

FSG1100HN

Wireless Active Fiber Router

User's Guide

Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version: 1.0
Edition1, 3/2010

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the FSG1100HN using the Web Configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Tips for Reading User's Guides On-Screen

When reading a ZyXEL User's Guide On-Screen, keep the following in mind:

- If you don't already have the latest version of Adobe Reader, you can download it from <http://www.adobe.com>.
- Use the PDF's bookmarks to quickly navigate to the areas that interest you. Adobe Reader's bookmarks pane opens by default in all ZyXEL User's Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF.

Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get your FSG1100HN up and running right away. It contains information on setting up your network and configuring for Internet access.

- Supporting Disc

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

- Support Disc

Refer to the included CD for support documents.

Documentation Feedback

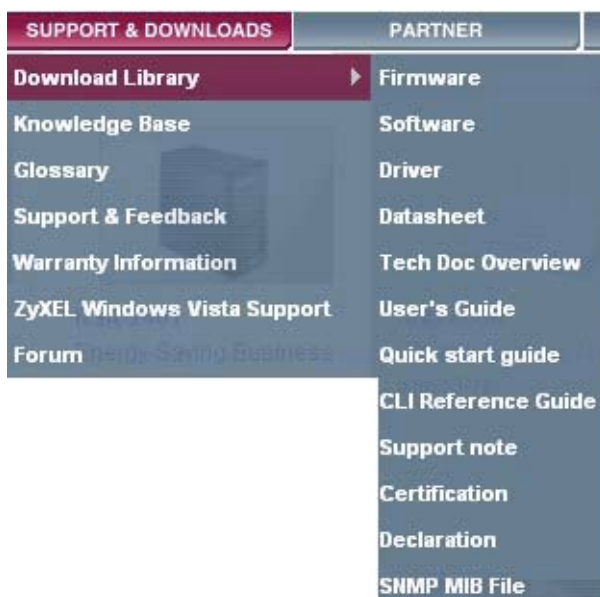
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw.

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 User Guide, Quick Start Guide and Command Line Interface Reference Guide 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.

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

- The FSG1100HN may be referred to as the “FSG1100HN”, the “device”, the “product” 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 ZyXEL icon is not an exact representation of your device.

ZyXEL Device 	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 power outlet.
- 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.
- Antenna Warning! This device meets ETSI 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.
- Optical Warning! "PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11"
"PRODUIT CONFORME SELON 21CFR 1040.10 ET 1040.11"
CLASS 1 LASER PRODUCT
APPAREIL À LASER DE CLASSE 1

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.



Table of Contents

FSG1100HN	1
About This User's Guide.....	3
Safety Warnings	8
Table of Contents.....	10
Introduction.....	13
1 Getting to Know Your FSG1100HN	15
1.1 Overview.....	15
1.2 Applications.....	15
1.3 Ways to Manage the FSG1100HN	16
1.4 Good Habits for Managing the FSG1100HN.....	16
1.5 LEDs.....	16
2 The WPS Button.....	19
2.1 Overview.....	19
3 Introducing the Web Configurator.....	21
3.1 Overview.....	21
3.2 Accessing the Web Configurator.....	21
3.3 Resetting the FSG1100HN.....	22
3.3.1 Procedure to Use the Reset Button.....	22
3.4 Navigating the Web Configurator	23
3.4.1 WLAN Information: Multiple AP Table	24
3.4.2 Summary: Active Session Table.....	25
3.5 Setting the Device Mode.....	26
Network.....	28
4 Wireless LAN	30
4.1 Overview.....	30
4.2 What You Can Do.....	31
4.3 What You Should Know.....	31
4.4 Wireless Basic Settings Screen.....	32
4.4.1 Multiple AP Table	33
4.4.2 Active Wireless Client Table	34
4.5 Wireless Advanced Settings Screen	35
4.6 Wireless Security Screen.....	37
4.6.1 WEP.....	37
4.6.2 WPA.....	39
4.6.3 WPA2.....	41
4.6.4 WPA-Mixed.....	42
4.7 Wireless Access Control Screen	44
4.8 Wi-Fi Protected Setup Screen.....	44
5 WAN.....	48
5.1 Overview.....	48
5.2 What You Can Do.....	48
5.3 WAN for DHCP Client Screen.....	49
5.4 WAN for Static IP Screen.....	51
5.5 WAN for PPPoE Screen.....	53
6 LAN.....	56
6.1 Overview.....	56
6.2 What You Can Do.....	56
6.3 What You Need To Know.....	57
6.3.1 IP Pool Setup	57
6.3.2 LAN TCP/IP.....	57
6.4 LAN General Screen	58

6.4.1	Active DHCP Client Table.....	59
6.4.2	Static DHCP.....	60
6.5	VLAN Screen.....	61
7	NAT.....	63
7.1	Overview.....	63
7.2	What You Can Do.....	63
7.3	NAT General Screen.....	64
7.4	NAT DMZ Screen.....	66
7.5	NAT Port Forwarding Screen.....	67
	Security.....	69
8	Firewall.....	71
8.1	What You Can Do.....	72
8.2	What You Need To Know.....	72
8.2.1	About the FSG1100HN Firewall.....	72
8.3	Firewall Filter Screen.....	73
8.4	Firewall Filter Add Screen.....	74
8.5	Firewall Denial of Service Screen.....	75
8.6	Firewall Content Filter Screen.....	77
	Management.....	80
9	Media Bandwidth Management.....	82
9.1	Media Bandwidth Management Screen.....	82
10	TR-069.....	85
10.1	TR-069 General Screen.....	85
11	Auto Provision.....	88
11.1	Auto Provision Screen.....	88
	Maintenance and Troubleshooting.....	91
12	System Settings.....	93
12.1	System Settings General Screen.....	93
12.2	System Settings Dynamic DNS Screen.....	94
12.3	System Settings Time Screen.....	95
13	Log.....	98
13.1	Log Screen.....	98
14	Tools.....	100
14.1	Tools Firmware Screen.....	100
14.2	Tools Configuration Screen.....	100
14.3	Tools Restart Screen.....	101
	Appendices.....	104
A	Pop-up Windows, JavaScripts and Java Permissions.....	106
B	IP Addresses and Subnetting.....	114
C	Setting up Your Computer's IP Address.....	124
D	Wireless LANs.....	142
E	Services.....	154
F	Legal Information.....	158

PART I

Introduction

Getting to Know Your FSG-100HN (15)

The WPS Button (19)

Introducing the Web Configurator (21)

Setting the Device Mode (24)

Getting to Know Your FSG1100HN

1.1 Overview

This chapter introduces the main features and applications of the FSG1100HN.

The FSG1100HN extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

A range of services such as a firewall and content filtering are also available for secure Internet computing.

1.2 Applications

You can create the following networks using the FSG1100HN:

- **Wired.** You can connect network devices via the Ethernet ports of the FSG1100HN so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the FSG1100HN to access network resources.
- **WAN.** Connect to a broadband modem/router for Internet access.

FSG1100HN Network



1.3 Ways to Manage the FSG1100HN

Use any of the following methods to manage the FSG1100HN.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.
- Web Configurator. This is recommended for everyday management of the FSG1100HN using a (supported) web browser.

1.4 Good Habits for Managing the FSG1100HN

Do the following things regularly to make the FSG1100HN more secure and to manage the FSG1100HN 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 FSG1100HN to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the FSG1100HN. You could simply restore your last configuration.

1.5 LED and Rear Panel





The following table describes the LEDs and the WPS button.

Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The FSG1100HN is receiving power and functioning properly
		Off	The FSG1100HN is not receiving power.
	Red	On	A system error has occurred.
WAN	Green	On	The FSG1100HN has a successful 10/100Mbps WAN connection.
		Blinking	The FSG1100HN is sending/receiving data through the WAN.
		Off	The WAN connection is not ready, or has failed.
WLAN/WPS	Green	On	The FSG1100HN is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The FSG1100HN is sending/receiving data through the wireless LAN. The FSG1100HN is negotiating a WPS connection with a wireless client.
		Off	The FSG1100HN is not ready or has failed.
	Orange	Blinking	The FSG1100HN's WPS connection is being configured.
Internet	Green	On	The FSG1100HN's IP is connected (the device has a WAN IP address from IPCP or DHCP and fiber is linked or a static IP address is configured, PPP negotiation has successfully completed – if used – and fiber is linked) and no traffic is detected. If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if a fiber connection is still present. If the session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.
		Blinking	The FSG1100HN's IP is connected and IP traffic is passing through the device (either direction), flashing at 4 Hz with a 50% duty cycle.

		Off	The FSG1100HN's power is off, it is in bridged mode, or a connection not present.
	Red	On	The FSG1100HN's attempt to achieve an IP connection failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.).
LAN 1-4	Green	On	The FSG1100HN has a successful 10/100Mbps Ethernet connection.
		Blinking	The FSG1100HN is sending/receiving data through the LAN, flashing at 4 HZ with a 50% duty cycle.
		Off	The LAN is not connected or the FSG1100HN is powered off.
WPS Button	Press this button for 1 second to set up a wireless connection via WiFi Protected Setup with another WPS-enabled client. You must press the WPS button on the client side, holding the button for at least 5 seconds, for a successful connection.		

The WPS Button

2.1 Overview

Your FSG1100N 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.

Introducing the Web Configurator

3.1 Overview

This chapter describes how to access the FSG1100HN Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the FSG1100HN via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

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

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

3.2 Accessing the Web Configurator

1. Make sure your FSG1100HN hardware is properly connected and prepare your computer or computer network to connect to the FSG1100HN (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.254" as the website address.

Your computer must be in the same subnet in order to access this website address.

4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
5. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Password Screen



Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the FSG1100HN if this happens.

3.3 Resetting the FSG1100HN

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the FSG1100HN to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.254".

3.3.1 Procedure to Use the Reset Button

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the FSG1100HN.
- 3 Press the **RESET** button for longer than five seconds to set the FSG1100HN back to its factory-default configurations.

3.4 Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Status** screen.

Status Screen



Click this icon at anytime to exit the Web Configurator.

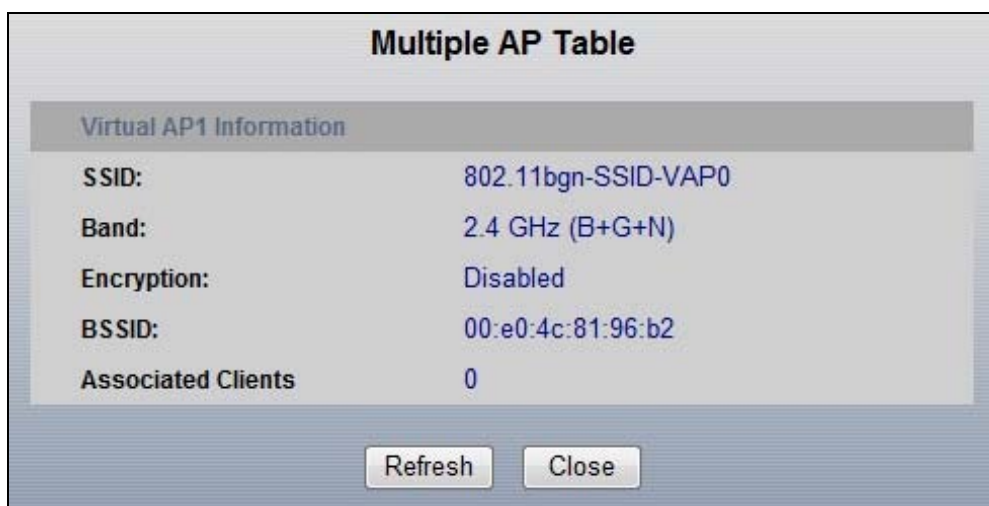
Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the System Name you enter in the Maintenance > System Settings > General screen. It is for identification purposes.
Firmware Version	This is the firmware version.
System Up Time	This is the total time the FSG1100HN has been on.
Current Date/Time	This is the FSG1100HN's present date and time.
Device Mode	This is the current FSG1100HN mode. The device can function as a Router, Bridge, or Mixed. See the Device Mode window (System Information > Device Mode) to change this setting.
WAN Information	
IP Address	This is the WAN port's IP address.
IP Subnet Mask	This is the WAN port's subnet mask.
Connection Type	This displays the connection type status.
DNS	This displays the IP address of the DNS.

LAN Information	
IP Address	This is the LAN port's IP address.
IP Subnet Mask	This is the LAN port's subnet mask.
DHCP	This is the LAN port's DHCP role, Enable or Disable .
System Status	
Interface	These are the devices three types of interfaces.
Status	This is the current status of each interface type.
CPU Usage	This displays what percentage of the FSG1100HN's processing ability is currently used. When this percentage is close to 100%, the FSG1100H 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 displays what percentage of the heap memory the FSG1100HN is using.
WLAN Information	
SSID	This is a descriptive name used to identify the FSG1100HN on the wireless LAN.
Mode	This is the level of wireless security the FSG1100HN is currently using.
Band	This is the manually selected operating frequency currently being used on the wireless LAN.
Channel Number	This is the manually selected channel number currently being used on the wireless LAN.
Encryption	This is the type of encryption security currently being used on the wireless LAN.
WPS	This displays Enabled when the WPS has been set up. This displays Disabled if the WPS has not been set up.
Multiple AP	Click the Detail hyperlink to display the Multiple AP Table.
Summary	
Active Session	Click the Detail hyperlink to display the Active Session Table.
Refresh	Click Refresh to begin configuring this screen afresh.

3.4.1 WLAN Information: Multiple AP Table

Click the Multiple AP Table [Detail](#) hyperlink in the **Status** screen. Read-only information includes SSID, Band, Encryption, BSSID, and Associated Clients.



The following table describes the multiple AP labels in this screen

Status > Multiple AP

LABEL	DESCRIPTION
SSID	This displays the Service Set Identity (SSID) associated with the AP.
Band	This displays the operating frequency for the AP. The options are: 2.4 GHz (B+G+N) for networks using a mix of 802.11b, 802.11g, and 802.11n wireless clients, 2.4 GHz (G+N) for networks using a mix of 802.11g and 802.11n wireless clients, 2.4 GHz (B+G) for networks using a mix of 802.11b and 802.11g wireless clients, 2.4 GHz (N) for networks using 802.11n wireless clients only, 2.4 GHz (G) for networks using 802.11g wireless clients only, or 2.4 GHz (B) for networks using 802.11b wireless clients only.
Encryption	This displays whether encryption is enabled or disabled.
Broadcast SSID	This displays the broadcast SSID.
Associated Clients	This displays the number of associated clients.
Refresh	Click Refresh to display the information on this screen afresh.
Close	Click Close to close this pop-up window.

3.4.2 Summary: Active Session Table

The Active Session Table displays all current active sessions.

Click **System Information > Active Session** to open the **Active Session Table** screen.

System Information > Active Session

Index	Internal	Protocol	External	NAT (Port)	Time Out (sec)
1	192.168.1.50:52641	tcp	192.168.1.1:80	52641	432000

Page:1/1 (Active Session Number:1)

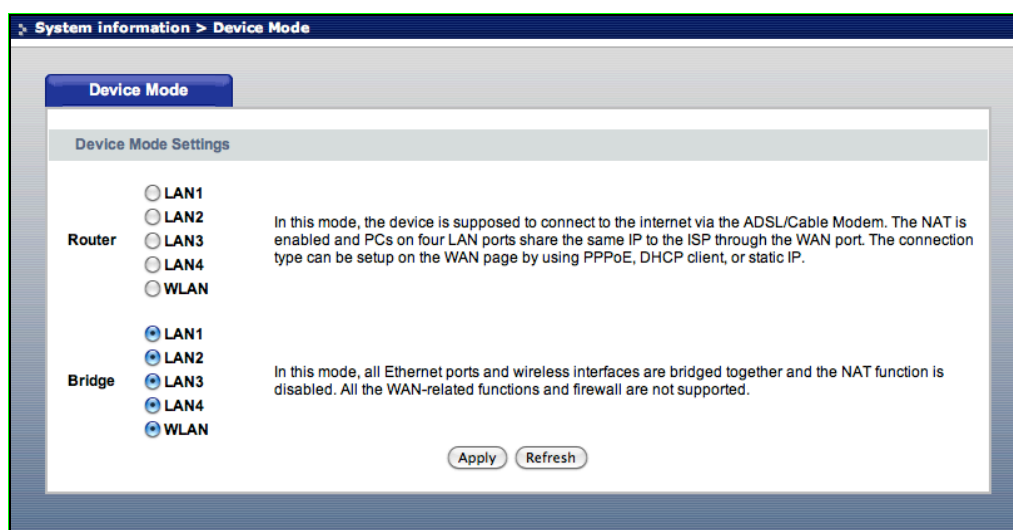
The following table describes the active session labels in this screen.

System Information > Active Session

LABEL	DESCRIPTION
Index	The index number of the active session table entry.
Internal	The internal IP address of the of the active session table entry.
Protocol	The protocol of the active session table entry.
External	The external IP address of the of the active session table entry.
NAT (Port)	The NAT port number of the active session entry.
Time Out (sec)	The time, in seconds, until the active session entry times out.
Page Up	Click to scroll up the page.
Page Down	Click to scroll down the page.
First Page	Click to advance to the first page of the table.
Last Page	Click to advance to the last page of the table.
Refresh	Click to refresh the values on the table.

3.5 Setting the Device Mode

The Device Mode window allows users to select the operating mode, Router mode, Bridge mode, or a Mixed mode employing both Router and Bridge mode. Access this window by clicking **System Information > Device Mode**.



Device Mode window

LABEL	DESCRIPTION
LAN1-LAN4	Select LAN1 to LAN4 for router, bridge, or a mix of each.
WLAN	Select WLAN for router or bridge.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

PART II

Network

Wireless LAN (30)

WAN (48)

LAN (56)

Network Address Translation (NAT) (63)

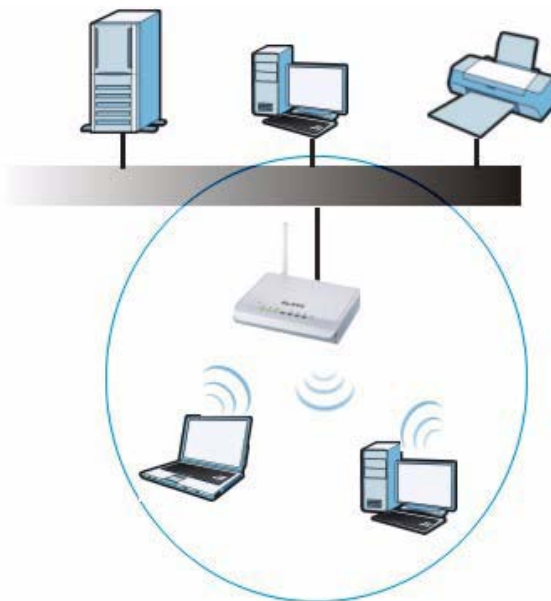
4 Wireless LAN

4.1 Overview

This chapter discusses how to configure the wireless network settings in your FSG1100HN. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Example of a Wireless Network



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

Your FSG1100HN is the AP.

4.2 What You Can Do

- Use the **Basic** screen (32) to configure the basic wireless settings, including to enable the Wireless LAN, select the band, display the currently configured multiple APs, enter the SSID, select the channel width, set the control sideband, select a channel number, enable broadcast SSID, set the data rate, and display active clients.
- Use the **Advanced** screen (35) to configure the fragment threshold, RTS threshold, preamble type, IAPP, B/G protection, frame aggregation, short GI, block intra-BSS traffic, and RF output power.
- Use the **Security** screen (37) to select and configure the wireless security mode on your wireless network.
- Use the **Access Control** screen (44) to enable access control on your wireless network.
- Use the **Wi-Fi Protected Setup** screen (44) to configure WPS on your wireless network.

