends it to the computer on the LAN in Subnet 1.

Figure 73 IP Alias



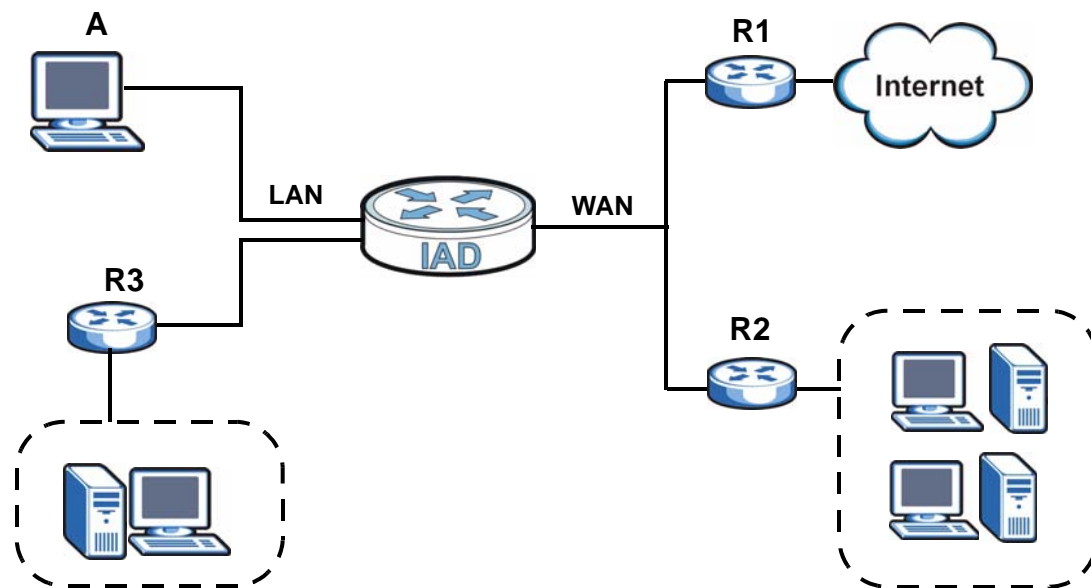
Static Route

13.1 Overview

The IAD usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the IAD send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the IAD's LAN interface. The IAD routes most traffic from **A** to the Internet through the IAD's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 74 Example of Static Routing Topology



13.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the IAD ([Section 13.2 on page 160](#)).

13.2 The Static Route Screen

Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 75 Static Route

Static Route						
Static Route Rules						
#	Active	Name	Destination	Netmask	Gateway	Modify
1	-	-	-	-	-	
2	-	-	-	-	-	
3	-	-	-	-	-	
4	-	-	-	-	-	
5	-	-	-	-	-	
6	-	-	-	-	-	
7	-	-	-	-	-	
8	-	-	-	-	-	
9	-	-	-	-	-	
10	-	-	-	-	-	
11	-	-	-	-	-	
12	-	-	-	-	-	
13	-	-	-	-	-	
14	-	-	-	-	-	
15	-	-	-	-	-	
16	-	-	-	-	-	

The following table describes the labels in this screen.

Table 49 Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the IAD. Click the Remove icon to remove a static route from the IAD. A window displays asking you to confirm that you want to delete the route.
Apply	Click this to apply your changes to the IAD.
Cancel	Click this to return to the previously saved configuration.

13.2.1 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 76 Static Route Edit

The following table describes the labels in this screen.

Table 50 Static Route Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

Quality of Service (QoS)

14.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the IAD to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Assign priority and define actions to be performed for a classified traffic flow.

The IAD assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

14.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth ([Section 14.2 on page 164](#)).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers ([Section 14.3 on page 166](#)).
- The **Monitor** screen lets you view the IAD's QoS-related packet statistics ([Section 14.4 on page 175](#)).

14.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

14.2 The QoS General Screen

Click **Advanced** > **QoS** to open the screen as shown next.

Use this screen to enable or disable QoS, and select to have the IAD automatically assign priority to traffic according to the IEEE 802.1p priority level, IP precedence and/or packet length. See [Section 14.1 on page 163](#) for more information.

Figure 77 QoS > General

The screenshot shows a configuration window with three tabs: 'General', 'Class Setup', and 'Monitor'. The 'General' tab is active. Under the 'General' heading, there is a checked checkbox for 'Active QoS'. Below it, 'WAN Managed Bandwidth' is set to '1000' in a text box, followed by '(kbps)'. A section titled 'Traffic priority will be automatically assigned by' contains three items: '1. Ethernet Priority' with a dropdown menu set to 'OFF', '2. IP Precedence' with a dropdown menu set to 'OFF', and '3. Packet Length' with a dropdown menu set to 'OFF'. At the bottom of the window are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 51 QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the IAD forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interface's actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. You can also set this number lower than the interface's actual transmission speed. This will cause the IAD to not use some of the interface's available bandwidth.

Table 51 QoS > General

LABEL	DESCRIPTION
Traffic priority will be automatically assigned by	<p>These fields are ignored if traffic matches a class you configured in the Class Setup screen.</p> <p>If you select ON and traffic does not match a class configured in the Class Setup screen, the IAD assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and/or packet length. See Section 14.5.4 on page 177 for more information.</p> <p>If you select OFF, traffic which does not match a class is mapped to queue two.</p>
Apply	Click Apply to save your settings back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

14.3 The Class Setup Screen

Use this screen to add, edit or delete classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Click **Advanced** > **QoS** > **Class Setup** to open the following screen.

Figure 78 QoS > Class Setup

Order	Active	Name:	Interface	Priority	Filter Content	Modify
1	<input checked="" type="checkbox"/>	sip1	From LAN	7	Destination Address: 193.213.120.0/27	
2	<input checked="" type="checkbox"/>	sip2	From LAN	7	Destination Address: 146.172.161.24/28	
3	<input checked="" type="checkbox"/>	sip3	From LAN	7	Destination Address: 148.122.48.128/26	
4	<input checked="" type="checkbox"/>	sip4	From LAN	7	Destination Address: 148.122.250.0/24	

The following table describes the labels in this screen.

Table 52 QoS > Class Setup

LABEL	DESCRIPTION
Create a new Class	Click Add to create a new classifier.
Order	This is the number of each classifier. The ordering of the classifiers is important as the classifiers are applied in turn.
Active	Select the check box to enable this classifier.
Name	This is the name of the classifier.
Interface	This shows the interface from which traffic of this classifier should come.
Priority	This is the priority assigned to traffic of this classifier.
Filter Content	This shows criteria specified in this classifier.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

14.3.1 Class Configuration

Click the **Add** button or the **Edit** icon in the **Modify** field to configure a classifier.

Figure 79 QoS Class Configuration

Class Configuration

Active

Name:

Interface:

Priority:

Routing Policy:

- WAN Index:

- Gateway Address:

Order:

Tag Configuration

DSCP Value: (0~63)

802.1Q Tag:

- Ethernet Priority:

- VLAN ID: (2~4094)

Filter Configuration

Source:

Address: Subnet Netmask: Exclude

Port: ~ Exclude

MAC: MAC Mask: Exclude

Destination

Address: Subnet Netmask: Exclude

Port: ~ Exclude

MAC: MAC Mask: Exclude

Others

Service:

Protocol: Exclude

Packet Length: ~ Exclude

DSCP: (0~63) Exclude

Ethernet Priority: Exclude

VLAN ID: (2~4094) Exclude

Physical Port: Exclude

TCP ACK

See [Appendix F on page 313](#) for a list of commonly-used services. The following table describes the labels in this screen.

Table 53 QoS Class Configuration

LABEL	DESCRIPTION
Class Configuration	
Active	Select the check box to enable this classifier.
Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Interface	Select from which interface traffic of this class should come.
Priority	Select a priority level (between 0 and 7) or select Auto to have the IAD map the matched traffic to a queue according to the internal QoS mapping table. See Section 14.5.4 on page 177 for more information. "0" is the lowest priority level and "7" is the highest.
Routing Policy	Select the next hop to which traffic of this class should be forwarded. Select By Routing Table to have the IAD use the routing table to find a next hop and forward the matched packets automatically. Select To Gateway Address to route the matched packets to the router or switch you specified in the Gateway Address field.
WAN Index	This field is not configurable at the time of writing.
Gateway Address	Enter the IP address of the gateway, which should be a router or switch on the same segment as the IAD's interface(s), that can forward the packet to the destination.
Order	This shows the ordering number of this classifier. Select an existing number for where you want to put this classifier and click Apply to move the classifier to the number you selected. For example, if you select 2, the classifier you are moving becomes number 2 and the previous classifier 2 gets pushed down one.
Tag Configuration	
DSCP Value	Select Same to keep the DSCP fields in the packets. Select Auto to map the DSCP value to 802.1 priority level automatically. Select Mark to set the DSCP field with the value you configure in the field provided.
802.1Q Tag	Select Same to keep the priority setting and VLAN ID of the frames. Select Auto to map the 802.1 priority level to the DSCP value automatically. Select Remove to delete the priority queue tag and VLAN ID of the frames. Select Mark to replace the 802.1 priority field and VLAN ID with the value you set in the fields below. Select Add to treat all matched traffic untagged and add a second priority queue tag and VLAN.

Table 53 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Ethernet Priority	Select a priority level (between 0 and 7) from the drop down list box.
VLAN ID	Specify a VLAN ID number between 2 and 4094.
Filter Configuration	Use the following fields to configure the criteria for traffic classification.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the source. 0 means any source port number. See Appendix F on page 313 for some common services and port numbers.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the destination IP address in dotted decimal notation.
Subnet Netmask	Enter the destination subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the destination. 0 means any source port number. See Appendix F on page 313 for some common services and port numbers.
MAC	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified destination MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 53 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Service	<p>This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.</p> <p>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select the check box and select VoIP(SIP) from the drop-down list box to configure this classifier for traffic that uses SIP.</p> <p>File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select the check box and select FTP from the drop-down list box to configure this classifier for FTP traffic.</p>
Protocol	Select this option and select the protocol (TCP or UDP) or select User defined and enter the protocol (service type) number. 0 means any protocol number.
Packet Length	Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Ethernet Priority	<p>Select this option and select a priority level (between 0 and 7) from the drop down list box.</p> <p>"0" is the lowest priority level and "7" is the highest.</p>
VLAN ID	Select this option and specify a VLAN ID number between 2 and 4094.
Physical Port	Select this option and select a LAN port.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
TCP ACK	Select this option to set this classifier for TCP ACK (acknowledgement) packets.
Back	Click Back to go to the previous screen.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

14.3.2 QoS Example

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (10.1.1.23 for example) is mapped to queue 5. Traffic that does not match these

two classes are assigned priority queue based on the internal QoS mapping table on the IAD.

Figure 80 QoS Example

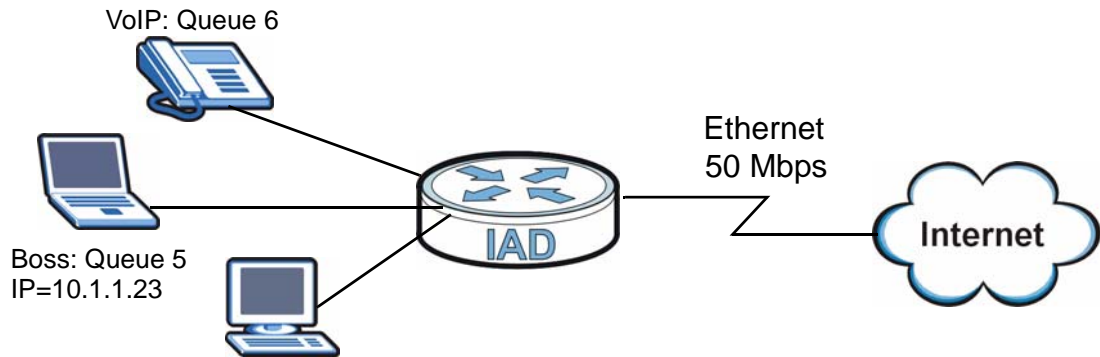


Figure 81 QoS Class Example: VoIP

Configuration-changes to the QoS can take up to 30 seconds, please do not power-off or reboot the device during this period.

Class Configuration

Active
 Name: Ex_VoIP
 Interface: From LAN
 Priority: 6
 Routing Policy: By Routing Table
 - WAN Index: 1
 - Gateway Address: 0.0.0.0
 Order: 1

Tag Configuration

Address: 0.0.0.0 Subnet Netmask: 0.0.0.0 Exclude
 Port: 0 ~ 0 Exclude
 MAC: 00:00:00:00:00:00 MAC Mask: 00:00:00:00:00:00 Exclude

Others

Service: VoIP(SIP)
 Protocol: TCP Exclude
 Packet Length: 0 ~ 0 Exclude
 DSCP: 0 (0~63) Exclude
 Ethernet Priority: 0-BE Exclude
 VLAN ID: 2 (2~4094) Exclude
 Physical Port: 1 Exclude
 TCP ACK

Figure 82 QoS Class Example: Boss

Configuration-changes to the QoS can take up to 30 seconds, please do not power-off or reboot the device during this period.

Class Configuration

Active

Name:

Interface:

Priority:

Routing Policy:

- WAN Index:

- Gateway Address:

Order:

Tag Configuration

Filter Configuration

Source:

Address Subnet Netmask Exclude

Port ~ Exclude

MAC MAC Mask Exclude

Destination

Address Subnet Netmask Exclude

Port ~ Exclude

MAC MAC Mask Exclude

Others

Service

Protocol Exclude

Packet Length ~ Exclude

DSCP (0~63) Exclude

Ethernet Priority Exclude

VLAN ID (2~4094) Exclude

Physical Port Exclude

TCP ACK

14.4 The QoS Monitor Screen

To view the IAD's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.

Figure 83 QoS Monitor

Priority Queue	Pass	Drop
0	0 bps	0 bps
1	0 bps	0 bps
2	512 bps	0 bps
3	0 bps	0 bps
4	0 bps	0 bps
5	0 bps	0 bps
6	0 bps	0 bps
7	0 bps	0 bps

At the bottom of the screen, there is a control area with the following elements:

- Label: Poll Interval(s) :
- Input field:
- Unit: sec
- Button: Set Interval
- Button: Stop

The following table describes the labels in this screen.

Table 54 QoS Monitor

LABEL	DESCRIPTION
Priority Queue	This shows the priority queue number. Traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.
Pass	This shows how many packets mapped to this priority queue are transmitted successfully.
Drop	This shows how many packets mapped to this priority queue are dropped.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval(s) field.
Stop	Click Stop to stop refreshing statistics.

14.5 Technical Reference

The following section contains additional technical information about the IAD features described in this chapter.

14.5.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 55 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

14.5.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

14.5.3 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) 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.

14.5.3.1 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.



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 kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

14.5.4 Automatic Priority Queue Assignment

If you enable QoS on the IAD, the IAD can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the IAD. On the IAD, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 56 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			

Table 56 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Dynamic DNS Setup

15.1 Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

15.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen ([Section 15.2 on page 180](#)) to enable DDNS and configure the DDNS settings on the IAD.

15.1.2 What You Need To Know

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

15.2 The Dynamic DNS Screen

To change your IAD's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

See [Section 15.1 on page 179](#) for more information.

Figure 84 Dynamic DNS

The following table describes the fields in this screen.

Table 57 Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your IAD by your Dynamic DNS provider.
User Name	Type your user name.
Password	Type the password assigned to you.
Email Address	If you select WWW.No-IP.com or WWW.TZO.com in the Service Provider field, enter the user name you used to register for this service.

Table 57 Dynamic DNS (continued)

LABEL	DESCRIPTION
Key	If you select WWW.TZO.com in the Service Provider field, enter the password you used to register for this service.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when CustomDNS is selected in the DDNS Type field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name to the WAN IP address.
Dynamic DNS server auto detect IP Address	<p>Select this option only when there are one or more NAT routers between the IAD and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.</p> <p>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the IAD and the DDNS server.</p>
Use specified IP Address	Type the IP address of the host name. Use this if you have a static IP address.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

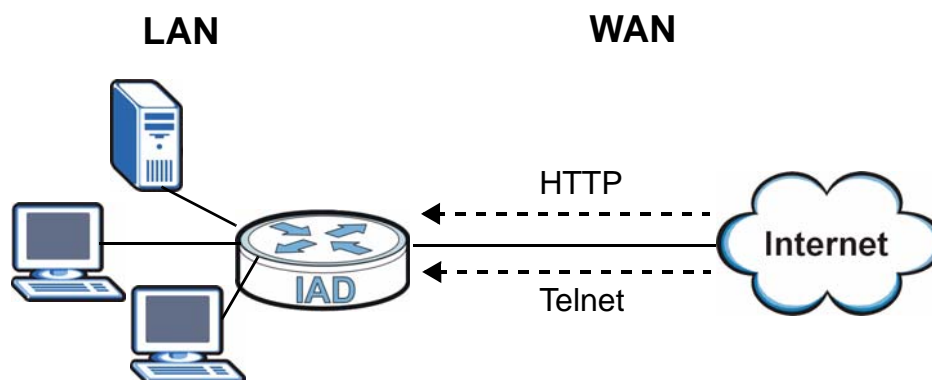
Remote Management

16.1 Overview

Remote management allows you to determine which services/protocols can access which IAD interface (if any) from which computers.

The following figure shows remote management of the IAD coming in from the WAN.

Figure 85 Remote Management From the WAN



Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your IAD from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

Note: When you choose **WAN** only or **LAN & WAN**, you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

You may only have one remote management session running at a time. The IAD automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. **The priorities for the different types of remote management sessions are as follows.**

- 1 SSH
- 2 Telnet
- 3 HTTP

16.1.1 What You Can Do in this Chapter

- Use the **WWW** screen (Section 16.2 on page 185) to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the IAD.
- Use the **Telnet** screen (Section 16.3 on page 186) to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the IAD.
- Use the **FTP** screen (Section 16.4 on page 187) to configure through which interface(s) and from which IP address(es) users can use FTP to access the IAD.
- ~~Use the **SNMP** screen (Section 16.5.3 on page 190) to configure your IAD's settings for Simple Network Management Protocol management.~~
- ~~Use the **DNS** screen (Section 16.6 on page 191) to configure through which interface(s) and from which IP address(es) users can send DNS queries to the IAD.~~
- Use the **ICMP** screen (Section 16.7 on page 192) to set whether or not your IAD will respond to pings and probes for services that you have not made available.
- Use the **SSH** screen (Section 16.11 on page 195) to change your IAD's Secure Shell settings.
- Use the **TR-069** screen

16.1.2 What You Need to Know

Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the IAD will disconnect the session immediately.

- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

- Use the IAD's WAN IP address when configuring from the WAN.
- Use the IAD's LAN IP address when configuring from the LAN.

System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The IAD automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

16.2 The HTTP Screen

To change your IAD's World Wide Web settings, click **Advanced > Remote MGMT** to display the **WWW** screen.

Figure 86 Remote Management > HTTP



The following table describes the labels in this screen.

Table 58 Remote Management > WWW

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the IAD using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the IAD using this service. Select All to allow any computer to access the IAD using this service. Choose Selected to just allow the computer with the IP address that you specify to access the IAD using this service.
Apply	Click Apply to save your settings back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

16.3 The Telnet Screen

You can use Telnet to access the IAD's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Advanced** > **Remote MGMT** > **Telnet** to display the screen as shown.

Figure 87 Remote Management > Telnet

The screenshot shows the 'Telnet' configuration window. At the top, the title 'Telnet' is displayed. Below the title, there are two configuration options:

- Access Status:** A dropdown menu is set to 'LAN & WAN'.
- Secured Client IP:** Two radio buttons are present: 'All' (selected) and 'Selected'. To the right of the 'Selected' radio button is a text input field.

The following table describes the labels in this screen.

Table 59 Remote Management > Telnet

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the IAD using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the IAD using this service. Select All to allow any computer to access the IAD using this service. Choose Selected to just allow the computer with the IP address that you specify to access the IAD using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.4 The FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the IAD's firmware and configuration files, please see the User's Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your IAD's FTP settings, click **Advanced > Remote MGMT > FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

Figure 88 Remote Management > FTP

The screenshot shows the 'FTP' configuration screen. At the top, there is a title bar labeled 'FTP'. Below it, there are two main sections:

- Access Status:** A dropdown menu is set to 'LAN & WAN'.
- Secured Client IP:** There are two radio buttons: 'All' (which is selected) and 'Selected'. To the right of the 'Selected' radio button is a text input field.

The following table describes the labels in this screen.