4.3 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client 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 different channels.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

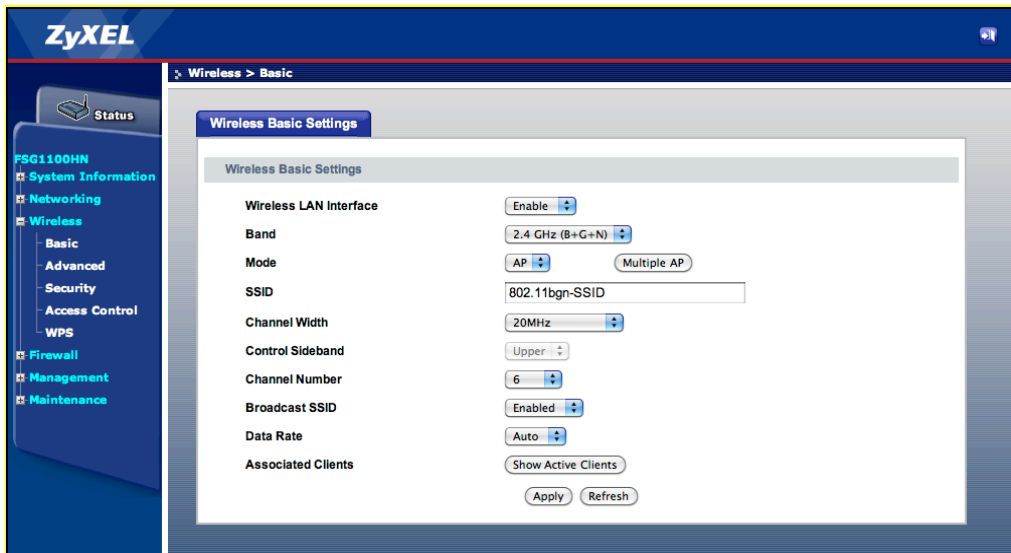
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

4.4 Wireless Basic Settings Screen

The Wireless Basic Settings window allows users to configure the Wireless LAN Interface.

Click **Wireless > Basic Settings** to open the **Wireless Basic Settings** screen.

Wireless > Basic Settings



The following table describes the basic wireless labels in this screen.

Wireless > Basic Settings

LABEL	DESCRIPTION
Wireless Basic Settings	
Wireless LAN Interface	Enable or disable the wireless LAN interface on the FSG1100HN.
Band	Choose the proper operating frequency for the wireless network. The options are: 2.4 GHz (B+G+N) for networks using a mix of 802.11b, 802.11g, and 802.11n wireless clients, 2.4 GHz (G+N) for networks using a mix of 802.11g and 802.11n wireless clients, 2.4 GHz (B+G) for networks using a mix of 802.11b and 802.11g wireless clients, 2.4 GHz (N) for networks using 802.11n wireless clients only, 2.4 GHz (G) for networks using 802.11g wireless clients only, or 2.4 GHz (B) for networks using 802.11b wireless clients only.
Mode	Choose the desired mode. The option is AP . Click the Multiple AP button to open the Multiple AP table, as shown on the next page. Up to four APs can be enabled and configured on this table.
SSID	Enter a descriptive name for the Service Set Identity (SSID) associated with the wireless station. All wireless stations associating with the access point built-in to the FSG1100HN must have the same SSID.
Channel Width	Select the channel width. Select 20MHz if no 802.11n wireless clients are being used. A standard 20 MHz channel offers transfer speeds up to 150Mbps whereas a 40 MHz channel uses two standard channels and offers speeds up to 300Mbps. As not all wireless devices support 40 MHz channels, most users select Auto 20/40MHz to allow the

	FSG1100HN to adjust the channel bandwidth automatically.
Channel Number	Select the channel number for the wireless network between 1 and 11 or select Auto to automatically scan for an active channel on the network.
Broadcast SSID	Enable or disable the broadcasting of the FSG1100HN's SSID. If this is disabled, the SSID in the outgoing beacon frame will be hidden. This prevents a station from obtaining the SSID through scanning using a site survey tool.
Data Rate	Select the data transmission rate. For best performance, it is strongly suggested to choose the default, Auto .
Associated Clients	Click the Show Active Clients button to open the Active Wireless Client Table, as shown below. This displays all current associated wireless clients.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

4.4.1 Multiple AP Table

The FSG1100HN allows up to four APs to be enabled and configured on the Multiple AP window.

Click **Wireless > Basic Settings > Multiple AP** to open the **Multiple AP** screen.

Wireless > Basic Settings > Multiple AP

Index	Enable	Band	SSID	Data Rate	Broadcast SSID	Block Intra-BSS Traffic	Active Client List
AP1	<input type="checkbox"/>	2.4 GHz (B+G+N)	802.11bgn-5	Auto	Enabled	Disable	Show
AP2	<input type="checkbox"/>	2.4 GHz (B+G+N)	802.11bgn-5	Auto	Enabled	Disable	Show
AP3	<input type="checkbox"/>	2.4 GHz (B+G+N)	802.11bgn-5	Auto	Enabled	Disable	Show
AP4	<input type="checkbox"/>	2.4 GHz (B+G+N)	802.11bgn-5	Auto	Enabled	Disable	Show

The following table describes the multiple AP labels in this screen.

Wireless > Basic Settings > Multiple AP

LABEL	DESCRIPTION
Multiple AP	
Index	The index number of the multiple AP table entry.
Enable	Tick to enable the multiple AP table entry.
Band	Select the proper operating frequency for the wireless network. The options are: 2.4 GHz (B+G+N) for networks using a mix of 802.11b, 802.11g, and 802.11n wireless clients, 2.4 GHz (G+N) for networks using a mix of 802.11g and 802.11n wireless clients, 2.4 GHz (B+G) for networks using a mix of 802.11b and 802.11g wireless clients, 2.4 GHz (N) for networks using 802.11n wireless clients only, 2.4 GHz (G) for networks using 802.11g wireless clients only, or 2.4 GHz (B) for networks using 802.11b wireless clients only.
SSID	Enter a Service Set Identity (SSID) associated with the wireless station. All wireless stations associating with the access point

	built-in to the FSG1100HN must have the same SSID.
Data Rate	Select the data transmission rate. For best performance, it is strongly suggested to choose the default, Auto .
Broadcast SSID	Enable or disable the broadcasting of the FSG1100HN's SSID. If this is disabled, the SSID in the outgoing beacon frame will be hidden. This prevents a station from obtaining the SSID through scanning using a site survey tool.
Block Intra-BSS Traffic	Enable this feature to prevent clients on each WLAN from being able to ping each other.
Active Client List	Click the Show button to display the Active Wireless Client Table window for AP1, AP2, AP3, or AP4.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.
Close	Click Close to close this pop-up window.

4.4.2 Active Wireless Client Table

The Active Wireless Client Table displays all current associated wireless clients.

Click **Wireless > Basic Settings > Show Active Clients** to open the **Active Wireless Client Table** screen.

Wireless > Basic Settings > Show Active Clients

Active Wireless Client Table						
MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---	---

The following table describes the active wireless client labels in this screen

Wireless > Basic Settings > Show Active Clients

LABEL	DESCRIPTION
MAC Address	The MAC address of the wireless client.
Mode	The current mode of the wireless client.
Tx Packet	The number of packets transmitted by this wireless client.
Rx Packets	The number of packets received by this wireless client.
Tx Rate (Mbps)	The packet transmitted rate in Mbps.
Power Saving	The current power saving setting on this wireless client.
Expired Time(s)	The time before this wireless client times out.
Refresh	Click Refresh to begin configuring this screen afresh.
Close	Click Close to close this pop-up window.

4.5 Wireless Advanced Settings Screen

The Wireless Advanced Settings window allows users to configure the Wireless LAN Interface.

Click **Wireless > Advanced Settings** to open the **Wireless Advanced Settings** screen.

Wireless > Advanced Settings

The following table describes the advanced wireless labels in this screen

Wireless > Advanced Settings

LABEL	DESCRIPTION
Wireless Advanced Settings	
Fragment Threshold	This is the threshold, specified in bytes, for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Packets exceeding the 2346-byte setting will be fragmented before transmission. Enter an even number between 256 and 2346. 2346 is the default.
RTS Threshold	Data with its frame size larger than this value will perform the Request To Send (RTS)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347. 0 means always send RTS.
Preamble Type	Choose either Long Preamble or Short Preamble . A preamble affects the timing in the wireless network. There are two preamble types: long and short. If a wireless device uses a different preamble type than the FSG1100HN, then it cannot communicate with the FSG1100HN.
IAPP	Enable or disable Inter-Access Point Protocol (IAPP). This protocol is designed for the enforcement of unique association throughout the Extended Service Set and for the secure exchange of a wireless station's security context between a current AP and a new AP during the handoff period.
B/G Protection	Enable or disable B/G Protection. This feature limits cross-talk in a mixed 802.11b and 802.11g environment.
Frame Aggregation	Enable or disable Frame Aggregation. This feature increases throughput by sending two or more data frames in a single transmission.

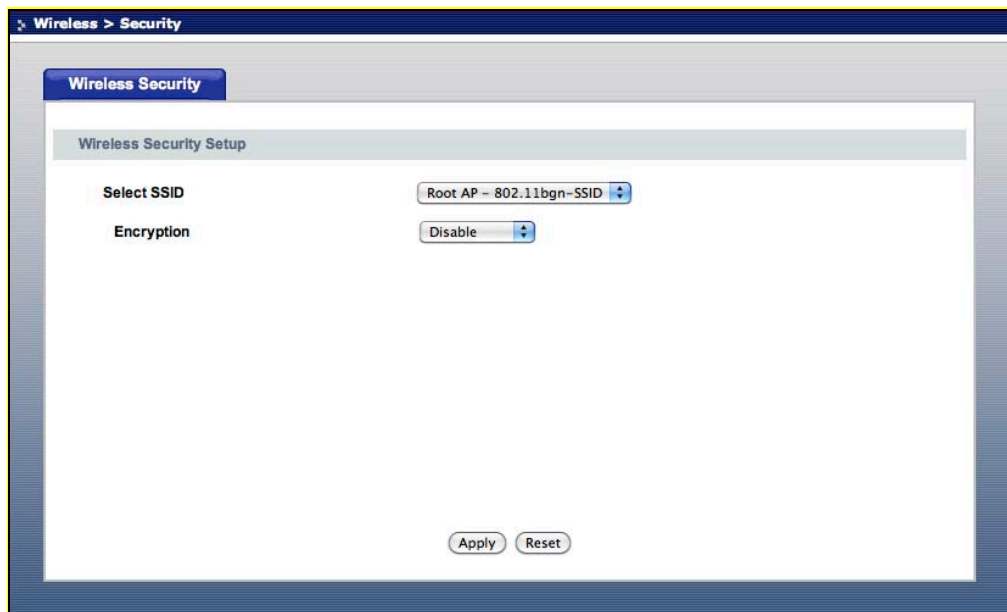
Short GI	Enable or disable Short Guard Interval (GI). Enabling this feature reduces the guard interval time thereby increasing data capacity. The drawback is that it can be less reliable and may create higher data loss.
Block Intra-BSS Traffic	Enable or disable Intra-BSS Traffic. A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point. Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client A and B can still access the wired network but cannot communicate with each other.
RF Output Power	Select the transmit power of the antennas. The default is 100%.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

4.6 Wireless Security Screen

The Wireless Security Setup window allows users to configure WEP, WPA, WPA2, and WPA-Mixed encryption.

Click **Wireless > Security** to open the **Wireless Security** screen.

Wireless > Security



The following table describes the wireless security labels in this screen

Wireless > Security

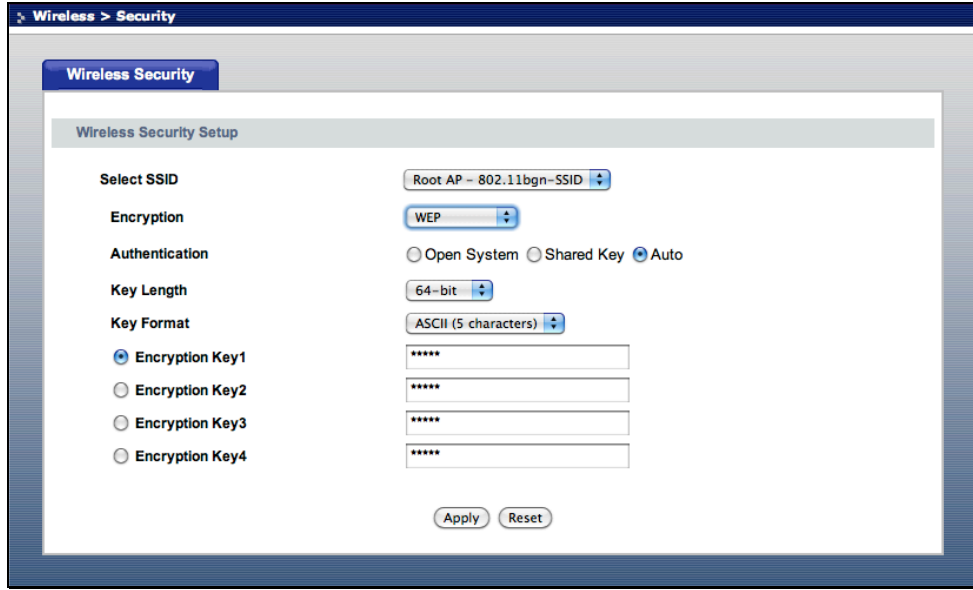
LABEL	DESCRIPTION
Wireless Security Setup	
Select SSID	Select the desired Service Set Identity (SSID).
Encryption	Choose from the following encryption options: WEP , WPA , WPA2 , WPA-Mixed , and Disable . The default is Disable .
Apply	Click Apply to save your changes back to the FSG1100HN.
Reset	Click Reset the settings on this screen.

4.6.1 WEP

Wired Equivalent Privacy (WEP) is an encryption security option based on IEEE 802.11 that uses the RC4 encryption algorithm. WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key. The FSG1100HN allows configuration of up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

Click Wireless > Security > WEP to open the Wireless Security WEP screen.

Wireless > Security > WEP



The following table describes the wireless security for WEP labels in this screen

Wireless > Security > WEP

LABEL	DESCRIPTION
Wireless Security Setup	
Select SSID	Select the desired Service Set Identity (SSID).
Encryption	Choose the encryption security type, WEP . The other encryption security options are: WPA , WPA2 , WPA-Mixed , and Disable . The default is Disable .
Authentication	Select Open System , Shared Key , or Auto authentication. Auto is the default. This specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Most users keep this setting at Auto or Open System unless they want to force a key verification before communication between the wireless client and the FSG1100HN occurs. Selecting Shared Key forces clients to provide the WEP key prior to communication.
Key Length	Select the level of encryption, 64-bit or 128-bit .
Key Format	Select ASCII (5 characters) or Hex (10 characters) . American Standard Code for Information Interchange (ASCII) is a system using alphanumeric characters. ASCII strings are automatically converted to hexadecimal format for use over a network. Hex uses the actual hexadecimal format based on the numbers 0 to 9 and the letters A to F.
Encryption Key 1 to 4	Keys are used to encrypt data. Both the FSG1100HN and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit , then enter any five ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). At least one key must be configured and up to four keys overall can be configured. However, only one key can be activated at any single time. The default key is Encryption Key 1 .
Apply	Click Apply to save your changes back to the FSG1100HN.
Reset	Click Reset to reset the settings on this screen.

4.6.2 WPA

Wi-Fi Protected Access (WPA) is an encryption security option designed to improve upon the features of WEP. It employs Temporal Key Integrity Protocol (TKIP) to scramble the keys using a hash algorithm and, by adding an integrity-checking feature, ensures that the keys have not been tampered with. WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate wireless connections. The key is an alphanumeric password between 8 and 63 characters long. The password can also be symbols (!?*&_) and spaces. In addition, WPA/WPA2 includes Extensible Authentication Protocol (EAP) to ensure only authorized network users can access the network.

Click **Wireless > Security > WPA** to open the **Wireless Security WPA** screens.

Wireless > Security > WPA

The screenshot shows the 'Wireless Security Setup' window for WPA (Personal (Pre-Shared Key)). The window title is 'Wireless > Security' and the sub-header is 'Wireless Security'. The main content area is titled 'Wireless Security Setup'. The settings are as follows:

- Select SSID: Root AP - 802.11bgn-SSID
- Encryption: WPA
- Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)
- WPA Cipher Suite: TKIP AES
- Pre-Shared Key Format: Passphrase
- Pre-Shared Key: (empty text field)

At the bottom of the window are 'Apply' and 'Reset' buttons.

Wireless Security Setup window for WPA (Personal (Pre-Shared Key))

The screenshot shows the 'Wireless Security Setup' window for WPA (Enterprise (RADIUS)). The window title is 'Wireless > Security' and the sub-header is 'Wireless Security'. The main content area is titled 'Wireless Security Setup'. The settings are as follows:

- Select SSID: Root AP - 802.11bgn-SSID
- Encryption: WPA
- Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)
- WPA Cipher Suite: TKIP AES
- RADIUS Server IP Address: (empty text field)
- RADIUS Server Port: 1812
- RADIUS Server Password: (empty text field)

At the bottom of the window are 'Apply' and 'Reset' buttons.

Wireless Security Setup window for WPA (Enterprise (RADIUS))

The following table describes the wireless security for WPA labels in these screens.

Wireless > Security > WPA

LABEL	DESCRIPTION
Wireless Security Setup	
Select SSID	Select the desired Service Set Identity (SSID).
Encryption	Choose the encryption security type, WPA . The other encryption security options are: WEP , WPA2 , WPA-Mixed , and Disable . The default is Disable .
Authentication Mode	Select Enterprise (RADIUS) or Personal (Pre-Shared Key) authentication. Personal (Pre-Shared Key) is the default.
WPA Cipher Suite	Tick the Cipher Suite type, TKIP or AES .
Pre-Shared Key Format	Select the PSK format, Passphrase or HEX – 64 characters .
Pre-Shared Key	Enter a simple common password for the PSK. The pre-shared key is from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or less than 64 case-sensitive HEX characters ("0-9", "A-F").
RADIUS Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Server Port	Enter the port number being used with the RADIUS server. 1812 is the default port.
RADIUS Server Password	Enter the security key for the RADIUS server.
Apply	Click Apply to save your changes back to the FSG1100HN.
Reset	Click Reset to reset the settings on this screen.

4.6.3 WPA2

Click **Wireless > Security > WPA2** to open the **Wireless Security WPA2** screens.

Wireless > Security > WPA2

The screenshot shows the 'Wireless Security Setup' window for WPA2 (Personal (Pre-Shared Key)). The window title is 'Wireless > Security'. The main content area is titled 'Wireless Security Setup'. It contains the following fields and options:

- Select SSID:** Root AP - 802.11bgn-SSID
- Encryption:** WPA2
- Authentication Mode:** Enterprise (RADIUS) Personal (Pre-Shared Key)
- WPA2 Cipher Suite:** TKIP AES
- Pre-Shared Key Format:** Passphrase
- Pre-Shared Key:** (Empty text input field)

At the bottom of the window are 'Apply' and 'Reset' buttons.

Wireless Security Setup window for WPA2 (Personal (Pre-Shared Key))

The screenshot shows the 'Wireless Security Setup' window for WPA2 (Enterprise (RADIUS)). The window title is 'Wireless > Security'. The main content area is titled 'Wireless Security Setup'. It contains the following fields and options:

- Select SSID:** Root AP - 802.11bgn-SSID
- Encryption:** WPA2
- Authentication Mode:** Enterprise (RADIUS) Personal (Pre-Shared Key)
- WPA2 Cipher Suite:** TKIP AES
- RADIUS Server IP Address:** (Empty text input field)
- RADIUS Server Port:** 1812
- RADIUS Server Password:** (Empty text input field)

At the bottom of the window are 'Apply' and 'Reset' buttons.

Wireless Security Setup window for WPA2 (Enterprise (RADIUS))

The following table describes the wireless security for WPA2 labels in these screens.

Wireless > Security > WPA2

LABEL	DESCRIPTION
Wireless Security Setup	
Select SSID	Select the desired Service Set Identity (SSID).
Encryption	Choose encryption security type WPA2 . The other encryption security options are: WEP , WPA , WPA-Mixed , and Disable . The default is Disable .
Authentication Mode	Select Enterprise (RADIUS) or Personal (Pre-Shared Key) authentication. Personal (Pre-Shared Key) is the default.
WPA2 Cipher Suite	Tick the Cipher Suite type, TKIP or AES .
Pre-Shared Key Format	Select the PSK format, Passphrase or HEX – 64 characters .
Pre-Shared Key	Enter a simple common password for the PSK. The pre-shared key is from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or less than 64 case-sensitive HEX characters ("0-9", "A-F").
RADIUS Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Server Port	Enter the port number being used with the RADIUS server. 1812 is the default port.
RADIUS Server Password	Enter the security key for the RADIUS server.
Apply	Click Apply to save your changes back to the FSG1100HN.
Reset	Click Reset to reset the settings on this screen.

4.6.4 WPA-Mixed

Click **Wireless > Security > WPA-Mixed** to open the **Wireless Security WPA-Mixed** screens.

Wireless > Security > WPA-Mixed



Wireless Security Setup window for WPA-Mixed (Personal (Pre-Shared Key))

The screenshot shows the 'Wireless Security Setup' window. The 'Authentication Mode' is set to 'Enterprise (RADIUS)'. Under 'WPA Cipher Suite', 'TKIP' is checked. Under 'WPA2 Cipher Suite', 'TKIP' is checked. The 'RADIUS Server Port' is set to '1812'. There are 'Apply' and 'Reset' buttons at the bottom.

Wireless Security Setup window for WPA-Mixed (Personal (Enterprise (RADIUS)))

The following table describes the wireless security for WPA-Mixed labels in these screens.

Wireless > Security > WPA-Mixed

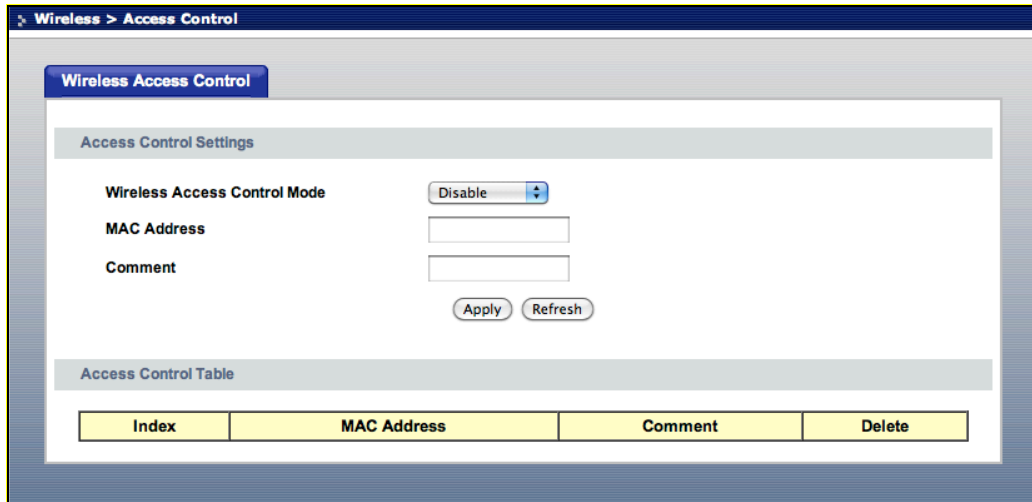
LABEL	DESCRIPTION
Wireless Security Setup	
Select SSID	Select the desired Service Set Identity (SSID).
Encryption	Choose the encryption security type, WPA-Mixed . The other encryption security options are: WEP , WPA , WPA2 , and Disable . The default is Disable .
Authentication Mode	Select Enterprise (RADIUS) or Personal (Pre-Shared Key) authentication. Personal (Pre-Shared Key) is the default.
WPA Cipher Suite	Tick the Cipher Suite type, TKIP or AES .
WPA2 Cipher Suite	Tick the Cipher Suite type, TKIP or AES .
Pre-Shared Key Format	Select the PSK format, Passphrase or HEX – 64 characters .
Pre-Shared Key	Enter a simple common password for the PSK. The pre-shared key is from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or less than 64 case-sensitive HEX characters ("0-9", "A-F").
RADIUS Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Server Port	Enter the port number being used with the RADIUS server. 1812 is the default port.
RADIUS Server Password	Enter the security key for the RADIUS server.
Apply	Click Apply to save your changes back to the FSG1100HN.
Reset	Click Reset to reset the settings on this screen.

4.7 Wireless Access Control Screen

The Wireless Access Control window allows users to configure wireless access control by creating a white list and a black list. This allows administrators to block users or only allow approved users to make a connection.

Click **Wireless > Access Control** to open the **Wireless Access Control** screen.

Wireless > Access Control



The following table describes the wireless access control labels in this screen.

Wireless > Access Control

LABEL	DESCRIPTION
Access Control Settings	
Wireless Access Control Mode	Select Allow Listed , Deny Listed , or Disable .
MAC Address	Enter a MAC address.
Comment	Enter a user-specified comment to help identify this access control rule.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.
Delete	Click button to delete the table entry.

4.8 Wi-Fi Protected Setup Screen

The Wi-Fi Protected Setup window allows users to quickly set up a wireless network with strong security, without having to configure security settings manually. WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. Depending on the devices on the network, users can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves.

Click **Wireless > WPS** to open the **Wi-Fi Protected Setup** screen.

Wireless > WPS

The following table describes the WPS labels in this screen.

Wireless > WPS

LABEL	DESCRIPTION
WPS Settings	
Active	Enable or Disable the WPS feature. Click Apply to commit the setting. Click Refresh to display current settings of the window.
WPS Summary	
WPS Configured	This indicates when the FSG1100HN has connected to a wireless network using WPS or when the Active setting is Enable and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the window. This displays No if WPS is disabled and there are no wireless or wireless security changes on the FSG1100HN or if the user clicks the Reset to Unconfigured button to remove the configured wireless and wireless security settings.
WPS SSID	Displays the Service Set Identity name.
WPS Security Mode	Indicates the current WPS security mode.
WPS Encryp Type	Indicates the current WPS encryption type.
WPS Default Key Index	Indicates the current WPS default key.
AP PIN	Indicates the access point personal identification number.
WPS Action	
PIN	Enter the personal identification number and then click the Configure via PIN button. This is commonly known as the PIN method of setting up WPS.

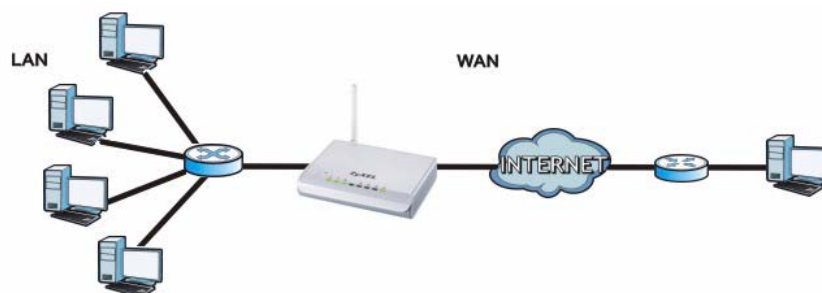
PBC	Push Button Configuration (PBC) allows users to click the Configure via PBC button to set up WPS. Once the button is clicked on this window, users have 2 minutes to press a similar virtual or actual button on the new wireless client device.
-----	---

5.1 Overview

This chapter discusses the FSG1100HN's **WAN** screens. Use these screens to configure your FSG1100HN for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

LAN and WAN



5.2 What You Can Do

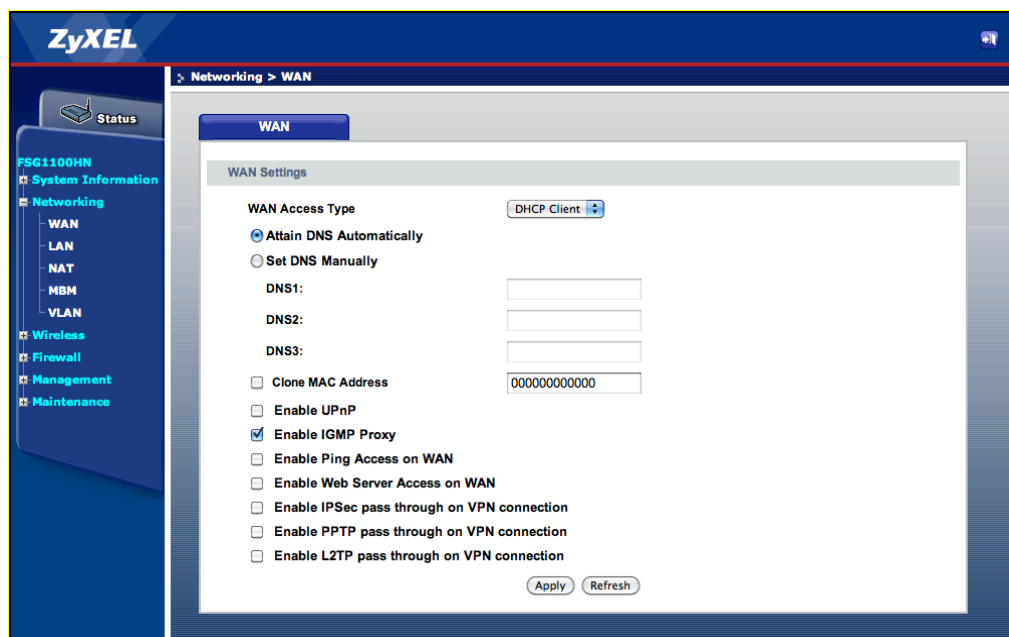
- Use the **WAN** screen for DHCP Client (49) to enter your ISP information and set up a DHCP client.
- Use the **WAN** screen for Static IP (51) to enter your IP address, subnet, default gateway (if applicable), and other settings to set up a static IP.
- Use the **WAN** screen for PPPoE (53) to set up PPPoE.

5.3 WAN for DHCP Client Screen

Dynamic Host Configuration Protocol (DHCP), based on RFC 2131 and RFC 2132, allows individual clients to obtain TCP/IP configuration at start-up from a server. Users can configure the FSG1100HN's LAN as a DHCP server or disable it. When configured as a server, the FSG1100HN provides the TCP/IP configuration for the clients. If DHCP service is disabled, another DHCP server must be available on that network, or the computer will need to be manually configured.

Click **Networking > WAN > DHCP Client** to open the **WAN** screen for DHCP Client (the default WAN screen).

Networking > WAN > DHCP Client



The following table describes the WAN DHCP client labels in this screen.

Networking > WAN > DHCP Client

LABEL	DESCRIPTION
WAN Settings	
WAN Access Type	Choose DHCP Client . The other options are Static IP or PPPoE .
Attain DNS Automatically	Click to attain DNS automatically. Otherwise, enter DNS manually using the field below.
Set DNS Manually	Enter the DNS server IP address(es) assigned by the ISP.
DNS1-DNS3	Enter the DNS server IP address(es) assigned by the ISP.
Clone MAC Address	Enable MAC address cloning.
Enable UPnP	Enable the Universal Plug and Play (UPnP) feature. 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.
Enable IGMP Proxy	Enable the IGMP proxy feature. IGMP proxy enables the device to issue IGMP host messages on behalf of hosts that

	the device discovered through standard IGMP interfaces.
Enable Ping Access on WAN	Enable the Ping access on WAN feature. This allows Ping to use the WAN to send ICMP echo request packets to the target host and listen for ICMP echo response replies.
Enable Web Server Access on WAN	Enable the Web server access on WAN feature. This allows Web server access via the WAN.
Enable IPSec Pass Through on VPN Connection	Enable the IPSec Pass Through on VPN connection feature. This encapsulates a complete IP datagram, forming a virtual tunnel between IPSec-capable devices.
Enable PPTP Pass Through on VPN Connection	Enable the PPTP Pass Through on VPN connection feature. Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN).
Enable L2TP Pass Through on VPN Connection	Enable the L2TP Pass Through on VPN connection feature. Layer 2 Tunneling Protocol (L2TP) is used to support data transfer through a Virtual Private Network (VPN). It relies on an encryption protocol that it passes within the tunnel to provide privacy.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

5.4 WAN for Static IP Screen

Select Static IP if the WAN port IP information is provided by the ISP. Users will need to enter the IP address, subnet mask, gateway address, and DNS(es) provided by the ISP.

Click **Networking > WAN > Static IP** to open the **WAN** screen for Static IP.

Networking > WAN > Static IP

The screenshot shows the WAN Settings configuration page. The 'WAN Access Type' is set to 'Static IP'. The IP Address is 10.0.0.250, Subnet Mask is 255.255.255.0, and Default Gateway is 10.0.0.254. There are three empty fields for DNS1, DNS2, and DNS3. The 'Clone MAC Address' field contains 000000000000. The 'Enable IGMP Proxy' checkbox is checked. Other options like 'Enable UPnP', 'Enable Ping Access on WAN', and various VPN pass-through options are unchecked. 'Apply' and 'Refresh' buttons are located at the bottom right of the form.

The following table describes the WAN static IP labels in this screen.

Networking > WAN > Static IP

LABEL	DESCRIPTION
WAN Settings	
WAN Access Type	Choose Static IP . The other options are DHCP Client or PPPoE .
IP Address	The WAN IP address is an IP address for the FSG1100HN, which makes it accessible from an outside network. It is used to communicate with other devices on other networks. If this static WAN IP address has been assigned by the ISP, it should also assign the subnet mask and DNS server IP address(es). A default gateway IP address may also be provided.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the default gateway IP address.
DNS1-DNS3	Enter the DNS server IP address(es) assigned by the ISP.
Clone MAC Address	Enable MAC address cloning.
Enable UPnP	Enable the Universal Plug and Play (UPnP) feature. 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.
Enable IGMP Proxy	Enable the IGMP proxy feature. IGMP proxy enables the device to issue IGMP host messages on behalf of hosts that the device discovered through standard IGMP interfaces.
Enable Ping Access on WAN	Enable the Ping access on WAN feature. This allows Ping to use the WAN to send ICMP echo request packets to the target host and listen for ICMP echo response replies.
Enable Web Server Access on WAN	Enable the Web server access on WAN feature. This allows Web server access via the WAN.
Enable IPSec Pass Through on VPN Connection	Enable the IPSec Pass Through on VPN connection feature. This encapsulates a complete IP datagram, forming a virtual tunnel between IPSec-capable devices.
Enable PPTP Pass Through on VPN Connection	Enable the PPTP Pass Through on VPN connection feature. Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN)
Enable L2TP Pass Through on VPN Connection	Enable the L2TP Pass Through on VPN connection feature. Layer 2 Tunneling Protocol (L2TP) is used to support data transfer through a Virtual Private Network (VPN). It relies on an encryption protocol that it passes within the tunnel to provide privacy.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

5.5 WAN for PPPoE Screen

Point-to-Point Protocol over Ethernet (PPPoE) emulates a dial-up connection. It allows an ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the FSG1100HN is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving users the need to manage PPPoE clients on individual computers.

Click **Networking > WAN > PPPoE** to open the **WAN** screen for PPPoE.

The screenshot shows the WAN Settings configuration page. The 'WAN Access Type' is set to 'PPPoE'. The 'User Name' and 'Password' fields are empty. 'Connection Type' is set to 'Continuous', with 'Connect' and 'Disconnect' buttons. 'Idle Time' is set to '5' minutes. Under 'DNS Settings', 'Set DNS Manually' is selected, with empty fields for DNS1, DNS2, and DNS3. A 'Clone MAC Address' checkbox is checked with the value '000000000000'. Other checkboxes include 'Enable UPnP', 'Enable IGMP Proxy' (checked), 'Enable Ping Access on WAN', 'Enable Web Server Access on WAN', 'Enable Multicast Shortcut', 'Enable IPSec pass through on VPN connection', 'Enable PPTP pass through on VPN connection', and 'Enable L2TP pass through on VPN connection'. 'Apply' and 'Refresh' buttons are at the bottom.

The following table describes the WAN PPPoE labels in this screen.

Networking > WAN > PPPoE

LABEL	DESCRIPTION
WAN Settings	
WAN Access Type	Choose PPPoE . The other options are DHCP Client or Static IP .
User Name	Enter the user name provided by the ISP.
Password	Enter the password associated with the user name above.
Connection Type	Select Continuous , Connect on Demand , or Manual . If Manual is selected, users will need to manually click Connect and Disconnect to use the Internet. If Connect on Demand is selected, users need to enter an Idle Time value in the next field.
Idle Time	Enter an age-out value, in minutes, between 1 and 1000.

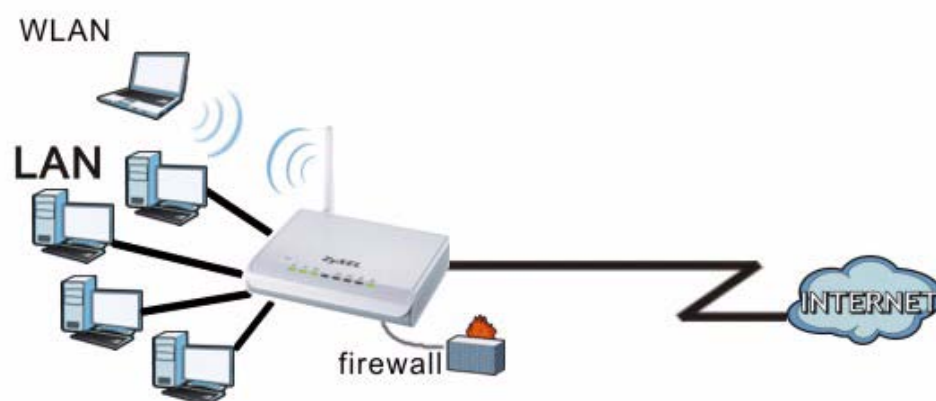
Attain DNS Automatically	Click to attain DNS automatically. Otherwise, enter DNS manually using the field below.
Set DNS Manually	Enter the DNS server IP address(es) assigned by the ISP.
DNS1-DNS3	Enter the DNS server IP address(es) assigned by the ISP.
Clone MAC Address	Enable MAC address cloning.
Enable UPnP	Enable the Universal Plug and Play (UPnP) feature. 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.
Enable IGMP Proxy	Enable the IGMP proxy feature. IGMP proxy enables the device to issue IGMP host messages on behalf of hosts that the device discovered through standard IGMP interfaces.
Enable Ping Access on WAN	Enable the Ping access on WAN feature. This allows Ping to use the WAN to send ICMP echo request packets to the target host and listen for ICMP echo response replies.
Enable Web Server Access on WAN	Enable the Web server access on WAN feature. This allows Web server access via the WAN.
Enable Multicast Shortcut	Enable the Multicast shortcut feature. 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. The FSG1100HN supports both IGMP version 1 and IGMP version 2. At start up, the FSG1100HN queries all directly connected networks to gather group membership. After that, it periodically updates this information.
Enable IPsec Pass Through on VPN Connection	Enable the IPsec Pass Through on VPN connection feature. This encapsulates a complete IP datagram, forming a virtual tunnel between IPsec-capable devices.
Enable PPTP Pass Through on VPN Connection	Enable the PPTP Pass Through on VPN connection feature. Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN).
Enable L2TP Pass Through on VPN Connection	Enable the L2TP Pass Through on VPN connection feature. Layer 2 Tunneling Protocol (L2TP) is used to support data transfer through a Virtual Private Network (VPN). It relies on an encryption protocol that it passes within the tunnel to provide privacy.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

6.1 Overview

This chapter describes how to configure LAN settings.

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, manage IP addresses, and partition your physical network into logical networks.

LAN Setup



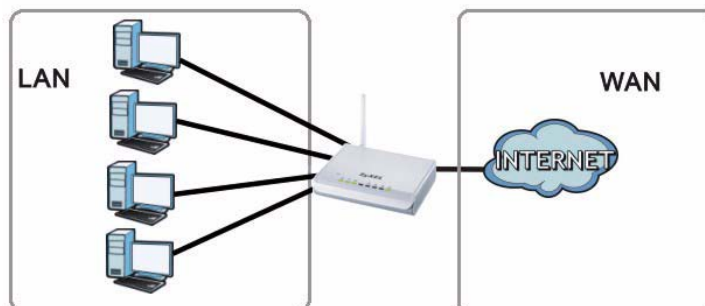
6.2 What You Can Do

- Use the **LAN General** screen (58) to change your basic LAN settings.
- Use the **VLAN** screen (61) to configure VLAN settings.