Table 60 Remote Management > FTP

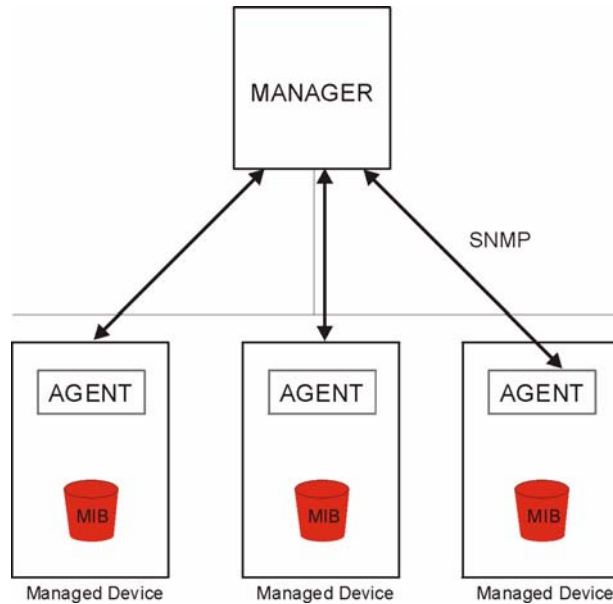
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the IAD using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the IAD using this service. Select All to allow any computer to access the IAD using this service. Choose Selected to just allow the computer with the IP address that you specify to access the IAD using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.5 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your IAD supports SNMP agent functionality, which allows a manager station to manage and monitor the IAD through the network. The IAD supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

Figure 89 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the IAD). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

16.5.1 Supported MIBs

The IAD supports MIB II, which is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

16.5.2 SNMP Traps

The IAD will send traps to the SNMP manager when any one of the following events occurs:

Table 61 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (software reboot).

16.5.3 The SNMP Screen

To change your IAD's SNMP settings, click **Advanced > Remote MGMT > SNMP**. The screen appears as shown.

Figure 90 Remote Management > SNMP

The screenshot shows the SNMP configuration page with the following fields and options:

- Port:** 161
- Access Status:** LAN & WAN
- Secured Client IP:** All Selected
- SNMP Configuration:**
 - Get Community:**
 - Set Community:**
 - TrapCommunity:**
 - TrapDestination:**
- Note:** You may also need to create a [Firewall rule](#)
- Buttons:** Apply, Cancel

The following table describes the labels in this screen.

Table 62 Remote Management > SNMP

LABEL	DESCRIPTION
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the IAD using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the IAD using this service. Select All to allow any computer to access the IAD using this service. Choose Selected to just allow the computer with the IP address that you specify to access the IAD using this service.
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.6 The DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to [Chapter 7 on page 59](#) for background information.

Click **Advanced > Remote MGMT > DNS** to change your IAD's DNS settings. Use this screen to set from which IP address the IAD will accept DNS queries and on which interface it can send them your IAD's DNS settings.

Figure 91 Remote Management > DNS

The following table describes the labels in this screen.

Table 63 Remote Management > DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the IAD.
Secured Client IP	A secured client is a "trusted" computer that is allowed to send DNS queries to the IAD. Select All to allow any computer to send DNS queries to the IAD. Choose Selected to just allow the computer with the IP address that you specify to send DNS queries to the IAD.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.7 The ICMP Screen

To change your IAD's security settings, click **Advanced > Remote MGMT > ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your IAD, an ICMP response packet is automatically returned. This allows the outside user to know the IAD exists. Your IAD supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your IAD when unsupported ports are probed.

Note: If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

Figure 92 Remote Management > ICMP

The following table describes the labels in this screen.

Table 64 Remote Management > ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The IAD will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN & WAN to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the IAD by probing for unused ports. If you select this option, the IAD will not respond to port request(s) for unused ports, thus leaving the unused ports and the IAD unseen. If this option is not selected, the IAD will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the IAD's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the IAD reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.8 SSH

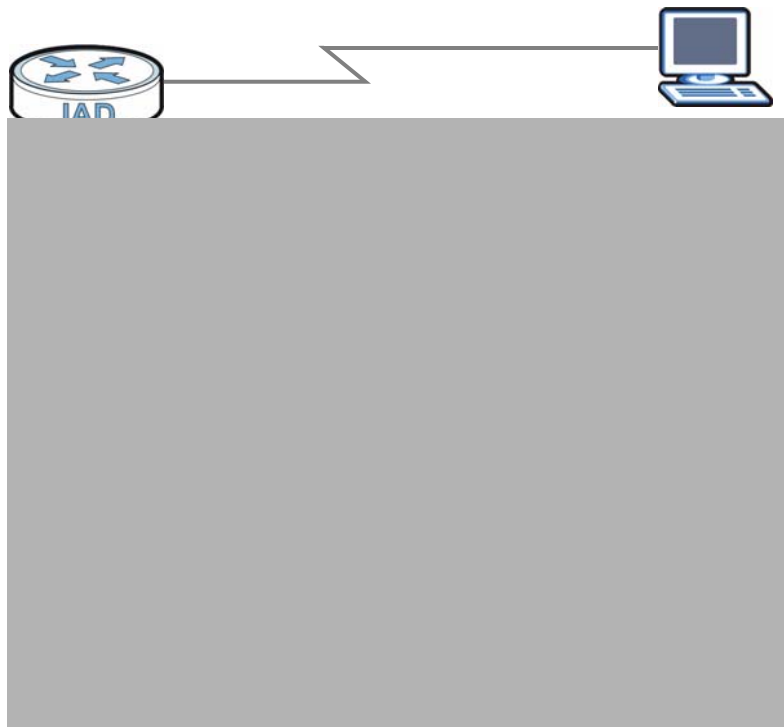
You can use SSH (Secure Shell) to securely access the IAD's command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

16.9 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 93 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

16.10 SSH Implementation on the IAD

Your IAD supports SSH version 1.0 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the IAD for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

16.10.1 Requirements for Using SSH

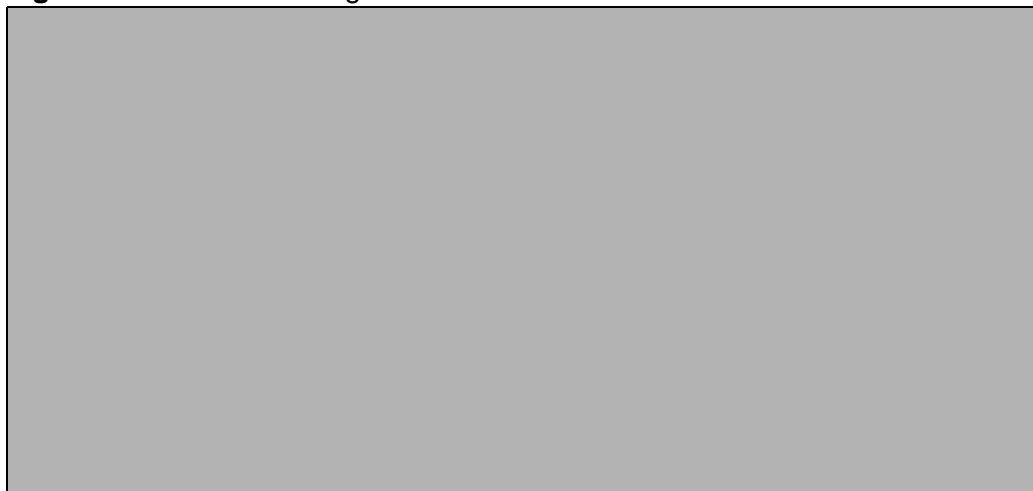
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the IAD over SSH.

16.11 The SSH Screen

Click **Advanced > Remote MGMT > Telnet** to change your IAD's Secure Shell settings.

Note: It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 94 Remote Management > SSH



The following table describes the labels in this screen.

Table 65 Remote Management > SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the IAD for SSH connections. You must have certificates already configured in the My Certificates screen (Click My Certificates and see Chapter 16 on page 37 for details).
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the IAD using this service.
Secured Client IP	A secure client is a “trusted” computer that is allowed to communicate with the IAD using this service. Select All to allow any computer to access the IAD using this service. Choose Selected to just allow the computer with the IP address that you specify to access the IAD using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Universal Plug-and-Play (UPnP)

17.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

17.1.1 What You Can Do in this Chapter

Use the **UPnP** screen ([Section 17.2 on page 198](#)) to enable UPnP on the IAD and allow UPnP-enabled applications to automatically configure the IAD.

17.1.2 What You Need to Know

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the IAD allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

17.2 The UPnP Screen

Click **Advanced** > **UPnP** to display the screen shown next.

See [Section 17.1 on page 197](#) for more information.

Figure 95 Configuring UPnP

The screenshot shows a web-based configuration interface for UPnP. At the top, there is a 'General' tab. Below it, the 'UPnP Setup' section is visible. The 'Device Name' is 'ZyXEL P-2602HW-F3 Internet Sharing Gateway'. Two checkboxes are present: 'Active the Universal Plug and Play(UPnP) Feature' and 'Allow users to make configuration changes through UPnP', both of which are checked. A note with a yellow icon states: 'For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.' At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the fields in this screen.

Table 66 Configuring UPnP

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the IAD's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the IAD so that they can communicate through the IAD, for example by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click Apply to save the setting to the IAD.
Cancel	Click Cancel to return to the previously saved settings.