6.3 What You Need To Know

The actual physical connection determines whether the FSG1100HN 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.

LAN and WAN IP Addresses



The LAN parameters of the FSG1100HN are preset in the factory with the following values:

- IP address of 192.168.1.254 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

6.3.1 IP Pool Setup

The FSG1100HN is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the FSG1100HN itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

6.3.2 LAN TCP/IP

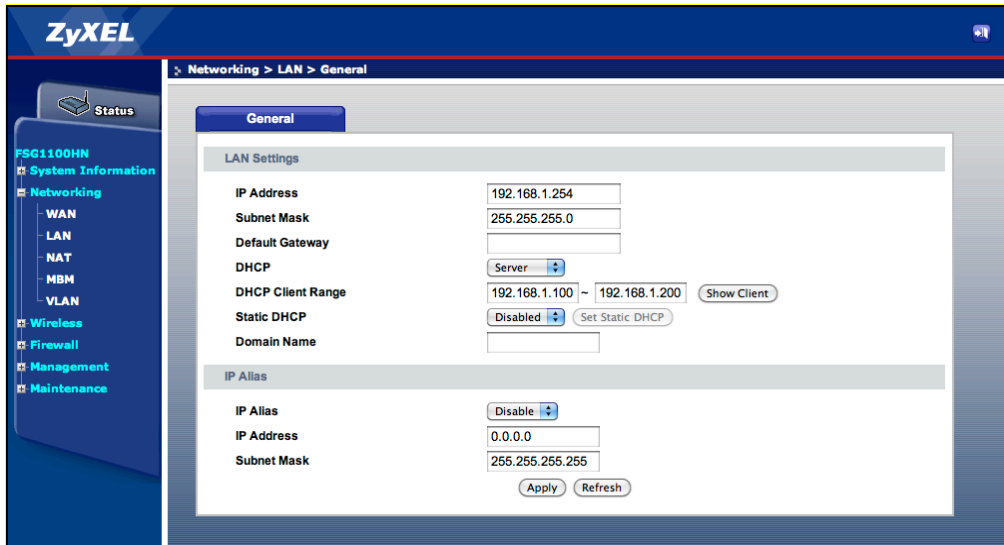
The FSG1100HN has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

6.4 LAN General Screen

The LAN window General tab allows users to configure and display LAN settings. 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 windows can help users configure a LAN DHCP server, manage IP addresses, and partition the physical network into logical networks.

Click **Networking > LAN > General** to open the **LAN** screen.

Networking > LAN > General



The following table describes the LAN general labels in this screen.

Networking > LAN > General

LABEL	DESCRIPTION
LAN Settings	
IP Address	Enter the (LAN) IP address of the FSG1100HN in dotted decimal notation 192.168.1.254 (factory default).
Subnet Mask	The subnet mask specifies the network number portion of an IP address. The FSG1100HN will automatically calculate the subnet mask based on the IP address assigned by the user. Unless a user is implementing subnetting, use the subnet mask computed by the FSG1100HN. Enter the subnet mask in dotted decimal notation.
Default Gateway	Enter a default gateway IP address. This is for use with a DHCP server (see the next field).
DHCP	Select Server , Client , or Disabled . If Server is selected, assign a range of IP addresses below in the DHCP Client Range fields and an IP address for the Default Gateway field above.
DHCP Client Range	When Server is selected, assign a range of contiguous IP addresses. Click Show Client to display the read-only Active DHCP Client Table displayed on the next page.
Static DHCP	Enable or Disable static DHCP. To set up static DHCP,

	Enable this setting and click Set Static DHCP . Select an Index between 1 and 20, enter an IP Address, a MAC Address, and an optional identifying Comment in the Static DHCP window displayed on the next page.
Domain Name	Enter the domain name. If this is left blank, the ISP may assign a domain name via DHCP.
IP Alias	
IP Alias	Choose Enable to configure the LAN network for the FSG1100HN.
IP Address	Enter the IP address of the FSG1100HN in dotted decimal notation.
Subnet Mask	The FSG1100HN will automatically calculate the subnet mask based on the IP address assigned by the user.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

6.4.1 Active DHCP Client Table

The Active DHCP Client Table provides users a view of the current DHCP clients, including IP address, MAC address, and the amount of time before the entry expires.

Click **Networking > LAN > Show Client** to open the **Active DHCP Client Table** screen.

Networking > LAN > Show Client

Index	IP Address	MAC Address	Time Left (sec)
---	---	---	---

Refresh Close

The following table describes the active DHCP client labels in this screen.

Networking > LAN > Show Client

LABEL	DESCRIPTION
Index	The index number of the static table entry.
IP Address	The LAN IP address of a computer on the LAN.
MAC Address	The MAC address of a computer on the LAN.
Time Left (sec)	The amount of time, in seconds, before the static table entry expires
Refresh	Click Refresh to begin configuring this screen afresh.
Close	Click Close to close this pop-up window.

6.4.2 Static DHCP

The Static DHCP window allows users to set up static DHCP on the FSG1100HN. Select an index between 1 and 20, enter an IP address, a MAC Address, and an optional identifying comment. A Static DHCP List at the bottom of the window displays the current static DHCP entries.

Click **Networking > LAN > Set Static DHCP** to open the **Static DHCP** screen.

Networking > LAN > Set Static DHCP

The following table describes the static DHCP labels in this screen.

Networking > LAN > Set Static DHCP

LABEL	DESCRIPTION
Static DHCP Setup	
IP Address	Enter the LAN IP address of a computer on the LAN.
MAC Address	Enter the MAC address (with colons) of a computer on the LAN.
Comment	Enter identifying information for this static DHCP table entry.
Add	Click Add to add an entry to the Static DHCP List.
Refresh	Click Refresh to begin configuring this screen afresh.
Index	An index number for the Static DHCP List entry (row).
Delete	Click button to delete the table entry.

6.5 VLAN Screen

The VLAN screen allows users to configure VLAN settings.

Click **Networking > VLAN** to open the **VLAN** screen.

Networking > VLAN

Index	Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1-4090)	Priority	CFI
1	<input type="checkbox"/>	Ethernet Port1	LAN	<input type="checkbox"/>	100	0	<input type="checkbox"/>
2	<input type="checkbox"/>	Ethernet Port2	LAN	<input type="checkbox"/>	101	0	<input type="checkbox"/>
3	<input type="checkbox"/>	Ethernet Port3	LAN	<input type="checkbox"/>	102	0	<input type="checkbox"/>
4	<input type="checkbox"/>	Ethernet Port4	LAN	<input type="checkbox"/>	103	0	<input type="checkbox"/>
5	<input type="checkbox"/>	Wireless Primary AP	LAN	<input type="checkbox"/>	104	0	<input type="checkbox"/>
6	<input type="checkbox"/>	Virtual AP1	LAN	<input type="checkbox"/>	105	0	<input type="checkbox"/>
7	<input type="checkbox"/>	Virtual AP2	LAN	<input type="checkbox"/>	106	0	<input type="checkbox"/>
8	<input type="checkbox"/>	Virtual AP3	LAN	<input type="checkbox"/>	107	0	<input type="checkbox"/>
9	<input type="checkbox"/>	Virtual AP4	LAN	<input type="checkbox"/>	108	0	<input type="checkbox"/>
10	<input type="checkbox"/>	Ethernet Port5	WAN	<input type="checkbox"/>	109	0	<input type="checkbox"/>

The following table describes the VLAN labels in this screen.

Networking > VLAN

LABEL	DESCRIPTION
VLAN Settings	
VLAN	Enable or disable VLANs.
Index	An index number for the VLAN entry (row)
Enable	Tick to enable the VLAN entry.
Ethernet/Wireless	This column displays the VLAN's interface.
WAN/LAN	This column displays whether the VLAN entry is a LAN or WAN.
Tag	Tick to tag the VLAN.
VID (1~4090)	Enter a VLAN ID between 1 and 4090.
Priority	Select a priority between 0 and 7 .
CFI	Tick the Canonical Format Indicator (CFI). This is used to determine whether a network is Ethernet or Token Ring.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

7 NAT

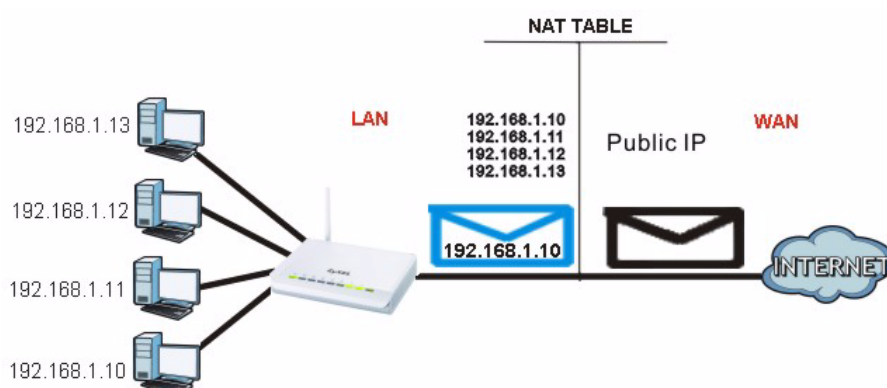
7.1 Overview

This chapter discusses how to configure NAT on the FSG1100HN.

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

Each packet has two addresses – a source address and a destination address. For outgoing packets, 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 in each packet and then forwards it to the Internet. The FSG1100HN keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

NAT Example



For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the FSG1100HN.

7.2 What You Can Do

- Use the **NAT General** screen (64) to enable NAT, NAT loopback, SIP ALG, and RTSP ALG.
- Use the **NAT DMZ** screen (66) to change your FSG1100HN's DMZ settings.
- Use the **NAT Port Forwarding** screen (67) change your FSG1100HN's port forwarding settings.

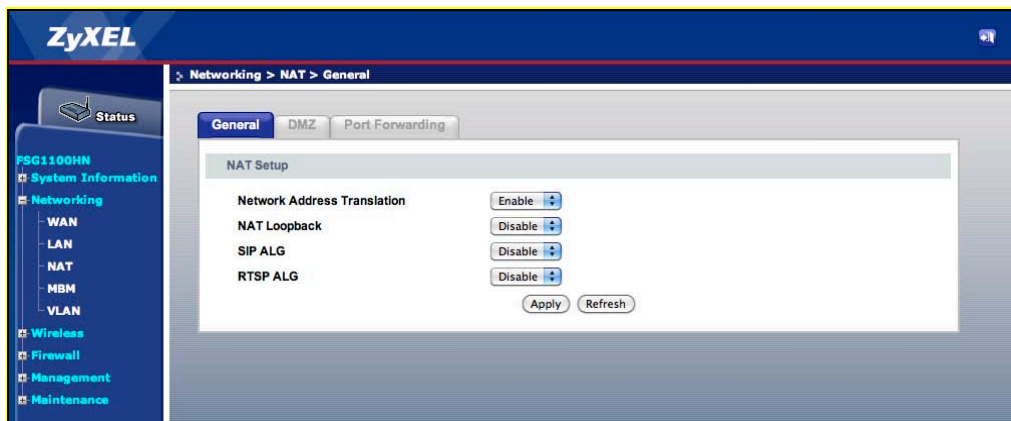
7.3 NAT General Screen

The NAT window General tab allows users to configure NAT settings. NAT (Network Address Translation – NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

Each packet has two addresses – a source address and a destination address. For outgoing packets, 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 in each packet and then forwards it to the Internet. The FSG1100HN keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

Click **Networking > NAT > General** to open the **NAT General** screen.

Networking > NAT > General



The following table describes the NAT general labels in this screen.

Networking > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Network Address Translation	Enable or Disable Network Address Translation (NAT). NAT allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
NAT Loopback	Enable or Disable NAT Loopback. NAT Loopback allows users on the LAN side to access a public server located on the LAN side by a public IP address or domain name.
SIP ALG	Enable or Disable SIP ALG. SIP Application Level Gateway (ALG) allows VoIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When a VoIP device behind the FSG1100HN registers with the SIP register server, the FSG1100HN translates the device's private IP address inside the SIP data stream to a public IP address.
RTSP ALG	Enable or Disable RTSP ALG. Application Level Gateway (ALG). This is designed to dynamically open pinholes for media streaming. When disabled, you are limited to static NAT only.

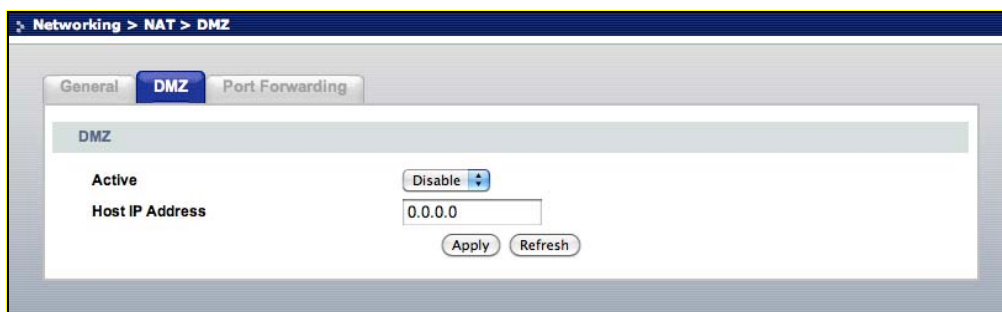
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

7.4 NAT DMZ Screen

Demilitarized Zone (DMZ) allows one IP address to be exposed to the Internet. This is useful for special-purpose services such as Internet gaming or video conferencing. However, as any user on the Internet can access in/out data from the DMZ host, care should be taken when using this feature to minimize security issues.

Click **Networking > NAT > DMZ** to open the **NAT DMZ** screen.

Networking > NAT > DMZ



The following table describes the NAT DMZ labels in this screen.

Networking > NAT > DMZ

LABEL	DESCRIPTION
DMZ	
Active	Enable or Disable DMZ.
Host IP Address	Enter an IP address that will be open to the Internet.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

7.5 NAT Port Forwarding Screen

Port forwarding allows users to define the local servers to which incoming services will be forwarded by creating a firewall between the internal network and the Internet. A tunnel is created so that computers on the Internet can communicate to computers on a user's LAN through a single port. This is useful for running Web servers, game servers, FTP servers, and video conferencing and is more secure than DMZ. A common example is one computer running a Web server on port 80 and another computer running an FTP server on port 23, each with the same IP address.

Click **Networking > NAT > Port Forwarding** to open the **Port Forwarding** screen.

Networking > NAT > Port Forwarding

The following table describes the NAT Port Forwarding labels in this screen.

Networking > NAT > Port Forwarding

LABEL	DESCRIPTION
Port Forwarding	
Active	Enable or Disable port forwarding. Enabling this setting allows forwarding to a host with a specified internal IP address.
Port Range	Enter the port number(s) to be forwarded.
Protocol	Select TCP , UDP , or Both . This is protocol of the traffic allowed to be forwarded by this feature.
IP Address	Enter the inside IP address of the server that receives packets from ports specified in the Port Range above.
Comment	This is a user-selected name or other information about a specific port forwarding entry in the Forward Table.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.
Index	An index number for the Forward Table entry (row).
Delete	Click button to delete the table entry.

PART III

Security

Firewall (71)

8 Firewall

Overview

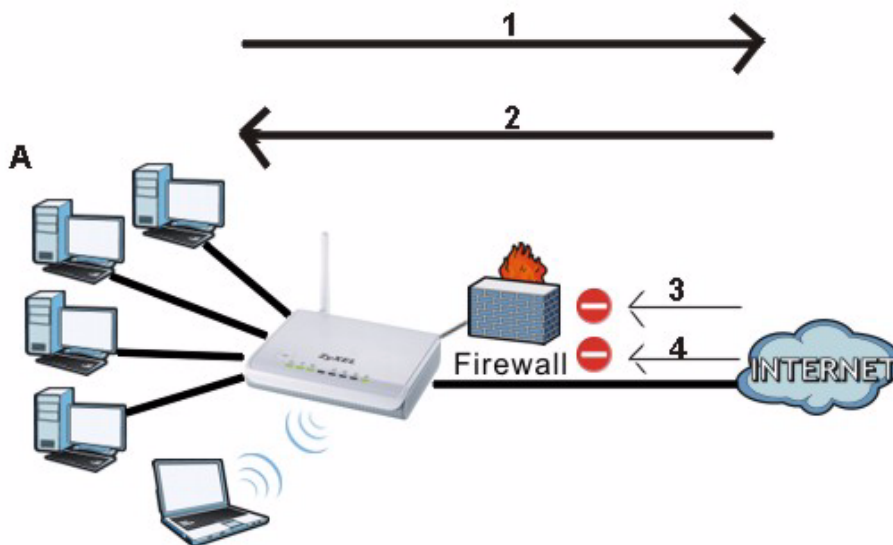
Use these screens to enable and configure the firewall that protects your FSG1100HN and your LAN from unwanted or malicious traffic.

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).

Default Firewall Action



8.1 What You Can Do

- Use the **Firewall Filter** screen (73) to enable or disable the FSG1100HN's firewall.
- Use the **Firewall Filter Add** screen (74) to add a filter to the FSG1100HN firewall.
- Use the **Firewall Denial of Service** screen (75) to enable and configure Denial of Service Prevention.
- Use the **Firewall Content Filter** screen (75) to restrict Web features, add keywords for blocking, and designate a trusted computer.

8.2 What You Need To Know

The FSG1100HN's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific Web sites. For example, you can configure one policy that blocks John Doe's access to arts and entertainment Web pages.

8.2.1 About the FSG1100HN Firewall

The FSG1100HN firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The FSG1100HN's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The FSG1100HN can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The FSG1100HN is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The FSG1100HN has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

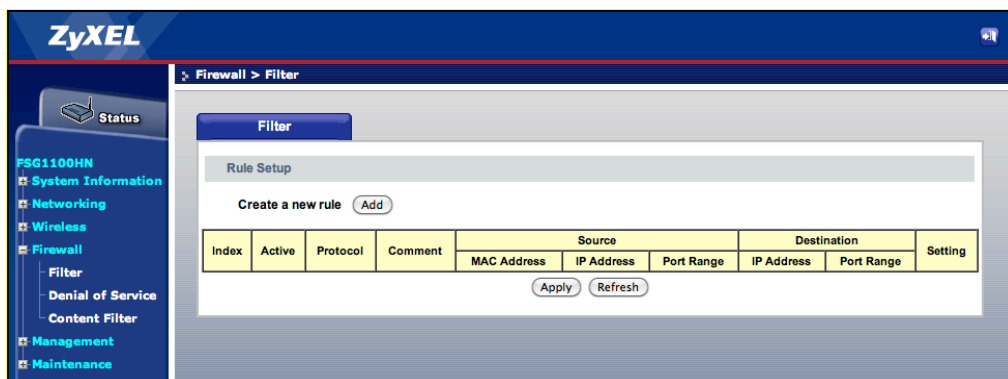
The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

8.3 Firewall Filter Screen

The Filter window allows users to view existing filters on the FSG1100HN. To set up a new filter, click the **Add** button.

Click **Firewall > Filter** to open the **Filter** screen.

Firewall > Filter



The following table describes the filter labels in this screen.

Firewall > Filter

LABEL	DESCRIPTION
Rule Setup	
Index	Displays filter index number.
Active	Displays current filter status.
Protocol	Displays the current filter protocol setting.
Comment	Displays information to help identify the port filter and any special circumstances related to it.
Source	Displays the current MAC address, IP address, and port range of the source filter.
Destination	Displays the current IP address and port range of the destination filter.
Setting	Displays the current filter settings.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

8.4 Firewall Filter Add Screen

The Rule Configuration screen allows users to set up filtering rules.

Click **Firewall > Filter > Add** to open the **Rule Configuration** screen.

Firewall > Filter > Add

The screenshot shows the 'Rule Configuration' screen with the following fields and controls:

- Active:** A dropdown menu currently set to 'Disable'.
- Protocol:** A dropdown menu currently set to 'TCP+UDP'.
- Comment:** A text input field.
- Source:**
 - MAC Address:** A text input field.
 - IP Address:** A text input field.
 - Subnet Mask:** A text input field.
 - Port Range:** Two text input fields separated by a tilde (~), with '(1-65535)' as a hint.
- Destination:**
 - IP Address:** A text input field.
 - Subnet Mask:** A text input field.
 - Port Range:** Two text input fields separated by a tilde (~), with '(1-65535)' as a hint.