17.3 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

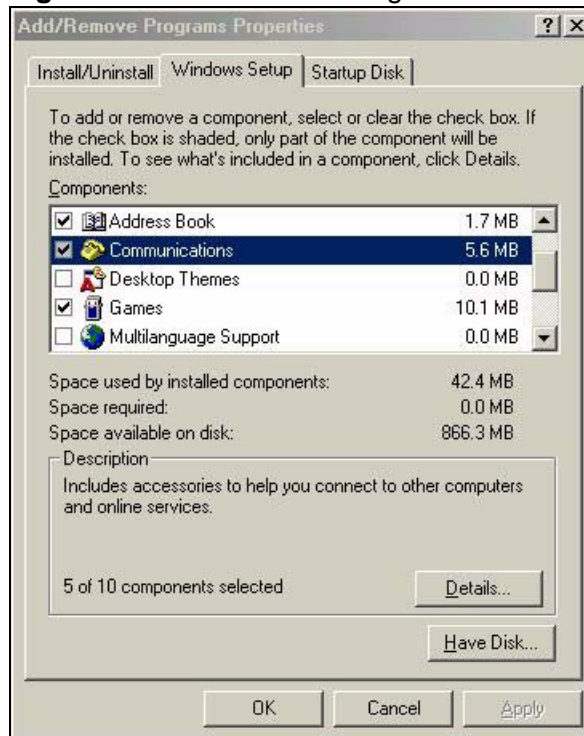
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

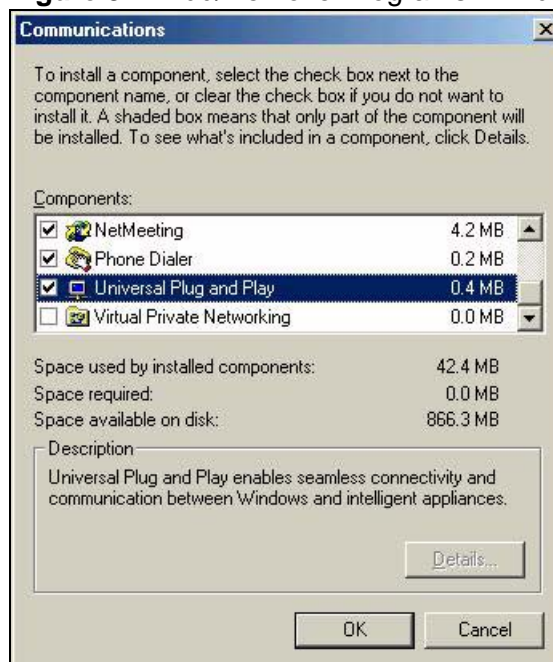
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 96 Add/Remove Programs: Windows Setup: Communication



- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 97 Add/Remove Programs: Windows Setup: Communication: Components



- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

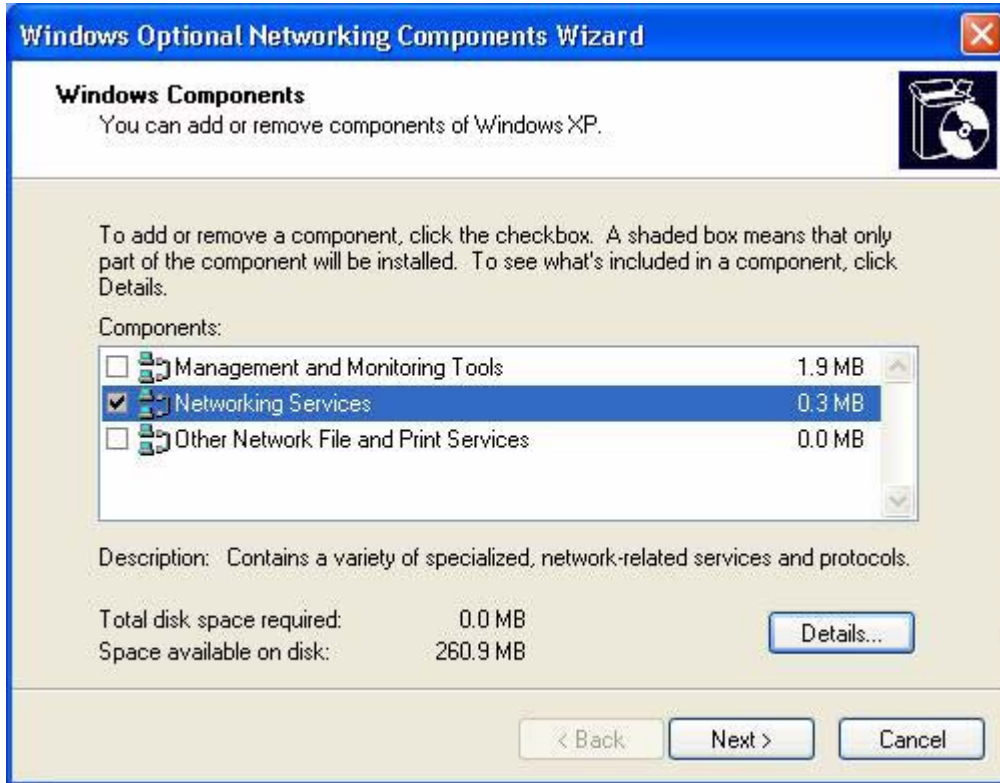
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components**

Figure 98 Network Connections



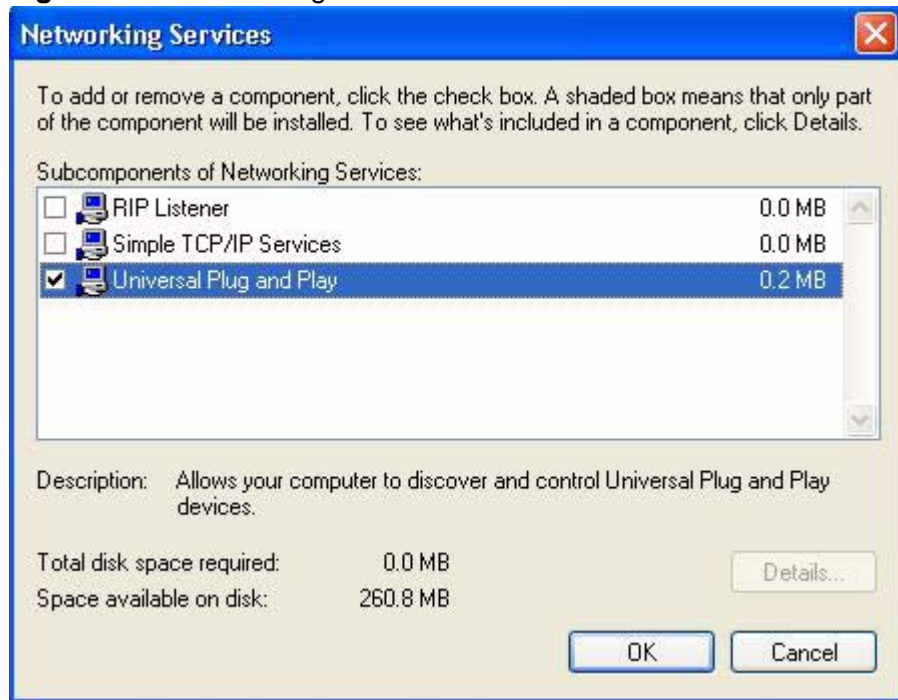
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 99 Windows Optional Networking Components Wizard



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 100 Networking Services



- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

17.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the IAD.

Make sure the computer is connected to a LAN port of the IAD. Turn on your computer and the IAD.

Auto-discover Your UPnP-enabled Network Device

- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

- 2 Right-click the icon and select **Properties**.

Figure 101 Network Connections



- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 102 Internet Connection Properties



- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 103 Internet Connection Properties: Advanced Settings

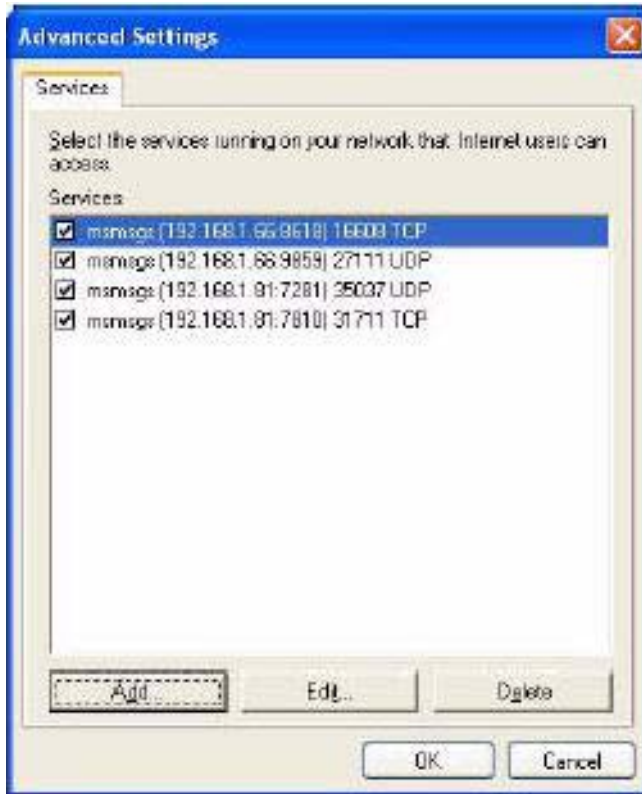


Figure 104 Internet Connection Properties: Advanced Settings: Add



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 105 System Tray Icon



- 7 Double-click on the icon to display your current Internet connection status.

Figure 106 Internet Connection Status



Web Configurator Easy Access

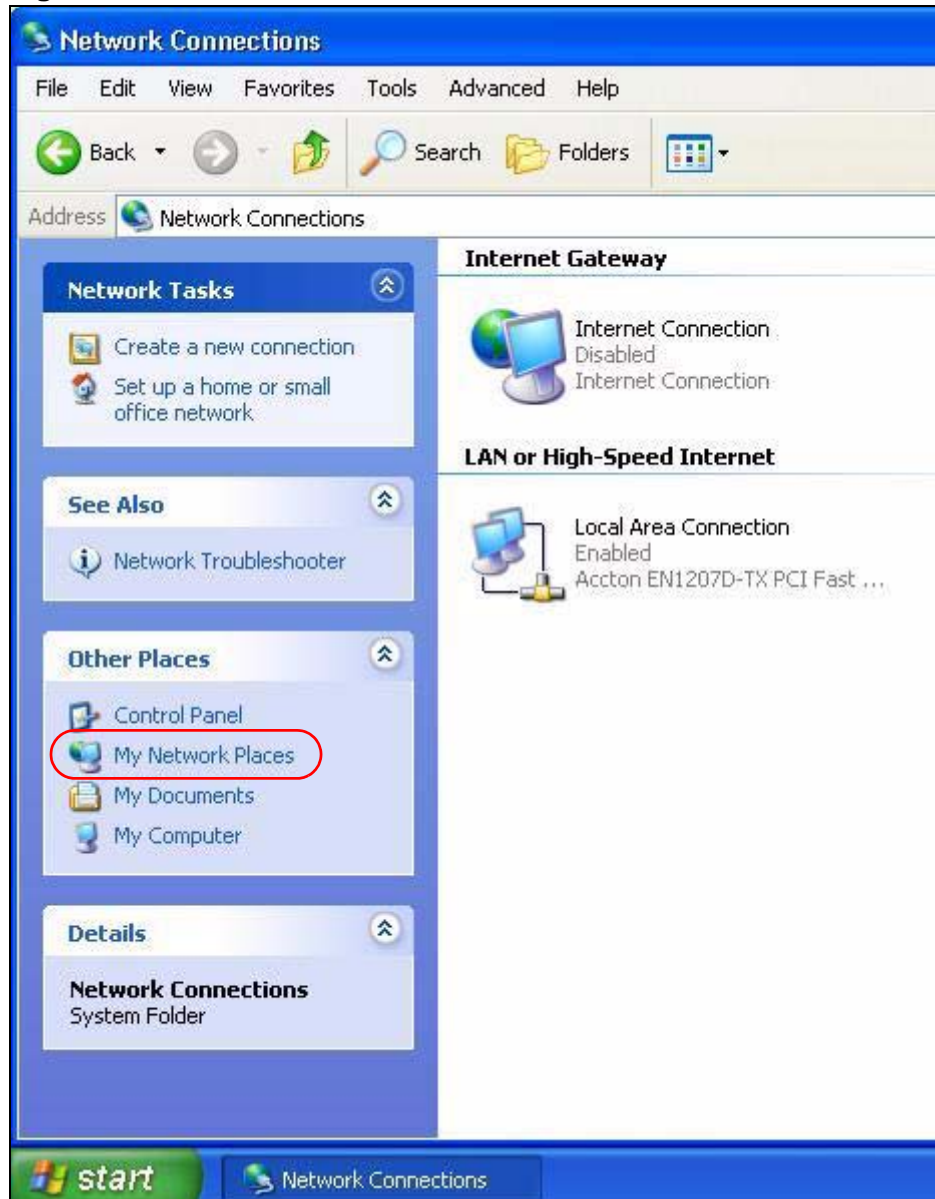
With UPnP, you can access the web-based configurator on the IAD without finding out the IP address of the IAD first. This comes helpful if you do not know the IP address of the IAD.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

- 3 Select **My Network Places** under **Other Places**.

Figure 107 Network Connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

- 5 Right-click on the icon for your IAD and select **Invoke**. The web configurator login screen displays.

Figure 108 Network Connections: My Network Places



- 6 Right-click on the icon for your IAD and select **Properties**. A properties window displays with basic information about the IAD.

Figure 109 Network Connections: My Network Places: Properties: Example



18.1 Overview

Use this screen to configure the IAD's time and date settings.

18.1.1 What You Need to Know

The following terms and concepts may help as you read through this chapter.

General Setup and System Name


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 2000, click **Start > Settings > 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 IAD **System Name**.

18.2 General Setup

Use this screen to configure the IAD's system name, inactivity timer, and password. Click **Maintenance > System** to open the **General** screen.

Figure 110 System > General Setup

System Setup	
System Name	<input type="text" value="P-3202H-Bb"/>
Administrator Inactivity Timer	<input type="text" value="5"/> (minutes, 0 means no timeout)
Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Retype to confirm	<input type="text"/>
<p> CAUTION: Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.</p>	

The following table describes the labels in this screen.

Table 67 General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or telnet) 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).
Password	
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the IAD.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

18.3 Time Setting

To change your IAD's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the IAD's time based on your local time zone.

Figure 111 System > Time Setting

The following table describes the fields in this screen.

Table 68 Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your IAD. Each time you reload this page, the IAD synchronizes the time with the time server.
Current Date	This field displays the date of your IAD. Each time you reload this page, the IAD synchronizes the date with the time server.
Time and Date Setup	
Get from Time Server	Select this radio button to have the IAD get the time and date from the time server you specified below.
Time Protocol	Indicates that the IAD uses the NTP format, which displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Apply	Click Apply to save your changes back to the IAD.
Cancel	Click Cancel to begin configuring this screen afresh.

19.1 Overview

This chapter contains information about configuring general log settings and viewing the IAD's logs.

The web configurator allows you to choose which categories of events and/or alerts to have the IAD log and then display the logs or have the IAD send them to an administrator (as e-mail) or to a syslog server.

19.2 View Log

Click **Maintenance > Logs** to open the **View Log** screen. Use this screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 19.3 on page 217](#)).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 112 View Log

The screenshot shows the 'View Logs' web interface. At the top, there is a header 'View Logs'. Below the header, there are two dropdown menus: 'Display' set to 'All Logs' and 'Level' set to 'All'. To the right of these are two buttons: 'Refresh' and 'ClearLog'. Below this is a table titled 'Log List'. The table has five columns: '#', 'Time', 'Facility', 'Level', and 'Message'. The table is currently empty, and below it, there is a pagination control showing 'Page 1 of 1' and a refresh icon. The text 'no record' is displayed at the bottom right of the table area.

The following table describes the fields in this screen.

Table 69 View Log

LABEL	DESCRIPTION
Display	<p>The categories that you select in the Log Settings screen display in the drop-down list box.</p> <p>Select a category of logs to view; select All Logs to view logs from all of the log categories that you selected in the Log Settings page.</p>
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	<p>This indicates the type of connection to the IAD.</p> <p>Facility types are as follows:</p> <ul style="list-style-type: none"> • tr069 - This indicates a log from an external auto-configuration server. • ntpclient - This indicates a log from the ntpclient. • login - This indicates a message from the login server. • udhcpc - This indicates a log message from the device's DHCP server. • dnsmasq - This indicates a log message from the device's DNS forwarder. • PPPD - This indicates a log message from the device's Point-to-Point Protocol daemon. • kernel - This indicates a log message related to the device's Central Processing Unit (CPU), memory, and I/O ports. • OMCI - This indicates a log message about the OpenManage Client Instrumentation. • VoIP - This indicates a log a message from the SIP server.
Level	This indicates the log severity.
Message	This field states the reason for the log.
First	Click this to cycle to the first page of logs.
Previous	Click this to cycle to the previous page of logs.
Page	This indicates which page you are on, out of how many. You can enter a page number here and press [Enter] to jump directly to that page.
Next	Click this to cycle to the next page of logs.
Last	Click this to cycle to the last page of logs
Refresh	Click this to refresh the logs screen.

19.3 Log Settings

Use this screen to configure which logs to display on the **View Logs** screen (see [Chapter 19 on page 215](#)). Click **Maintenance > Logs > Log Settings**.

Figure 113 Log Settings

Active Log		
<input type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors	<input type="checkbox"/> PON Link
<input type="checkbox"/> TR-069	<input type="checkbox"/> VoIP	<input type="checkbox"/> OMCI

The following table describes the fields in this screen.

Table 70 Log Settings

LABEL	DESCRIPTION
Active Log	
[Log Type]	Select the type of log you want to be displayed on the View Logs screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.

20.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your IAD.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality.

20.1.1 Some Warnings

The following are some friendly reminders about your device:

Do NOT turn off the IAD while a firmware upload is in progress!

Only use firmware for your device's specific model. Refer to the label on the bottom of your IAD.

20.2 Firmware Upgrade

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your IAD. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Figure 114 Firmware Upgrade

The following table describes the labels in this screen.

Table 71 Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
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.

After you see the **Firmware Upload in Progress** screen, wait three minutes before logging into the IAD again.

The IAD automatically restarts in this time causing a temporary network disconnect.

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

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

20.3 Configuration

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 115 Configuration

The screenshot shows a web interface with three sections:

- Backup Configuration:** A heading followed by the text "Click **Backup** to save the current configuration to your computer." and a "Backup" button.
- Restore Configuration:** A heading followed by the text "To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click **Browse** to look for one, and then click **Upload**." Below this is a "File Path:" label, a text input field, a "Browse..." button, and an "Upload" button.
- Reset to Factory Default Settings:** A heading followed by the text "Click **Reset** to clear all user-entered configuration and return the Prestige to the factory default settings." Below this is the text "The following default settings would become effective after click **Reset**" followed by "Password :1234" and "Lan IP : 192.168.1.1 ." and a "Reset" button.

20.3.1 Backup Configuration

Backup Configuration allows you to back up (save) the IAD's current configuration to a file on your computer. Once your IAD 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 IAD's current configuration to your computer.

20.3.2 Restore Configuration

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

Table 72 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.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the IAD again.

The IAD automatically restarts in this time causing a temporary network disconnect.

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 device IP address (10.0.0.138). See [Appendix B on page 245](#) for details on how to set up your computer’s IP address.

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

20.3.3 Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the IAD to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your IAD.

20.4 Restart

System restart allows you to reboot the IAD without turning the power off. Click **Maintenance > Tools > Restart**. Click **Restart** to have the IAD reboot. This does not affect the IAD's configuration.

Figure 116 Restart Screen



Diagnostic

21.1 Overview

This read-only screen displays information to help you identify problems with the IAD.

21.2 General

Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 117 Diagnostic > General

The screenshot shows a window titled "General". Inside the window, there is a large text area with the text "- Info -" at the top. Below the text area, there is a "TCP/IP Address" label followed by an input field and a "Ping" button.

The following table describes the fields in this screen.

Table 73 General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.

Troubleshooting

22.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [IAD Access and Login](#)
- [Internet Access](#)
- [Phone Calls and VoIP](#)

22.2 Power, Hardware Connections, and LEDs

The IAD does not turn on. None of the LEDs turn on.

- 1 Make sure the IAD is turned on.
- 2 Make sure you are using the power adaptor or cord included with the IAD.
- 3 Make sure the power adaptor or cord is connected to the IAD and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the IAD off and on.
- 5 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.6 on page 26](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the IAD off and on.
- 5 If the problem continues, contact the vendor.

22.3 IAD Access and Login

I forgot the IP address for the IAD.

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the IAD by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the IAD (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.5 on page 25](#).

I cannot see or access the **Login** screen in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is 192.168.1.1.
 - If you changed the IP address, use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the IAD](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
 - 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix C on page 275](#).
 - 4 Reset the device to its factory defaults, and try to access the IAD with the default IP address. See [Section 1.5 on page 25](#).
 - 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

I can see the **Login** screen, but I cannot log in to the IAD.

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the IAD. Log out of the IAD in the other session, or ask the person who is logged in to log out.
- 3 Turn the IAD off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 22.2 on page 225](#).

22.4 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.6 on page 26](#).
- 2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.

- 3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the IAD), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.6 on page 26](#).
- 2 Turn the IAD off and on.
- 3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.6 on page 26](#). If the IAD is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Turn the IAD off and on.
- 3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

22.5 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

- 1 Check the telephone connections and telephone wire.