At the bottom of the form are three buttons: 'Apply', 'Refresh', and 'Back'.

The following table describes the filter labels in this screen.

Firewall > Filter > Add

LABEL	DESCRIPTION
Rule Configuration	
Active	Enable or disable filtering.
Protocol	Select which protocol to use to filter incoming packets: Both , TCP , UDP , or Any .
Comment	Enter information to help identify the filter and any special circumstances related to it.
Source -- MAC Address	Enter the source MAC address of the device to be filtered. MAC filtering allows users to filter network access by machines based on the unique MAC address of their network adapter. It is most useful to prevent unauthorized wireless devices from connecting to a wireless network. A MAC address is a unique identification assigned by manufacturers of network adapters.
Source -- IP Address/Subnet Mask	Enter the source IP address and subnet mask of the device to be filtered.
Source -- Port Range	Enter the range of ports to be filtered between 1 and 65535.
Destination -- IP Address/Subnet Mask	Enter the destination IP address and subnet mask of the device to be filtered.

Destination -- Port Range	Enter the range of ports to be filtered between 1 and 65535.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.
Back	Click Back to return to the main Filter screen.

8.5 Firewall Denial of Service Screen

The Denial of Service screen allows users to prevent various types of Denial of Service attacks.

Click **Firewall > Denial of Service** to open the **Denial of Service** screen.

Firewall > Denial of Service

The screenshot shows the 'Denial of Service' configuration window. It contains the following settings:

- Enable DoS Prevention
- Whole System Flood: SYN (0 Packets/Second)
- Whole System Flood: FIN (0 Packets/Second)
- Whole System Flood: UDP (0 Packets/Second)
- Whole System Flood: ICMP (0 Packets/Second)
- Per-Source IP Flood: SYN (0 Packets/Second)
- Per-Source IP Flood: FIN (0 Packets/Second)
- Per-Source IP Flood: UDP (0 Packets/Second)
- Per-Source IP Flood: ICMP (0 Packets/Second)
- TCP/UDP PortScan (Low Sensitivity)
- ICMP Smurf
- IP Land
- IP Spoof
- IP TearDrop
- PingOfDeath
- TCP Scan
- TCP SYNWithData
- UDP Bomb
- UDP EchoChargen
- Enable Source IP Blocking (0 Block time (sec))

Buttons at the bottom: Select All, Clear All, Apply, Refresh.

The following table describes the denial of service labels in this screen.

Firewall > Denial of Service

LABEL	DESCRIPTION
Denial of Service	
Enable DoS Prevention	Enable Denial of Service Prevention.

Whole System Flood: SYN	Tick to enable whole system flooding for SYN DoS prevention.
Whole System Flood: FIN	Tick to enable whole system flooding for FIN DoS prevention.
Whole System Flood: UDP	Tick to enable whole system flooding for UDP DoS prevention.
Whole System Flood: ICMP	Tick to enable whole system flooding for ICMP DoS prevention.
Per-Source IP Flood: SYN	Tick to enable per-source IP flooding for SYN DoS prevention.
Per-Source IP Flood: FIN	Tick to enable per-source IP flooding for FIN DoS prevention.
Per-Source IP Flood: UDP	Tick to enable per-source IP flooding for UDP DoS prevention.
Per-Source IP Flood: ICMP	Tick to enable per-source IP flooding for ICMP DoS prevention.
TCP/UDP PortScan	Tick to enable TCP/UDP port scan for DoS prevention and select a Sensitivity of Low or High .
ICMP Smurf	Tick to enable ICMP DoS prevention.
IP Land	Tick to enable IP Land DoS prevention.
IP Spoof	Tick to enable IP Spoof DoS prevention.
IP TearDrop	Tick to enable IP Tear Drop DoS prevention.
PingOfDeath	Tick to enable Ping of Death DoS prevention.
TCP Scan	Tick to enable TCP Scan DoS prevention.
TCP SynWithData	Tick to enable TCP SYN with data DoS prevention.
UDP Bomb	Tick to enable UDP Bomb DoS prevention.
UDP EchoChargen	Tick to enable Echo Chargen DoS prevention.
Enable Source IP Blocking	Tick to enable Source IP blocking DoS prevention and enter a blocking time in seconds.
Select All	Click to select all of the DoS types on this screen.
Clear All	Click to deselect all the DoS types ticked on this screen.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

8.6 Firewall Content Filter Screen

The Content Filter screen allows users to restrict Web features, add keywords for blocking, and designate a trusted computer. A content filtering profile conveniently stores your custom settings for the following features.

Restrict Web Features

The FSG1100HN can disable Web proxies and block Web features such as ActiveX controls, Java applets, and cookies.

Keyword Blocking URL Checking

The FSG1100HN checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

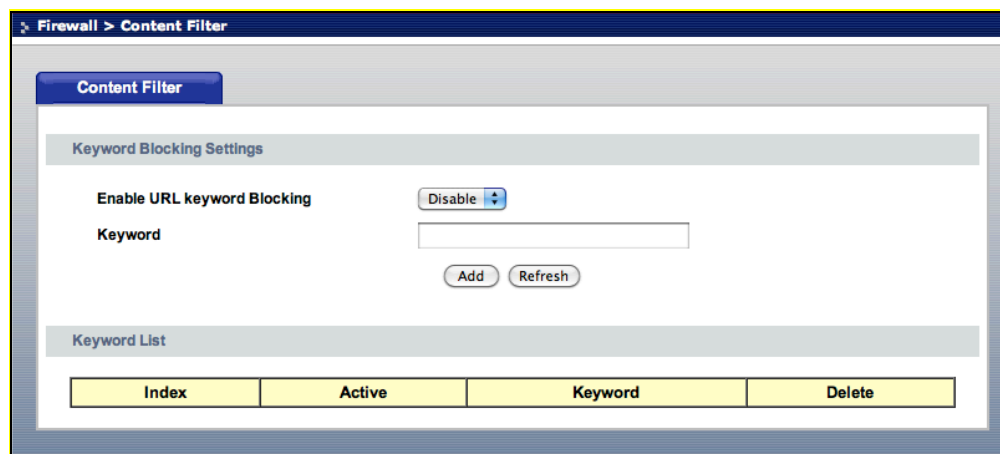
The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the FSG1100HN checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the FSG1100HN would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

Click **Firewall > Content Filter** to open the **Content Filter** screen.

Firewall > Content Filter



The following table describes the content filter labels in this screen.

Firewall > Content Filter

LABEL	DESCRIPTION
Keyword Blocking Settings	
Enable URL Keyword Blocking	The FSG1100HN can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select Enable to enable this feature.

Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Add	Click Add after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a Web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Refresh	Click Refresh to begin configuring this screen afresh.
Keyword List	
Index	An index number for the Keyword List Table entry (row).
Active	This column indicates if this entry is active or not.
Keyword	The keyword for this table entry.
Delete	Click button to delete the table entry.

PART IV

Management

Bandwidth Maintenance (82)

TR-069 (85)

Auto Provision (88)

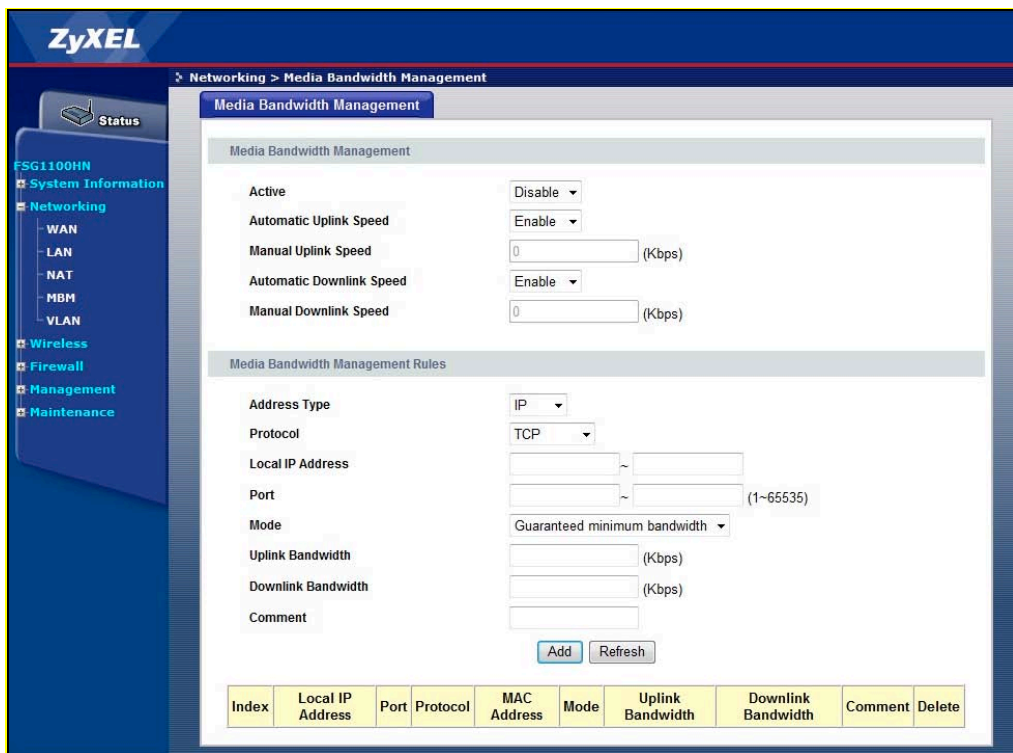
Media Bandwidth Management

9.1 Media Bandwidth Management Screen

The Media Bandwidth Management screen allows users to configure bandwidth rules for pre-defined services or applications.

Click **Networking > MBM** to open the **Media Bandwidth Management** screen.

Networking > MBM



The following table describes the media bandwidth management labels in this screen.

Networking > MBM

LABEL	DESCRIPTION
Media Bandwidth Management	
Active	Enable or Disable the bandwidth maintenance feature.
Automatic Uplink Speed	Enable or Disable automatic uplink speed.
Manual Uplink Speed	Enter the uplink speed in Kbps.
Automatic Downlink Speed	Enable or Disable automatic downlink speed.
Manual Downlink Speed	Enter the downlink speed in Kbps.
Media Bandwidth Management Rules	
Address Type	Choose IP or MAC .

Protocol	Select the protocol: TCP , UDP , TCP/UDP , ICMP , or Any .
Local IP Address	Enter the IP address of the computer to which the bandwidth rule does not apply.
Port	This is the range of ports for which the bandwidth rule applies.
Mode	Choose Guaranteed minimum bandwidth or Restricted maximum bandwidth .
Uplink Bandwidth	Enter the uplink bandwidth in Kbps.
Downlink Bandwidth	Enter the downlink bandwidth in Kbps.
Comment	This is a user-selected name or other information about this rule.
Add	Click Add to add the settings configured in the current session back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.
Index	An index number for the Media Bandwidth Management table entry (row).
MAC Address	Displays the MAC address of the Media Bandwidth Management table entry.
Delete	Click button to delete the table entry.

10

TR-069

10.1 TR-069 General Screen

The TR-069 General tab allows users to configure a TR-069 Auto-Configuration Server (ACS).

Click **Management > TR-069 > General** to open the **TR-069 General** screen.

Management > TR-069 > General

The following table describes the TR-069 general labels in this screen.

Management > TR-069 > General

LABEL	DESCRIPTION
ACS	
ACS URL	Enter the URL of the ACS.
User Name	Enter the user name for the ACS.
Password	Enter the password for the ACS.
Periodic Inform Active	Enable or disable the Periodic Inform Active feature.
Periodic Inform Interval	Enter a value for the Periodic Inform Interval.
Connection Request	
User Name	Enter a user name.
Password	Enter a password.
Action	
Auto Execution	Enable or Disable auto execution. If enabled, when the device reboots, TR-069 will be automatically enabled.
Apply	Click Apply to save your changes back to the FSG1100HN.

Refresh

Click **Refresh** to begin configuring this screen afresh.

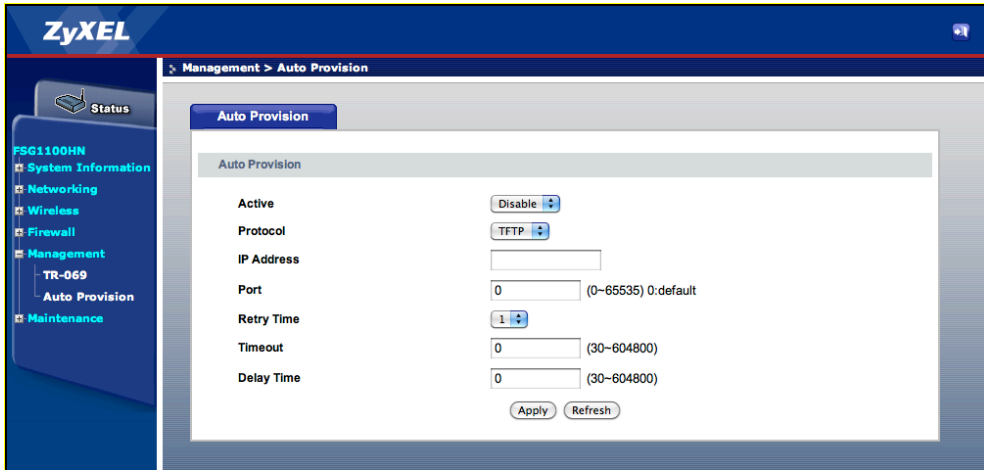
11 Auto Provision

11.1 Auto Provision Screen

The Auto Provision screen allows automatic updating of configurable settings for configuration files and image files via TFTP, FTP server, or HTTP server.

Click Management > Auto Provision to open the Auto Provision screen.

Management > Auto Provision



The following table describes the auto provision labels in this screen.

Management > Auto Provision

LABEL	DESCRIPTION
Auto Provision	
Active	Enable or Disable the automatic provision feature.
Protocol	Select the provision method: TFTP , FTP , or HTTP .
IP Address	Enter the IP address to be used in auto provisioning.
Port	Enter the port to be used in auto provisioning.
Retry Time	Select the number of retry attempts allowed. The range is from 0 to 5 attempts.
Timeout	Enter an age-out value, in seconds, between 30 and 604800.
Delay Time	Enter a delay time, in seconds, between 30 and 604800.
Apply	Click Apply to save your changes back to the FSG1100HN.

Refresh

Click **Refresh** to begin configuring this screen afresh.

PART V

Maintenance

and

Troubleshooting

System Settings (93)

Log (98)

Tools (100)

12 System Settings

12.1 System Settings General Screen

The System Settings screen's General tab allows users to enter a name to identify the FSG1100HN on the network, configure the administrator inactivity timer, and set the system password.

Click **Maintenance > System Settings > General** to open the **System Settings General** screen.

Maintenance > System Settings > General

The following table describes the system settings general labels in this screen.

Maintenance > System Settings > General

LABEL	DESCRIPTION
System Setup	
System Name	System Name is a unique name to identify the FSG1100HN in an Ethernet network. 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.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The range is 10 to 9999 seconds. The default is 10 seconds. 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 Setup	Change your FSG1100HN's password (recommended) using the fields as shown.
Old	Type the default password or the existing password you use to

Password	access the system in this field. The default password of the FSG1100HN is "1234".
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

12.2 System Settings Dynamic DNS Screen

Dynamic Domain Name System (DDNS) allows the use of a domain name with a dynamic IP address.

Click **Maintenance > System Settings > Dynamic DNS** to open the **System Settings Dynamic DNS** screen.

Maintenance > System Settings > Dynamic DNS



The following table describes the system settings dynamic DNS labels in this screen.

Maintenance > System Settings > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Enable or Disable Dynamic DNS (DDNS).
Service Provider	The DDNS Service Provider supported by the Gateway is www.dyndns.org.
Host Name	Enter a Host Name in this field.
User Name	Enter a User Name in this field.
Password	Enter the assigned Password in this field.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

12.3 System Settings Time Screen

The System Settings' Time tab allows time, date, and time zone configuration, including use of an NTP Server and setting up DST on the FSG1100HN.

Click **Maintenance > System Settings > Time** to open the **System Settings Time** screen.

Maintenance > System Settings > Dynamic DNS

The following table describes the system settings time labels in this screen.

Maintenance > System Settings > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your FSG1100HN. Each time you reload this page, the FSG1100HN synchronizes the time with the time server.
Current Date	This field displays the date of your FSG1100HN. Each time you reload this page, the FSG1100HN synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
NTP Client	To enable the system to get time settings from an NTP Server, click NTP Client. Next, either click an NTP Server from the list provided or click the second radio button and manually enter the IP address of another NTP Server.

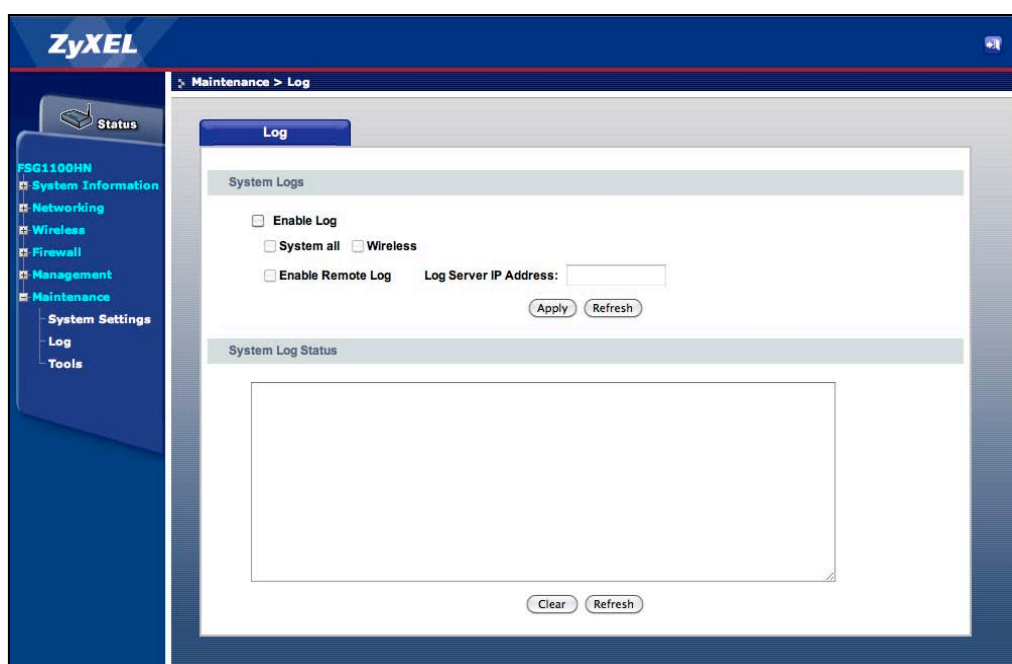
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, April and type 2 in the o'clock field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March. The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Daylight Savings. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Last, Sunday, October and type 2 in the o'clock field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October. The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to begin configuring this screen afresh.

13.1 Log Screen

The Log screen allows users to configure and display system logs.

Click **Maintenance > Log** to open the **Log** screen.

Maintenance > Log



The following table describes the system settings log labels in this screen.