I can access the Internet, but cannot make VoIP calls.

- 1 The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.
- 2 You can also check the VoIP status in the **Status** screen.
- 3 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

Product Specifications

The following tables summarize the IAD's hardware and firmware features.

Hardware Specifications

Table 74 Hardware Specifications

Dimensions	215 W x 145 D x 35 H mm
Weight	390 g
Power Specification	18V DC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
PHONE Port	2 RJ-11 FXS POTS ports
CATV Port	1 F-type coaxial connector
Antennas	2 attached external dipole antennas, 2dBi
WPS Button	1 second: turn on or off WLAN 5 seconds: enable WPS (Wi-Fi Protected Setup)
RESET Button	Restores factory defaults
PON Port	1 SC/UPC type fiber-optic connector
Operation Temperature	0° C ~ 40° C
Storage Temperature	-20° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH
Distance between the centers of the holes (for wall-mounting) on the device's back	137.20mm
Screw size for wall-mounting	M4 tap

Voice Specifications

Note: To take full advantage of the supplementary phone services available through the IAD's phone port, you may need to subscribe to the services from your VoIP service provider.

Note: Not all features are supported by all service providers. Consult your service provider for more information.

Table 75 Voice Features

Call Park and Pickup	<p>Call park and pickup lets you put a call on hold (park) and then continue the call (pickup). The caller must still pay while the call is parked.</p> <p>When you park the call, you enter a number of your choice (up to eight digits), which you must enter again when you pick up the call. If you do not enter the correct number, you cannot pickup the call. This means that only someone who knows the number you have chosen can pick up the call.</p> <p>You can have more than one call on hold at the same time, but you must give each call a different number.</p>
Call Return	<p>With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.</p>
Country Code	<p>Phone standards and settings differ from one country to another, so the settings on your IAD must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the IAD from one country to another.</p>
Do not Disturb (DnD)	<p>This feature allows you to set your phone not to ring when someone calls you. You can set each phone independently using its keypad, or configure global settings for all phones using the command line interpreter.</p>
Auto Dial	<p>You can set the IAD to automatically dial a specified number immediately whenever you lift a phone off the hook. Use the Web Configurator to set the specified number. Use the command line interpreter to have the IAD wait a specified length of time before dialing the number.</p>
Phone config	<p>The phone config table allows you to customize the phone keypad combinations you use to access certain features on the IAD, such as call waiting, call return, call forward, etc. The phone config table is configurable in command interpreter mode.</p>
HTTP pincode	<p>If your service provider uses an auto provisioning server, you need to enter a personal identification number (supplied by your service provider) before you first use the feature.</p>

Table 75 Voice Features

Firmware update enable / disable	If your service provider uses this feature, you hear a recorded message when you pick up the phone when new firmware is available for your IAD. Enter *99# in your phone's keypad to have the IAD upgrade the firmware, or enter #99# to not upgrade. If your service provider gave you different numbers to use, enter them instead. If you enter the code to not upgrade, you can make a call as normal. You will hear the recording again each time you pick up the phone, until you upgrade.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.
Call forwarding	With this feature, you can set the IAD to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
Caller ID	The IAD supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.
Multiple SIP Accounts	You can simultaneously use multiple voice (SIP) accounts and assign them to the telephone port.
Multiple Voice Channels	Your device 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 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	Your device 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).

Table 75 Voice Features

Echo Cancellation	You device 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.
Other Voice Features	<p>SIP version 2 (Session Initiating Protocol RFC 3261)</p> <p>SDP (Session Description Protocol RFC 2327)</p> <p>RTP (RFC 1889)</p> <p>RTCP (RFC 1890)</p> <p>Voice codecs (coder/decoders) G.711, G.726, G.729</p> <p>Fax and data modem discrimination</p> <p>DTMF Detection and Generation</p> <p>DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO)</p> <p>Point-to-point call establishment between two IADs</p> <p>Quick dialing through predefined phone book, which maps the phone dialing number and destination URL.</p> <p>Flexible Dial Plan (RFC3525 section 7.1.14)</p>

The following list, which is not exhaustive, illustrates the standards supported in the IAD.

Table 76 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC 2766	Network Address Translation - Protocol
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.

Table 76 Standards Supported (continued)

STANDARD	DESCRIPTION
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

Power Adaptor Specifications

Table 77 Power Adaptor Specifications

North American PLUG standards	LEI (LEADER ELECTRONICS INC.)
AC Power Adapter Model	MU18-2180100-A1
Input Power	AC 100~240Volts/50/60Hz/0.6A
Output Power	DC 18Volts/1A
Power Consumption	16 Watt max
Safety Standards	UL,CUL(UL 60950-1)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	MU18-Y1180-K105
Input Power	AC 230V~50Hz 0.5A
Output Power	DC 18Volts/1A
Power Consumption	16 Watt max
Safety Standards	TUV, CE(EN 60950-1)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adapter Model	MU18-2180100-B2
Input Power	AC 100~240Volts/50/60Hz/0.6A
Output Power	DC 18Volts/1A
Power Consumption	12 Watt max
Safety Standards	TUV, CE(EN 60950-1)

G-PON Specification

Table 78 G-PON Specifications

SPECIFICATION	DESCRIPTION
Standard	IEEE 802.3ah
Upstream Bit Rate	1.25 Gb/s
Downstream Bit Rate	1.25 Gb/s
Distance	10 Km/20 Km
Power Budget	Class A: 5~20 dB Class B: 10~25 dB
Wavelength Allocation	Up: 1260~1360 nm Down: 1480~1500 nm
Splitter Ratio	>16
FEC	Not Supported
DBA	Not Supported
Encryption	Not Supported

Wall-mounting Instructions

Do the following to hang your IAD on a wall.

Note: See [Table 74 on page 231](#) for the size of screws to use and how far apart to place them.

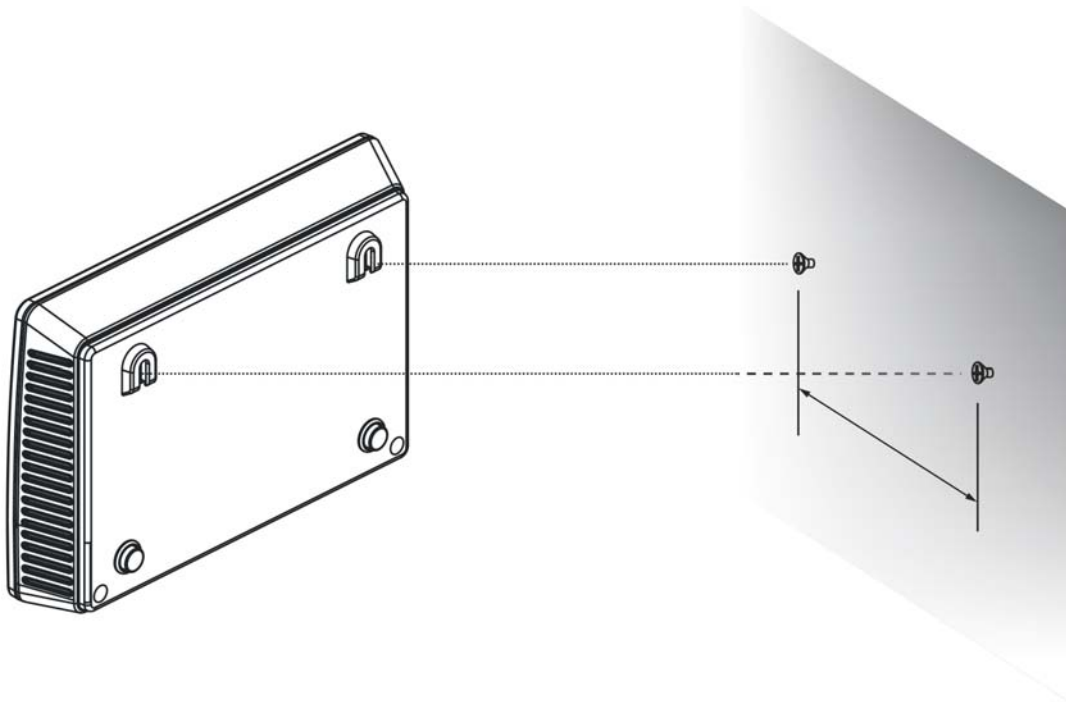
- 1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.
- 2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the IAD with the connection cables.

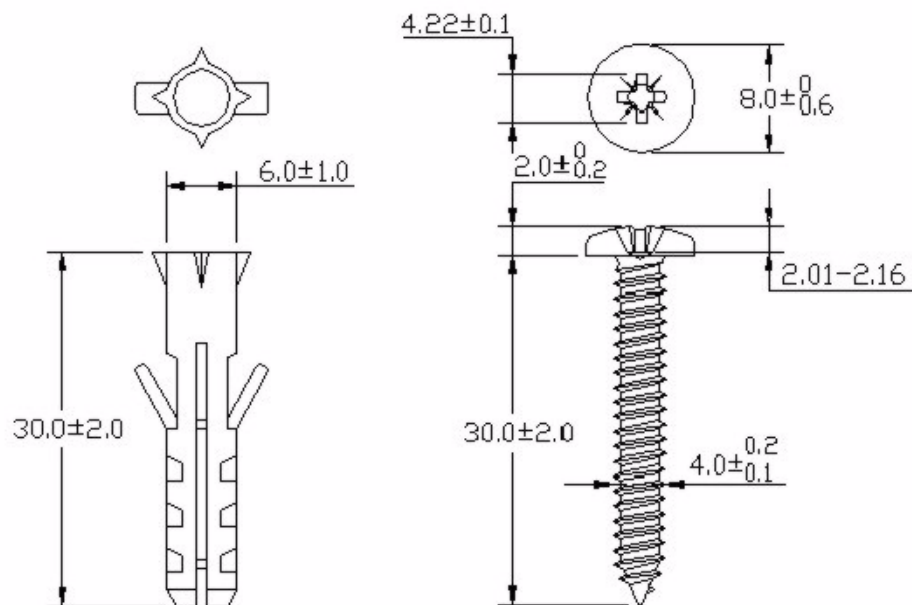
- 5 Align the holes on the back of the IAD with the screws on the wall. Hang the IAD on the screws.

Figure 118 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 119 Masonry Plug and M4 Tap Screw



Passive Optical Networks

Optical fiber allows for data to be transmitted in the form of staggered light impulses. It is composed of flexible plastic or glass piping. Light waves traverse the length of the piping by perpetually reflecting itself off of its mirrored inner core, much like an optical waveguide.

The most common application for optical fiber is as a medium to transmit digital information from one location to another over great distances. However, one of the drawbacks of this medium is that light attenuates and eventually loses its coherency. The great challenge in optical fiber research lies in the development of fiber cables capable of minimizing this light attenuation for as long as physically possible. Despite this, optical fiber technology remains on the cutting edge of network communications development.

Optical fiber offers enormous benefits in terms of speed, quality, and quantity over other methods such as copper wire, and is the core technology behind the Passive Optical Network (PON).

What You Need to Know

The following terms and concepts may help as you read through this chapter.

PON

A Passive Optical Network (PON) sends fiber optical cables from a service provider to the premises. "Passive" means that no power is required once the data, which is transmitted as light, enters the cables.

ONU

An Optical Network Unit (ONU) is a fiber optical modem that allows a subscriber or client to receive very high-speed Internet access.

OLT

An Optical Line Terminal (OLT) is placed at a broadband service provider's central office, where it receives voice, video, and other data from the service provider's networking servers. It then converts and transmits this data as light across a fiber optical network, where it is received and translated on the opposite end by one or more Optical Network Units (ONUs).

FTTx

Fiber-To-The-x (FTTx) refers to networking infrastructure that extends from a service provider to the x, where x can be one of many locations: Office (FTTO), Home (FTTH), Desk (FTTD), Building (FTTB) or even Curb (FTTC), to name a few. In an FTTO connection, the Optical Network Unit (ONU) is often placed inside the building, whereas in FTTH or FTTC the fiber ends at an end-user's house (or somewhere nearby), or at a curb-side unit.

Gigabit Ethernet

Gigabit Ethernet (IEEE 802.3z standard) uses Ethernet over copper wire technology to increase network data rates to 1 Gbit/sec. It is built upon standard 4-pair Category 5 copper cabling.

GEM

The Generic Encapsulation Method (GEM) provides a method for PON devices to natively transmit both Ethernet and TDM data over optical fiber.

ATM

Asynchronous Transfer Method (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.

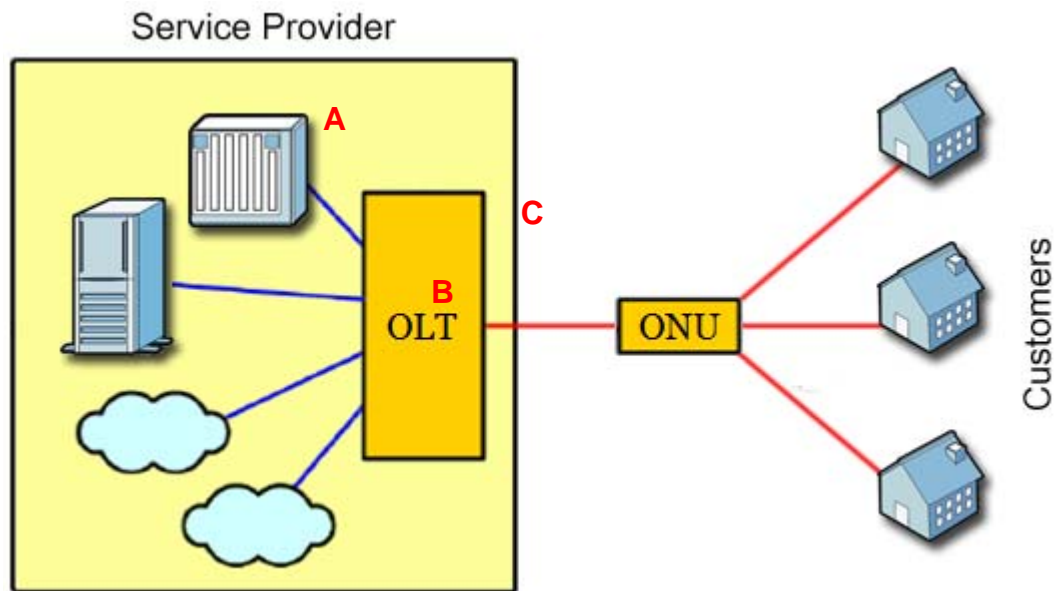
TDM

In Time Division Multiplexing (TDM), individual data subchannels can occupy the entire frequency bandwidth of a communication stream at certain specific times, and cannot transmit at other times. Each subchannel takes turns using the communications stream. TDM is typically used in FTTx and satellite communication.

How It Works

There are no active components in the PON backbone that require power. Light impulses move from point A to point B with nothing in between to facilitate it other than optical physics. Although the devices at the point of origin and the point of termination undoubtedly require power, the network itself does not.

Figure 120 An example of Passive Optical Networking



In this example, the PON consists of: one or more Optical Line Terminals (OLTs) located at the service provider's central office (**A**) to convert and transmit data; a network of fiber optical cables to passively carry the data (**B**); and one or more Optical Network Units (ONUs) at the subscriber end to receive the data (**C**).

PON Development

As a technology, PON has been around for quite some time although it was initially unusable for network communications.

One of the original improvements made to it was Asynchronous Transfer Method PON (ATM PON, more commonly called APON). The benefit of using a well established networking protocol (such as ATM in this case) to enhance the fiber network is that it is usually backwards-compatible with an existing Wide Area Network (WAN). Unfortunately, ATM has fallen out of favor due to its relative complexity and the rapid rise in popularity of the Internet Protocol (IP), which is both less complex and more cost effective due to the ubiquitousness of the hardware that supports it. A more robust off-shoot of APON offering faster transmission speeds is Broadband PON (BPON).

Ethernet PON (EPON), meanwhile, offers slightly slower data transmission rates but shows a smaller overhead and is markedly better at transmitting over the Ethernet layer using IP. Because Ethernet is so widespread and relies on a well-established universal networking protocol, manufacturers can use existing hardware to build EPON units, making it a very cost effective solution in comparison to the other types of PON devices available. Moreover, Ethernet cables (RJ-45) and infrastructure already exist in many office buildings, so making the transition to EPON is even easier.

GEAPON is the other name by which EPON is known and marketed. For all intents and purposes, it is the same. Both fall under the purview of the IEEE802.3ah specification.

Gigabit Ethernet PON (GPON) offers a speed boost over APON/BPON and EPON. It retains ATM compatibility in addition to offering Time-Division Multiplexing (TDM). It can utilize both the ATM and Ethernet transport layers, but only by emulating them with the Generic Encapsulation Protocol (GEM).

The following table outlines the major differences between the three PON protocols.

Table 79 PON Types Comparison

PARAMETERS	EPON/GEAPON	APON/BPON	GPON
Standard	IEEE802.3ah	ITU-T (FSAN)	ITU-T SG15 (FSAN)
Standardization Date	2004.07	1998 ITU.T G.983	2003.11 ITU.T G.984
Speed	1 Gbps	155/622 Mbps 622/1244 Mbps	1.25 Gbps symmetric and higher (up to 2.488 Gbps)
Basic Protocol	Ethernet	ATM	Ethernet/ATM/TDM
Protocol Overhead for IP	Small	Large	Middle
US MAC Scheme	TDMA	TDMA	TDMA
Coding Line	8B/10B	Scramble NRZ	Scramble NRZ
BER	10^{-12}	10^{-10}	10^{-12}
ODN Type	Type1, Type2	Class A, B	Class A, B, C
Max Reach	Type1 up to 10 km Type2 up to 20 km	20 km	20 km (Max 60 km for ranging protocol)
Standard Driver	Vendors	Service Provider	Service Provider

PON Limitations

The most significant limitation of PON is something known as “attenuation.” This is the gradual decrease in signal strength as the light wave passes down the fiber optical cable stemming from a combination of absorption and scattering.

Absorption happens as the light's energy is converted into heat; scattering occurs when the light hits stray particles of other matter inside the cable and some its photons are redirected in other directions. As a result, the further the light in the pipe travels, the less coherent it becomes and eventually it disintegrates. In current PON implementations, there are two standard distances that a service provider can choose: 1-10 kilometers and 1-20 kilometers. Light does not attenuate differently over the greater of the two distances; rather, the service provider simply uses much more powerful equipment to transmit the light signals into the network, thus boosting the relative signal strength to such a point that attenuation does not set in as rapidly.

The other major limitation is the "splitting." To make the most of available bandwidth, service providers must split a backbone line into many smaller lines which are then extended to multiple customers.

For example, a backbone line leaving the service provider's central office may split twice, sending subsidiary lines to branch office ONUs or secondary OLTs. These, in turn, can be split again and again until a certain number of customers have been served. However, each time a light signal is split each subsequent subsidiary beam is at a markedly lower intensity than the original. If a service provider's maximum bandwidth allocation is approximately 60 Mbps/sec (the physical limitation of the fiber), this bandwidth must be shared among all customers connected to the backbone. If only one customer is connected, they reap the benefits of full 60 Mbps/sec bandwidth; on the other hand, if the service provider splits the signal so that three customers in three disparate locations can benefit, each one only receives ~20 Mbps/sec of bandwidth because of the tripartite split. The maximum number of splits that a service provider can make is 64, at which point the data flood from the signal source becomes but a trickle by the time it reaches the end of its journey.

Bit Rate Requirements

The kind of transmission speeds a PON provides depends primarily on the kind of network your service provider maintains and any bandwidth limits it enforces (if it does so at all). Various programs and applications can take advantage of the network's bandwidth as long as it meets their requirements.

Below is a table listing the minimum bit rates various types of applications require in order to operate at their full potential over a PON. If you are not sure about

your connection speeds, check with your service provider or network administrator.