Maintenance > Log

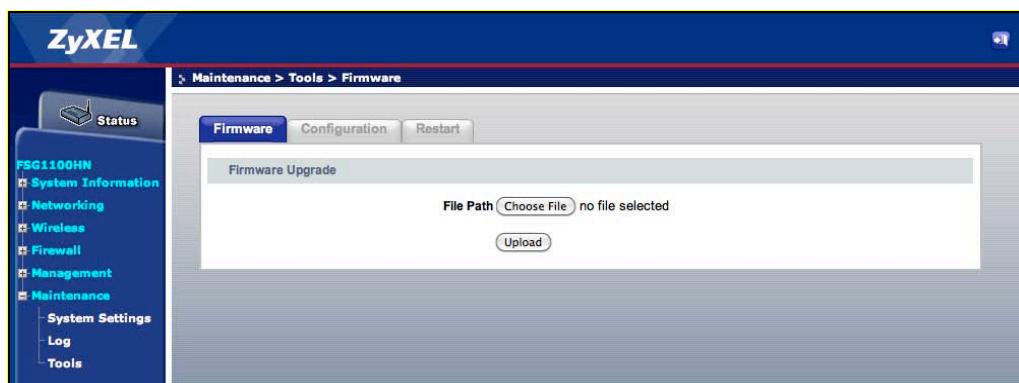
LABEL	DESCRIPTION
Enable Log	Tick to enable the system log.
System All	Tick to enable all types of system logs.
Wireless	Tick to enable the wireless system log.
Enable Remote Log	Tick to enable a remote system log. A valid Log Server IP Address must also be entered in the accompanying field.
Log Server IP Address	Enter a valid IP address in the field provided and tick the Enable Remote Log check box to use the remote log feature.
Apply	Click Apply to save your changes back to the FSG1100HN.
Refresh	Click Refresh to renew the log screen.
Clear	Click Clear to delete all the logs.

14.1 Tools Firmware Screen

This screen allows users to upgrade firmware.

Click **Maintenance > Tools > Firmware** to open the **Firmware** screen.

Maintenance > Tools > Firmware



Tools window – Firmware tab

The following table describes the tools firmware labels in this screen.

Maintenance > Tools > Firmware

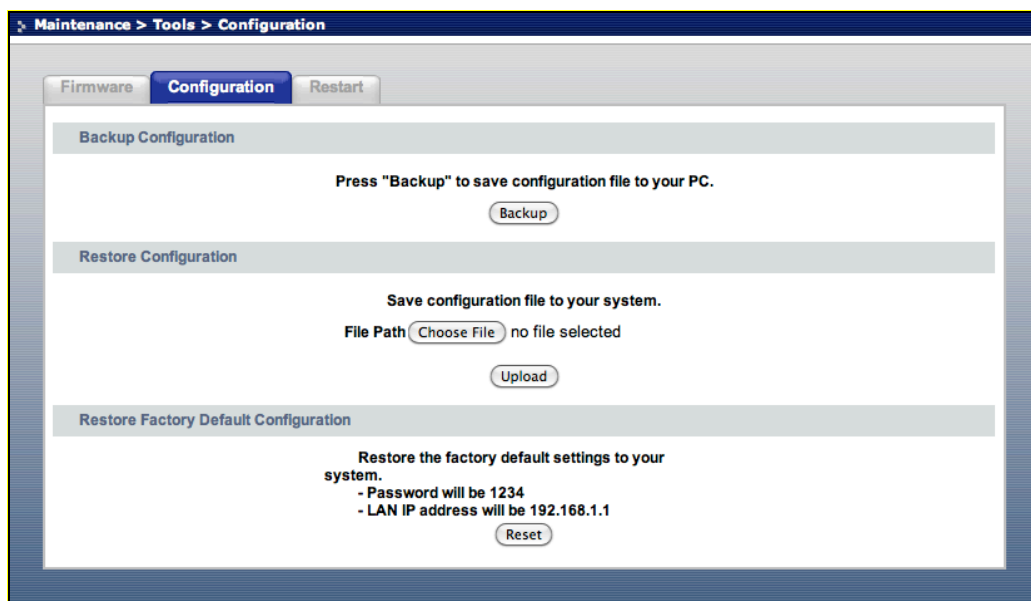
LABEL	DESCRIPTION
Firmware Upgrade	
Choose File	Click to choose the file name and file path of the configuration file to be restored.
Upload	Click to restore the selected configuration file.

14.2 Tools Configuration Screen

This tab allows users to backup configuration, restore configuration, and restore factory default configuration.

Click **Maintenance > Tools > Configuration** to open the **Configuration** screen.

Maintenance > Tools > Configuration



The following table describes the tools configuration labels in this screen.

Maintenance > Tools > Configuration

LABEL	DESCRIPTION
	Backup Configuration - Allows you to back up (save) the FSG1100HN's current configuration to a file on your computer. Once your FSG1100HN 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.
Backup	Click Backup to save the FSG1100HN's current configuration to your computer.
	Restore Configuration - Allows you to upload a new or previously saved configuration file from your computer to your FSG1100HN.
Choose File	Click Choose File 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.
	Restore Factory Default Configuration
Reset	Pressing the Reset button in this section clears all user-entered configuration information and returns the FSG1100HN to its factory defaults. You can also press the RESET button on the rear panel to reset the factory defaults of your FSG1100HN.

14.3 Tools Restart Screen

This tab allows users to restart the system.

Click **Maintenance > Tools > Restart** to open the **Restart** screen.

Maintenance > Tools > Restart



Tools window – Restart tab

Click **Restart** to reboot the FSG1100HN.

The following table describes the tools restart label in this screen.

Maintenance > Tools > Restart

LABEL	DESCRIPTION
Restart	
Restart	Click to have the FSG1100HN reboot. This does not effect the FSG1100HN's configuration.

PART VI

Appendices

[Pop-up Windows, JavaScripts and Java Permissions \(106\)](#)

[IP Addresses and Subnetting \(114\)](#)

[Setting up Your Computer's IP Address \(124\)](#)

[Wireless LANs \(142\)](#)

[Services \(154\)](#)

[Legal Information \(158\)](#)

A Pop-up Windows, JavaScripts and Java Permissions

In order to use the Web Configurator you need to allow:

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

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

Internet Explorer Pop-up Blockers

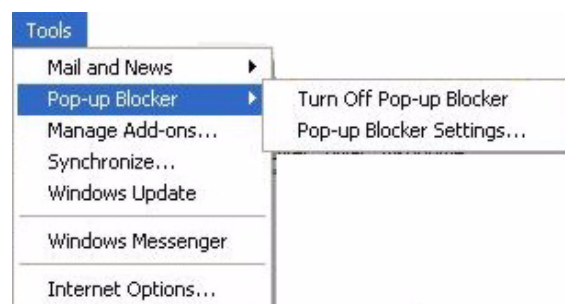
You may have to disable pop-up blocking to log into your device.

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

Disable pop-up Blockers

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

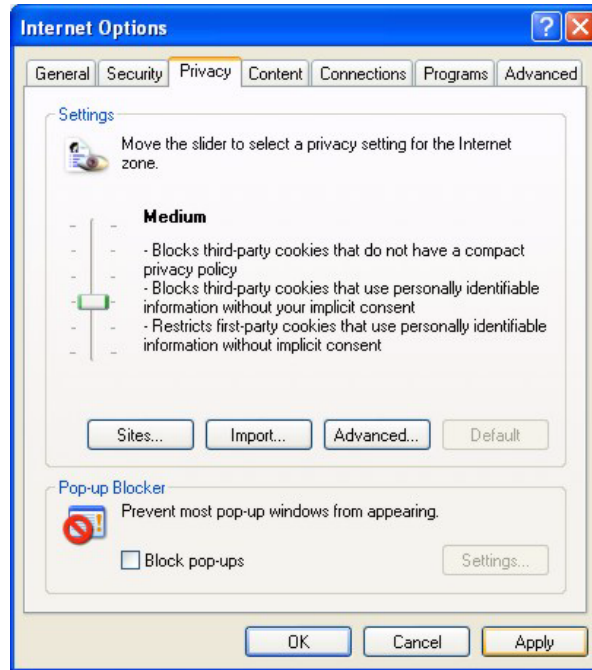
Pop-up Blocker



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

- 2 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 3 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Internet Options: Privacy



- 4 Click **Apply** to save this setting.

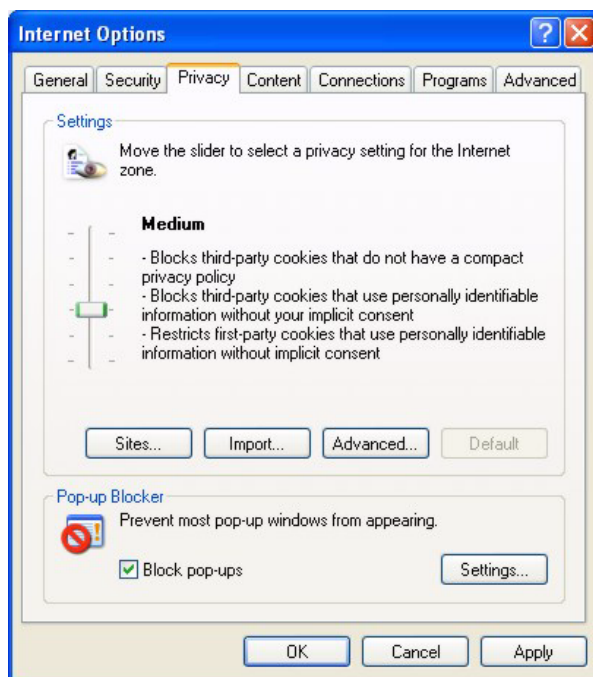
Enable pop-up Blockers with Exceptions

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

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

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

Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

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

Pop-up Blocker Settings



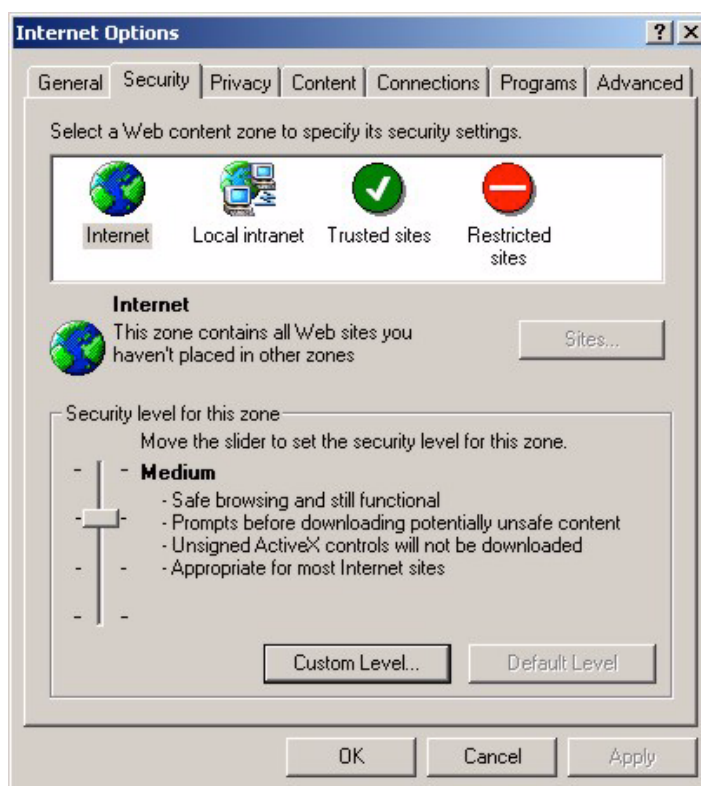
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

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

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

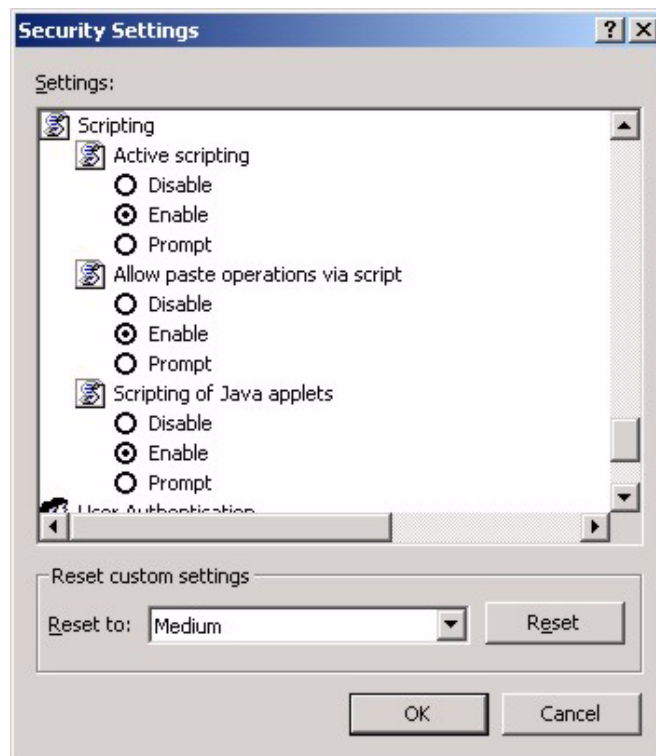
Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

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

Security Settings - Java Scripting

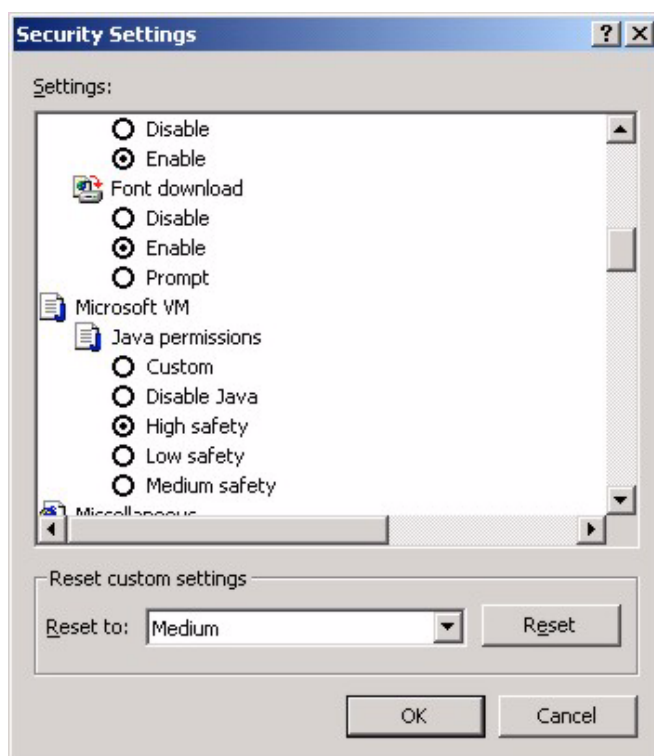


Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

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

Security Settings – Java

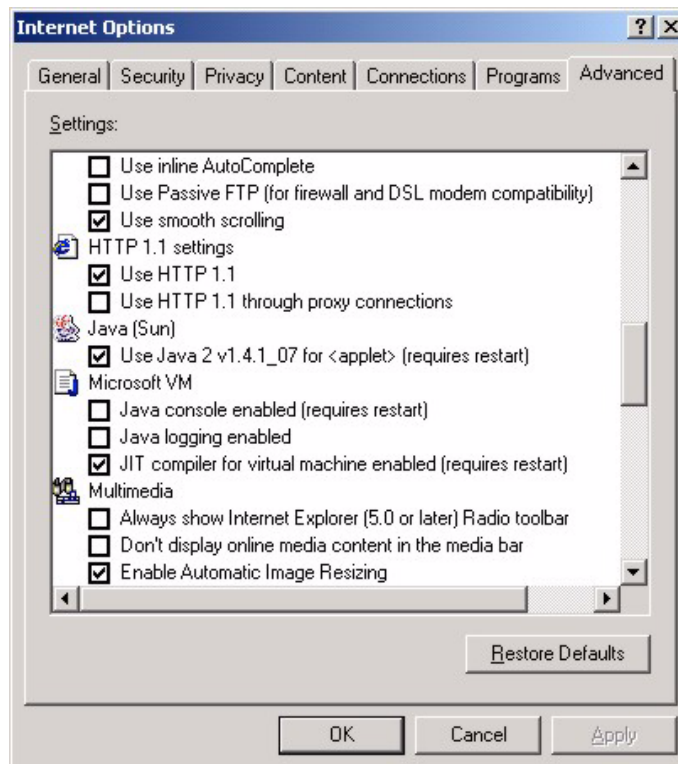


JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

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

Java (Sun)



IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

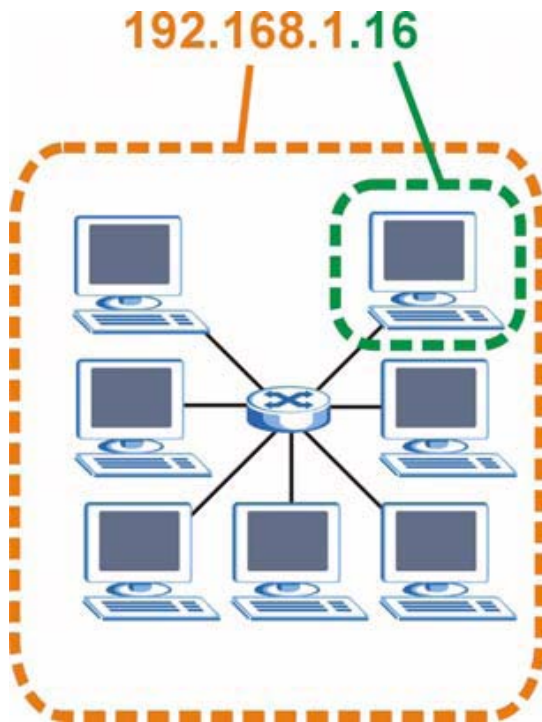
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET: (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000

Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET: (2)
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

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

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

The following table shows some possible subnet masks using both notations.

Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

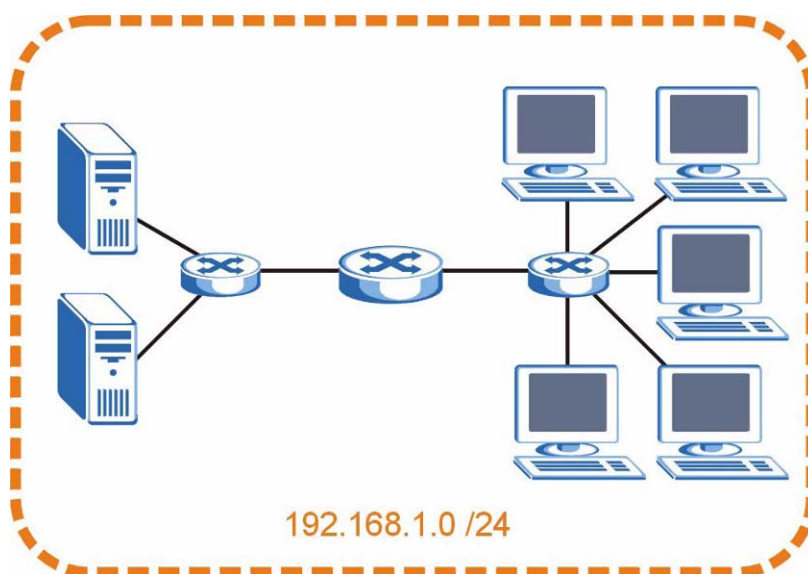
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Subnetting Example: Before Subnetting

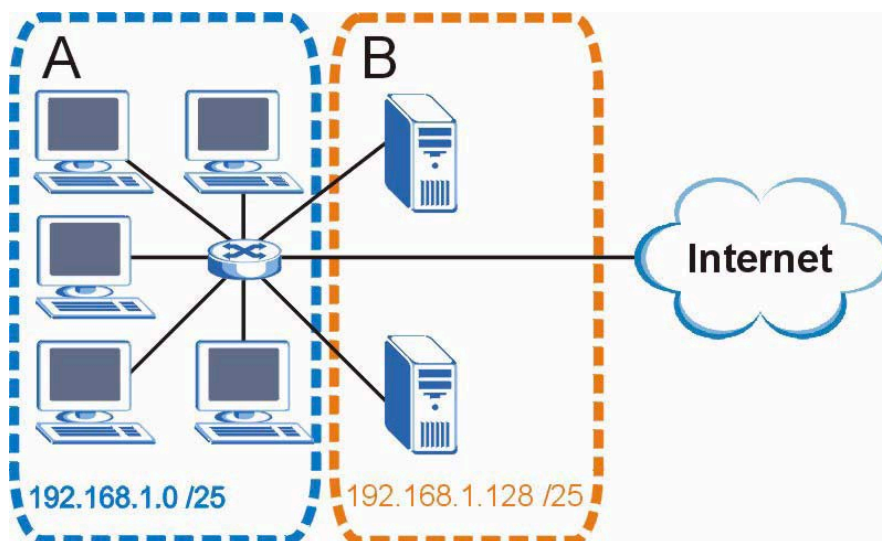


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address)	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

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

Eight Subnets

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

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

24-bit Network Number Subnet Planning

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

The following table is a summary for subnet planning on a network with a 16-bit network number.