Table 80 Applications and Required Bit Rates

APPLICATION	MINIMUM BIT RATE
Voice over Internet Protocol (VoIP)	16 kbps
Full-screen Video Conferencing (H.263)	384 kbps
Basic Web Browsing	1 Mbps
5-Megapixel JPG in 10 seconds	1.5 Mbps
SDTV (MPEG-2)	4 Mbps
SDTV (MPEG-4)	1.5 Mbps
HDTV (MPEG-2)	15 Mbps
HDTV (MPEG-4)	7-9 Mbps

Setting Up Your Computer's IP Address

Note: Your specific IAD may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

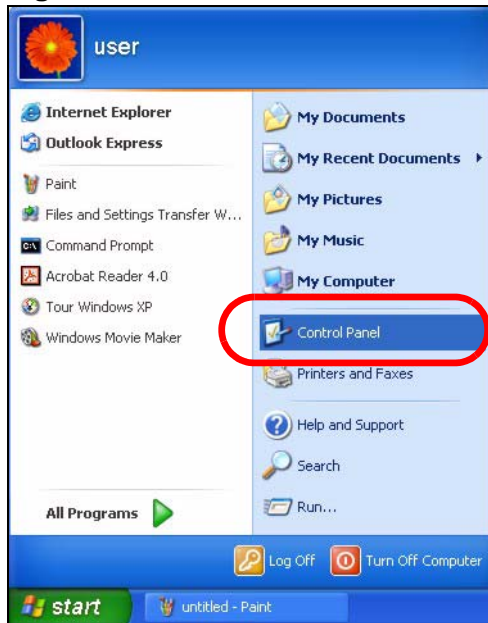
- [Windows XP/NT/2000](#) on [page 245](#)
- [Windows Vista](#) on [page 249](#)
- [Windows 7](#) on [page 253](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 257](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 261](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 264](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 269](#)

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

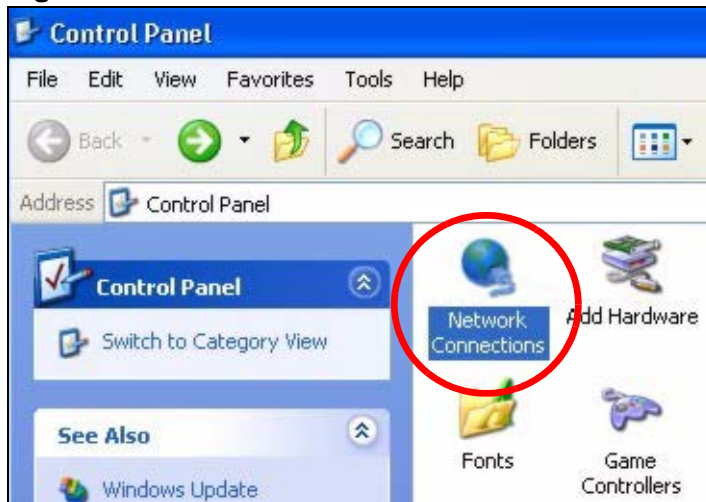
- 1 Click **Start > Control Panel**.

Figure 121 Windows XP: Start Menu



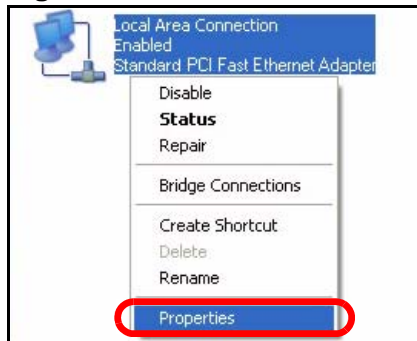
- 2 In the **Control Panel**, click the **Network Connections** icon.

Figure 122 Windows XP: Control Panel



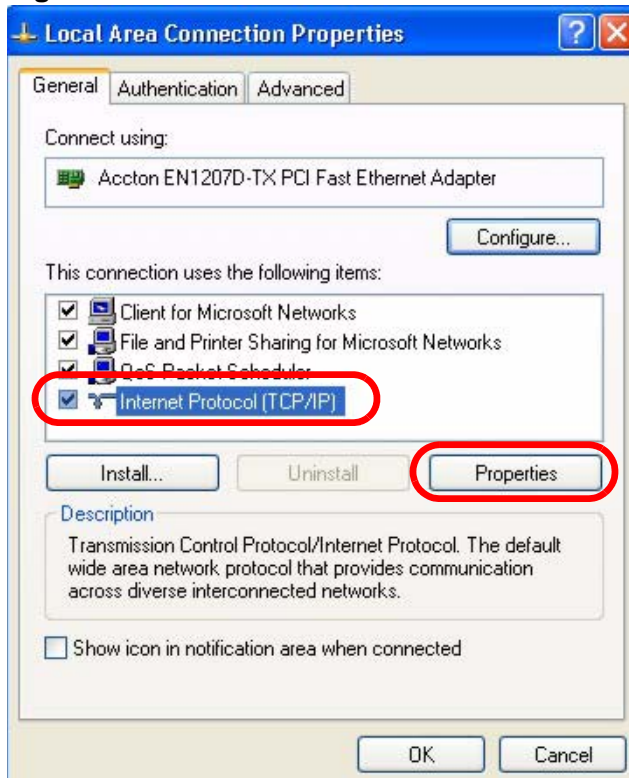
- 3 Right-click **Local Area Connection** and then select **Properties**.

Figure 123 Windows XP: Control Panel > Network Connections > Properties



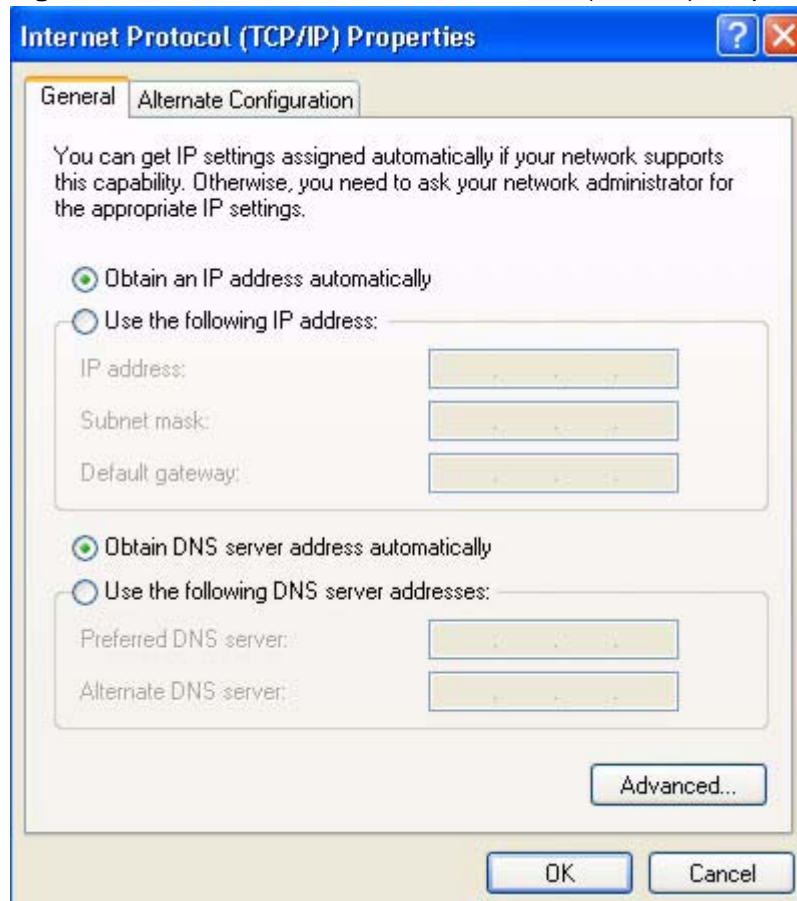
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 124 Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 125 Windows XP: Internet Protocol (TCP/IP) Properties



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.

- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

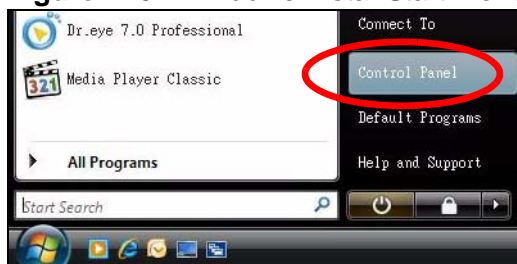
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

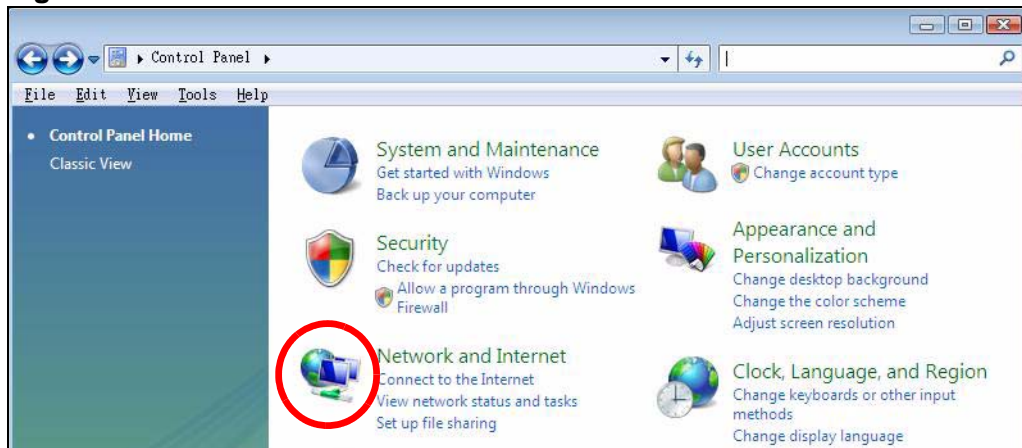
- 1 Click **Start > Control Panel**.

Figure 126 Windows Vista: Start Menu



- 2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 127 Windows Vista: Control Panel



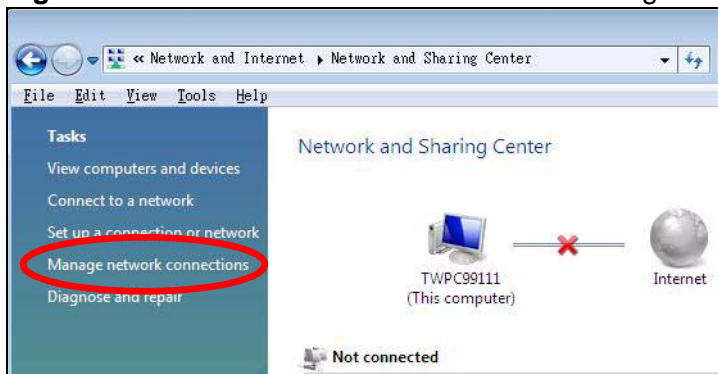
- 3 Click the **Network and Sharing Center** icon.

Figure 128 Windows Vista: Network And Internet



- 4 Click **Manage network connections**.

Figure 129 Windows Vista: Network and Sharing Center



- 5 Right-click **Local Area Connection** and then select **Properties**.

Figure 130 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.