16-bit Network Number Subnet Planning

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

Configuring IP Addresses

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. 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. You must also enable Network Address Translation (NAT) on the FSG1100HN.

Once you have decided on the network number, pick an IP address for your FSG1100HN that is easy to remember (for instance, 192.168.1.254) 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 FSG1100HN 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 FSG1100HN unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) 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.

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*.

C Setting up Your Computer's IP Address

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

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

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

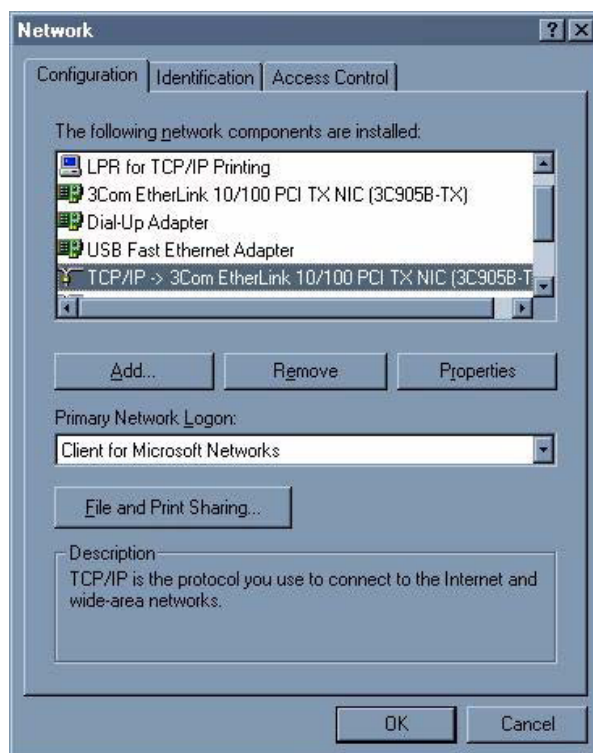
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the FSG1100HN's LAN port.

Windows 95/98/Me

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

Windows 95/98/Me: Network: Configuration



Installing Components

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

If you need the adapter:

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

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.

- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

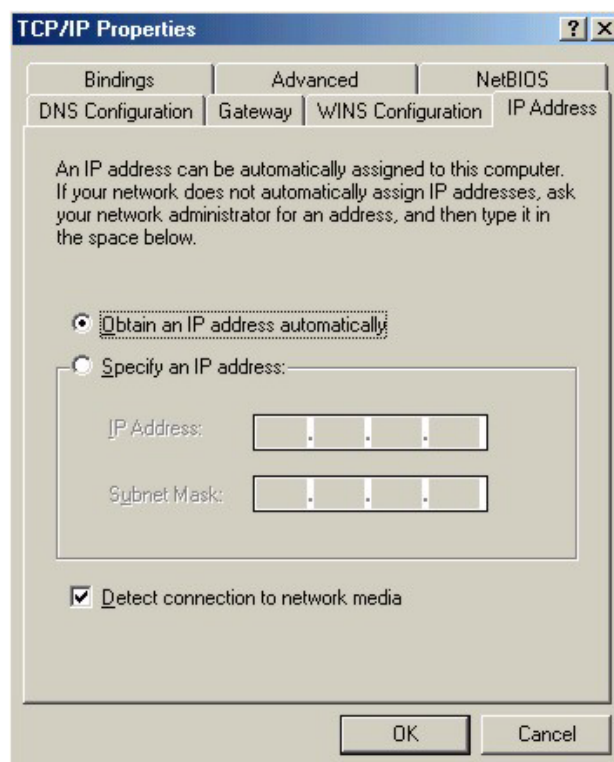
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

Configuring

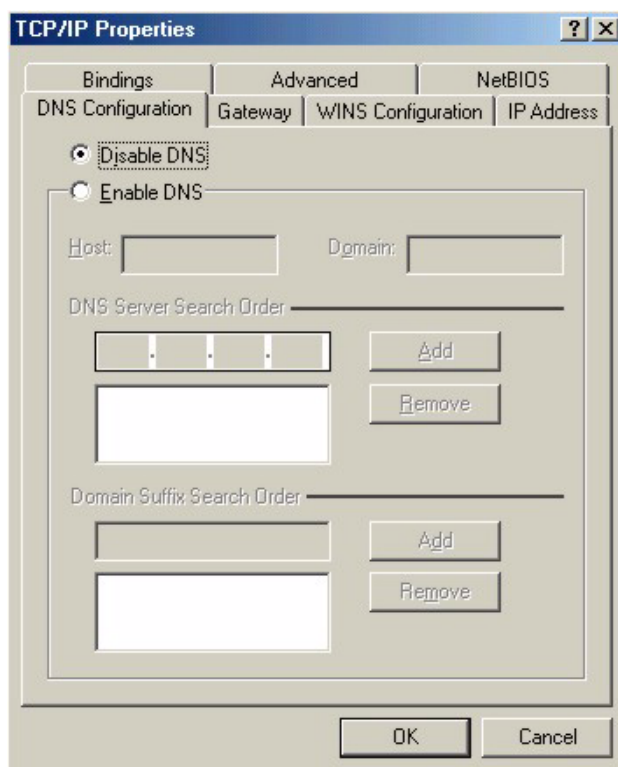
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

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



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

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



- 4 Click the **Gateway** tab.
 - If you do not know your gateway's IP address, remove previously installed gateways.
 - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

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

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

Windows 2000/NT/XP

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

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



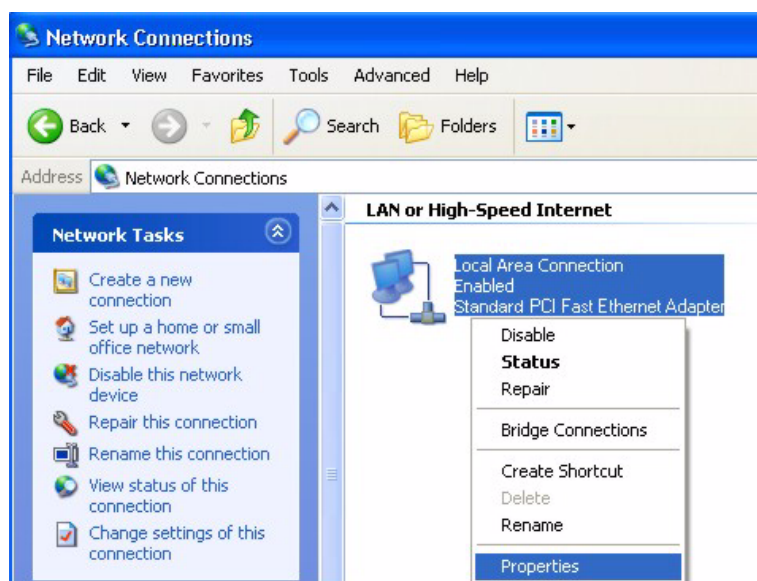
- In the **Control Panel**, double-click **Network Connections (Network and Dialup Connections)** in Windows 2000/NT).

Windows XP: Control Panel



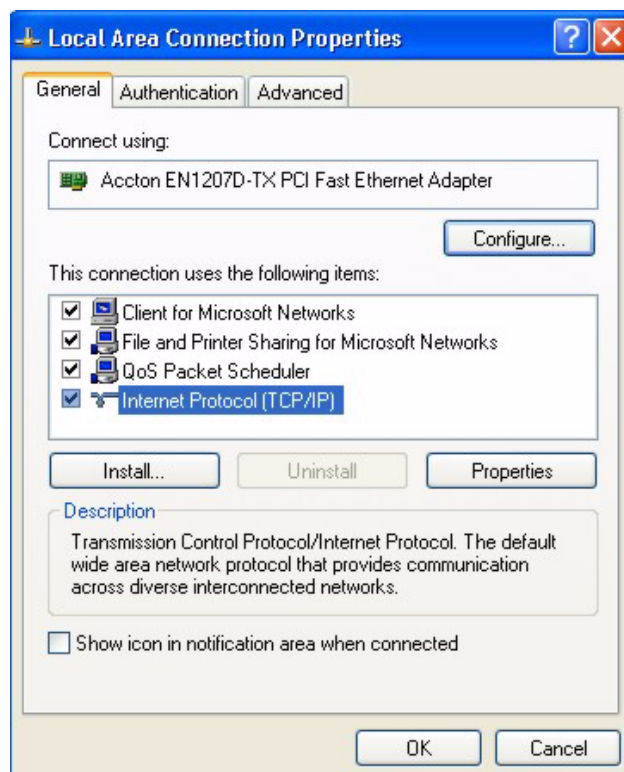
- Right-click **Local Area Connection** and then click **Properties**.

Windows XP: Control Panel: Network Connections: Properties



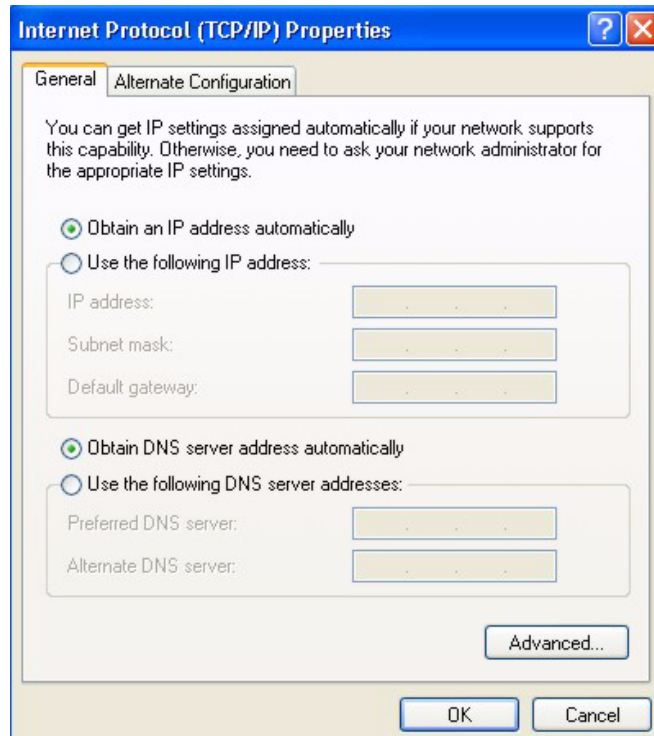
- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
 - If you have a dynamic IP address click **Obtain an IP address automatically**.
 - If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
 - Click **Advanced**.

Windows XP: Internet Protocol (TCP/IP) Properties



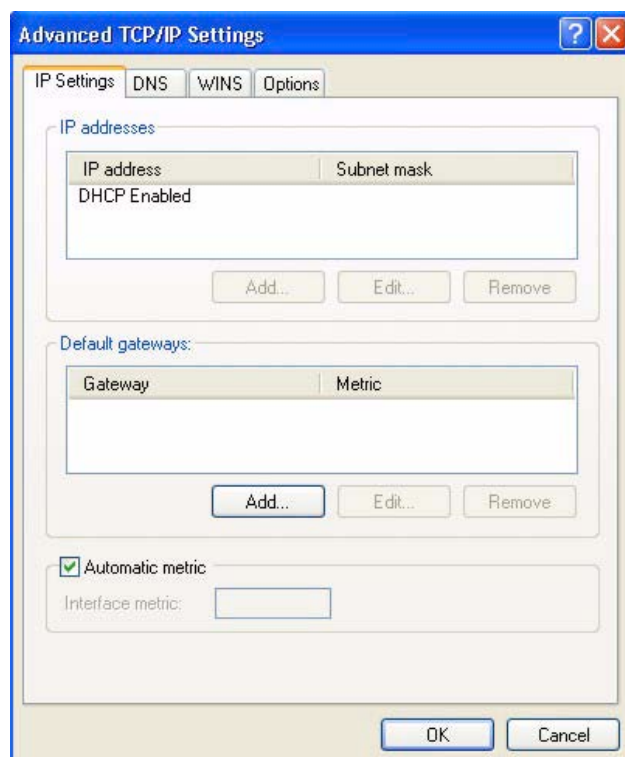
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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

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

- Click **OK** when finished.

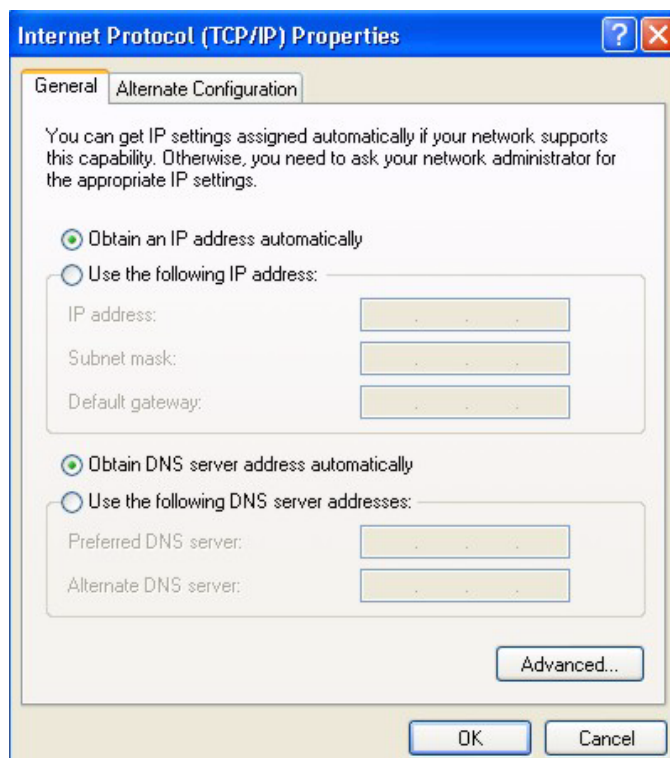
Windows XP: Advanced TCP/IP Properties



- 7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
 - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

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

Windows XP: Internet Protocol (TCP/IP) Properties



- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **Close (OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.
- 10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11 Turn on your Prestige and restart your computer (if prompted).

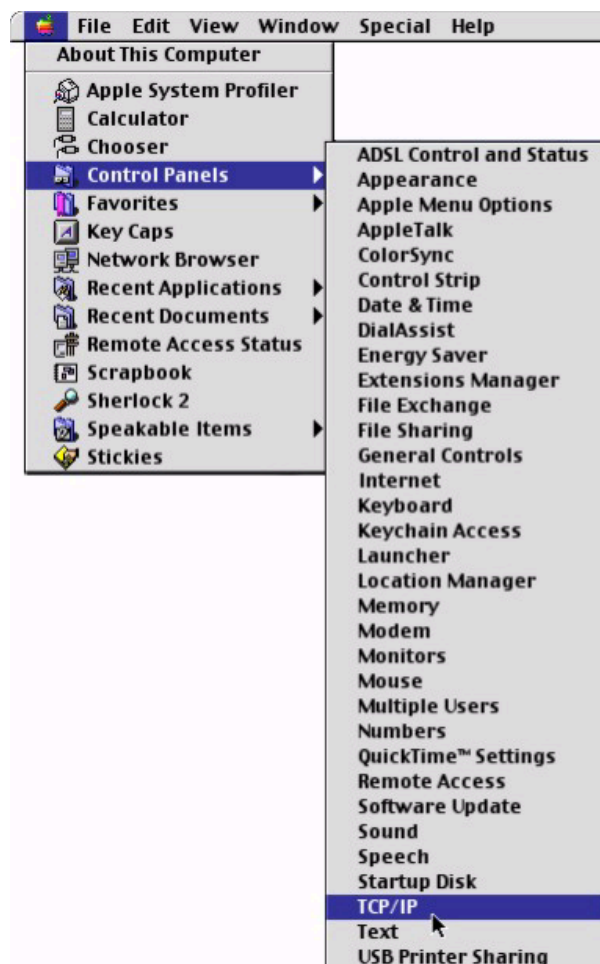
Verifying Settings

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

Macintosh OS 8/9

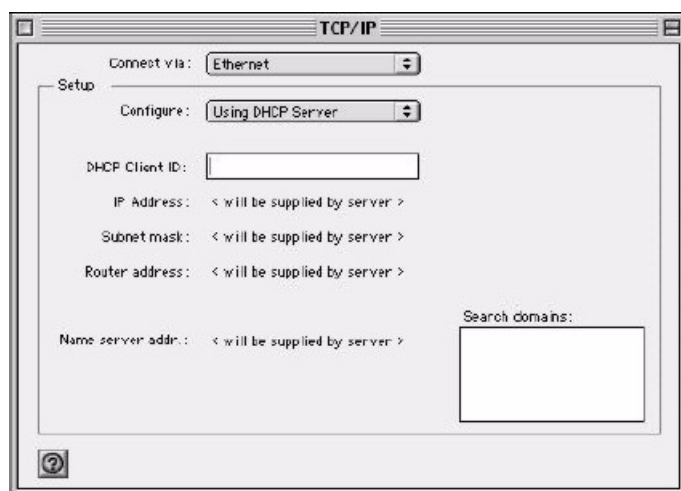
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Macintosh OS 8/9: Apple Menu



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

Macintosh OS 8/9: TCP/IP



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

4 For statically assigned settings, do the following:

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

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

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

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

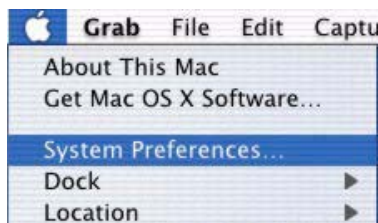
Verifying Settings

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

Macintosh OS X

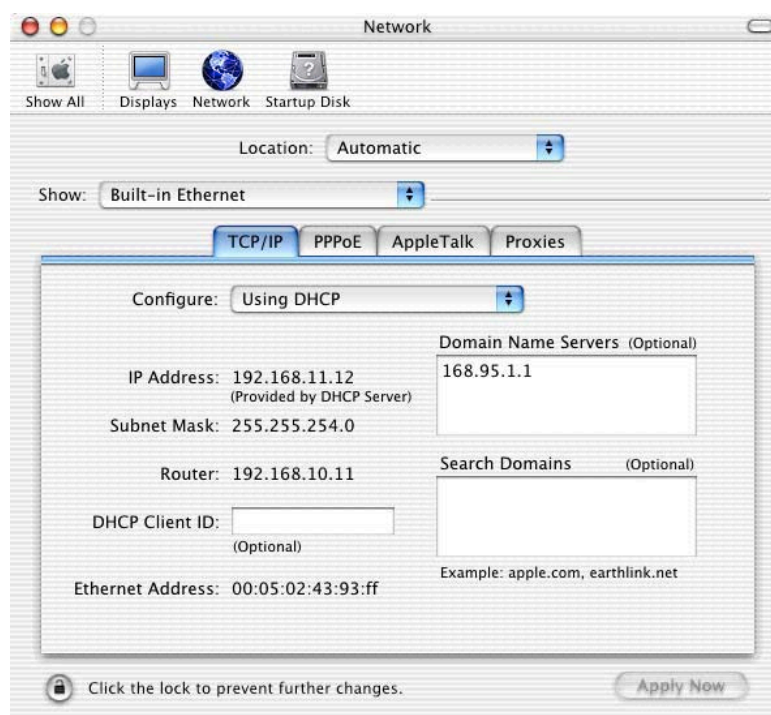
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Macintosh OS X: Network



- 4 For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

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

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

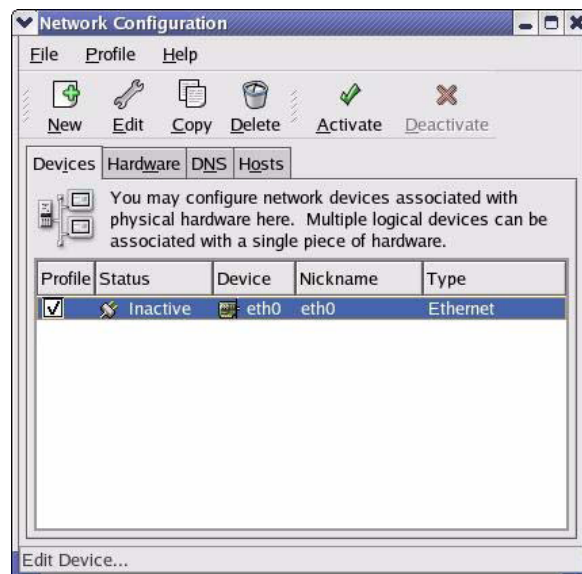
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

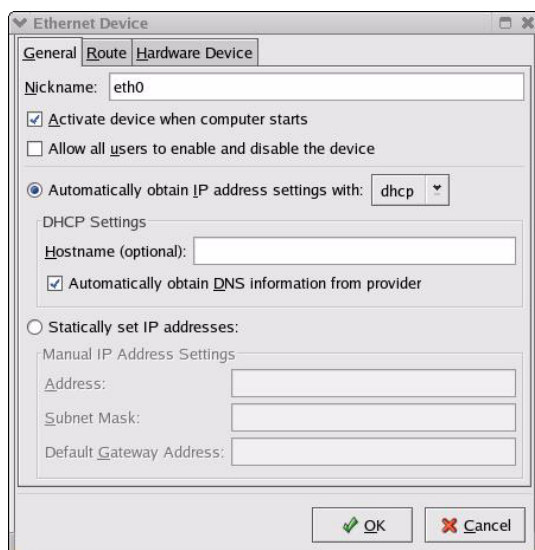
- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Red Hat 9.0: KDE: Network Configuration: Devices



- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

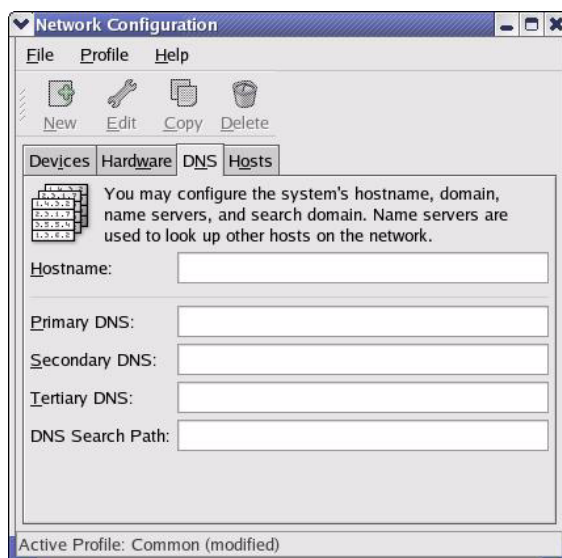
Red Hat 9.0: KDE: Ethernet Device: General



- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

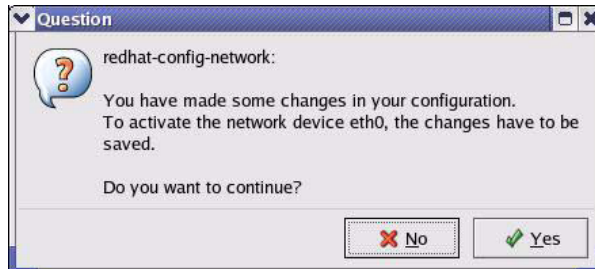
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
- 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Red Hat 9.0: KDE: Network Configuration: DNS



- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens**.

Red Hat 9.0: KDE: Network Configuration: Activate



- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
 - If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart
Shutting down interface eth0: [OK]
Shutting down loopback interface: [OK]
Setting network parameters: [OK]
Bringing up loopback interface: [OK]
Bringing up interface eth0: [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0 Link encap:Ethernet HWaddr 00:50:BA:72:5B:44
inet addr:172.23.19.129 Bcast:172.23.19.255
Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:717 errors:0 dropped:0 overruns:0 frame:0
TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:730412 (713.2 Kb) TX bytes:1570 (1.5 Kb)
Interrupt:10 Base address:0x1000
[root@localhost]#
```

D

Wireless LANs

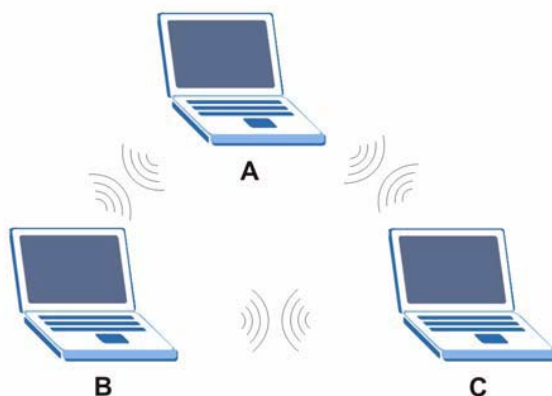
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Peer-to-Peer Communication in an Ad-hoc Network



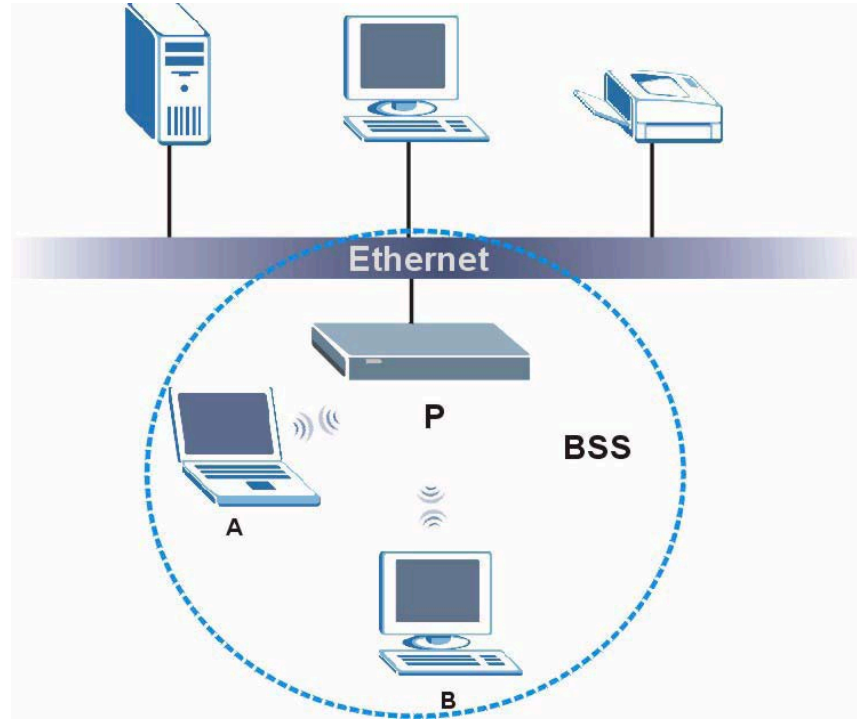
BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and

communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Basic Service Set



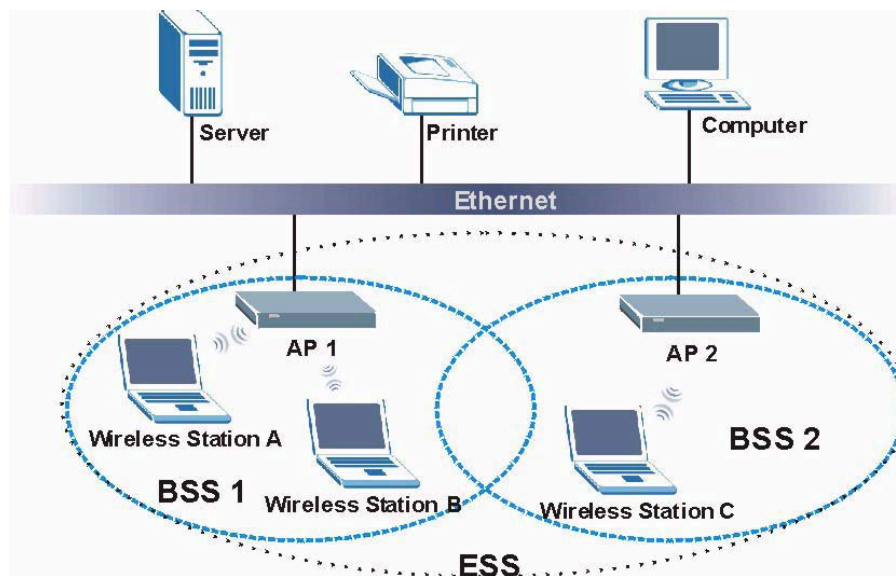
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS Identification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

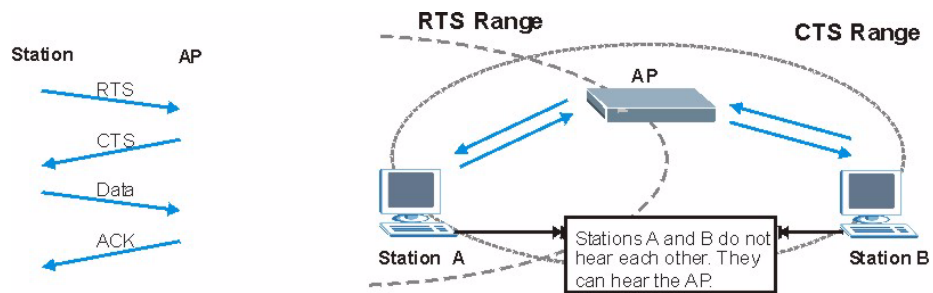
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

RTS/CTS



When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations **MUST** use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g

has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5/11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.
- Access-Challenge
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
Sent by the access point requesting accounting.
- Accounting-Response
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1X.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with dynamic WEP key exchange.

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1X. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPAPSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2 -PSK (WPA2 -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

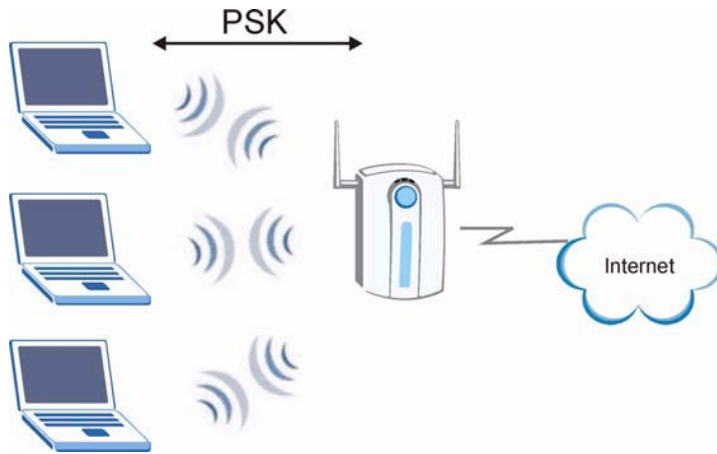
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
- 3 The AP derives and distributes keys to the wireless clients.
- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

WPA(2)-PSK Authentication



WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pairwise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Wireless Security Relational Matrix

AUTHENTICATION METHOD/KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

E Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
 - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP	20	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
	TCP	21	
H.323.	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client/server protocol for the World Wide Web.
HTTPS	TCP	443	HTTPS is a secured HTTP session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP	137	The Network Basic Input/Output System is used for communication between computers on a LAN.
	TCP/UDP	138	
	TCP/UDP	139	
	TCP/UDP	445	
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.

Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RMCD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is the ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	The Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems, and network servers.

Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol is used for Terminal Access Controller Access Control System (TACACS).
Telnet	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 User-Defined	A videoconferencing solution. The UDP port number is specified in the application.

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Certifications

Notices

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

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

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

Note

Repair or replacement, as provided under this warranty, is the exclusive

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

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

End-User License Agreement for "FSG1100HN"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove

any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Table (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the License Notice as below for the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the Software, and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30)

DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8. Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9. Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10. Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11. General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate source code covered under the open source code licenses. To obtain the source code covered under those Licenses, please check ZyXEL Technical Support (support@zyxel.com.tw) to get it.

Open-Sourced Components

3RD PARTY SOFTWARE	VERSION	WEB ADDRESS OF THE SOFTWARE LICENSE TERM
MIPS Linux Kernel	2.6.20	http://www.linux-mips.org
bridge-utils	0.9.5	http://bridge.sourceforge.net
busybox	1.8.2	http://www.busybox.net
Dnrd	2.12.1	http://dnrd.sourceforge.net/
Goahead Web Server	2.1.1	http://www.goahead.com
igmpproxy	0.1	http://igmpproxy.sourceforge.net/
iproute2	2.6.19	http://linux-net.osdl.org/index.php/lproute2
iptables	1.3.8	http://www.netfilter.org
ntpclient	2000_345	http://doolittle.icarus.com/ntpclient/
pppd	2.4.2	http://ppp.samba.org/
pptp	1.3.1	http://pptpclient.sourceforge.net/
tftpd	0.42	ftp://ftp.kernel.org/pub/software/network/tftpd/
udhcpd	0.9.9	http://freshmeat.net/projects/udhcp/
updatedd	2.5	http://freshmeat.net/projects/updatedd/
iwpriv	wireless_tools.25	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes MIPS Linux Kernel 2.6.20, bridge-utils 0.9.5, busybox 1.8.2, Dnrd 2.12.1, iproute2 2.6.19, iptables 1.3.8, ntpclient 2000_345, pptp1.3.1, iwpriv wireless_tools.25, udhcpd 0.9.9 and updated 2.5 software under GPL license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either

verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making

modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes tftpd 0.42 software under below license.

This is tftp-hpa, a conglomerate of a number of versions of the BSD TFTP code, changed around to port to a whole collection of operating systems. The goal is to work on any reasonably modern Unix with sockets.

The tftp-hpa series is maintained by H. Peter Anvin <hpa@zytor.com>.

The latest version of this collection can be found at:

<ftp://ftp.kernel.org/pub/software/network/tftp/>

See the file CHANGES for a list of changes between versions.

Please see the INSTALL and INSTALL.tftp files for compilation and installation instructions.

====> IMPORTANT: IF YOU ARE UPGRADING FROM ANOTHER TFTP SERVER, OR FROM

====> A VERSION OF TFTP-HPA OLDER THAN 0.17 SEE THE FILE

====> "README.security" FOR IMPORTANT SECURITY MODEL CHANGES!

This software can be discussed on the SYSLINUX mailing list. To subscribe, go to the list subscription page at:

<http://www.zytor.com/mailman/listinfo/syslinux>

```

/*_*- c -*----- *
*
* Copyright 2001 H. Peter Anvin - All Rights Reserved
*
* This program is free software available under the same license
* as the "OpenBSD" operating system, distributed at
* http://www.openbsd.org/.
*
*----- */
/*

/* tftp-hpa: $Id$ */

/* $OpenBSD: tftpd.c,v 1.13 1999/06/23 17:01:36 deraadt Exp $*/

/*
* Copyright (c) 1983 Regents of the University of California.
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
*This product includes software developed by the University of
*California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
* may be used to endorse or promote products derived from this software
* without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS
IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY

```

```
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
* SUCH DAMAGE.
*/
```

```
#include "config.h"/* Must be included first */
#include "tftpd.h"
```

```
#ifndef lint
static const char *copyright UNUSED =
"@(#) Copyright (c) 1983 Regents of the University of California.\n\
All rights reserved.
```

```
/* $Id$ */
/* ----- *
*
* Copyright 2001 H. Peter Anvin - All Rights Reserved
*
* This program is free software available under the same license
* as the "OpenBSD" operating system, distributed at
* http://www.openbsd.org/.
* ----- */
```

```
/*
*
.\" -*- nroff -*- ----- *
.\" $Id$
.\"
.\" Copyright (c) 1990, 1993, 1994
.\" The Regents of the University of California. All rights reserved.
.\"
.\" Copyright 2001 H. Peter Anvin - All Rights Reserved
.\"
.\" Redistribution and use in source and binary forms, with or without
.\" modification, are permitted provided that the following conditions
.\" are met:
.\" 1. Redistributions of source code must retain the above copyright
.\" notice, this list of conditions and the following disclaimer.
.\" 2. Redistributions in binary form must reproduce the above copyright
.\" notice, this list of conditions and the following disclaimer in the
.\" documentation and/or other materials provided with the distribution.
.\" 3. Neither the name of the University nor the names of its contributors
.\" may be used to endorse or promote products derived from this software
.\" without specific prior written permission.
.\"
.\" THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS
.\" ``AS IS'' AND
.\" ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
.\" TO, THE
.\" IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
.\" PARTICULAR PURPOSE
.\" ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
.\" BE LIABLE
.\" FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
.\" CONSEQUENTIAL
.\" DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
.\" SUBSTITUTE GOODS
.\" OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
.\" INTERRUPTION)
```

.\n HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 CONTRACT, STRICT
 .\n LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
 ANY WAY
 .\n OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 POSSIBILITY OF
 .\n SUCH DAMAGE.

.\n
 .\n----- */

/* \$Id\$ */
 /* ----- *

*
 * Copyright 2001-2004 H. Peter Anvin - All Rights Reserved
 *
 * This program is free software available under the same license
 * as the "OpenBSD" operating system, distributed at
 * <http://www.openbsd.org/>.
 *
 * ----- */

/*
 /* ----- *

*
 * Copyright 2001-2006 H. Peter Anvin - All Rights Reserved
 *
 * This program is free software available under the same license
 * as the "OpenBSD" operating system, distributed at
 * <http://www.openbsd.org/>.
 *
 * ----- */

/*
 /* ----- *

/* \$Id\$ */
 /* ----- *

*
 * Copyright 2001 H. Peter Anvin - All Rights Reserved
 *
 * This program is free software available under the same license
 * as the "OpenBSD" operating system, distributed at
 * <http://www.openbsd.org/>.
 *
 * ----- */

/*
 /* ----- *

/* \$Id\$ */
 /* \$OpenBSD: extern.h,v 1.2 1996/06/26 05:40:33 deraadt Exp \$*/
 /* \$NetBSD: extern.h,v 1.2 1994/12/08 09:51:24 jtc Exp \$*/

/*
 * Copyright (c) 1993
 *The Regents of the University of California. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
*This product includes software developed by the University of
*California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
* may be used to endorse or promote products derived from this software
* without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS
IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
* SUCH DAMAGE.
*
*

/*\$OpenBSD: main.c,v 1.4 1997/01/17 07:13:30 millert Exp \$*/

/*\$NetBSD: main.c,v 1.6 1995/05/21 16:54:10 mycroft Exp \$*/

/*

* Copyright (c) 1983, 1993

*The Regents of the University of California. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in the

* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software

* must display the following acknowledgement:

*This product includes software developed by the University of

*California, Berkeley and its contributors.

* 4. Neither the name of the University nor the names of its contributors

* may be used to endorse or promote products derived from this software

* without specific prior written permission.
*

```

* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS
IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
* SUCH DAMAGE.
*/

```

```
#include "tftpsubs.h"
```

```

#ifndef lint
static const char *copyright UNUSED =
"@(#) Copyright (c) 1983, 1993\n
The Regents of the University of California. All rights reserved.

```

```

\'' *- nroff *- ----- *
.\" $Id$
.\"
.\" Copyright (c) 1990, 1993, 1994
.\" The Regents of the University of California. All rights reserved.
.\"
.\" Copyright 2001 H. Peter Anvin - All Rights Reserved
.\"
.\" Redistribution and use in source and binary forms, with or without
.\" modification, are permitted provided that the following conditions
.\" are met:
.\" 1. Redistributions of source code must retain the above copyright
.\" notice, this list of conditions and the following disclaimer.
.\" 2. Redistributions in binary form must reproduce the above copyright
.\" notice, this list of conditions and the following disclaimer in the
.\" documentation and/or other materials provided with the distribution.
.\" 3. Neither the name of the University nor the names of its contributors
.\" may be used to endorse or promote products derived from this software
.\" without specific prior written permission.
.\"
.\" THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS
``AS IS" AND
.\" ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
.\" IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
.\" ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
BE LIABLE
.\" FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL

```

```
.\" DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
.\" OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
.\" HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
.\" LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY
.\" OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
.\" SUCH DAMAGE.
.\"
.\"----- */
/* $Id$ */

/* $OpenBSD: ftp.c,v 1.4 1997/08/06 06:43:45 deraadt Exp $*/
/* $NetBSD: ftp.c,v 1.5 1995/04/29 05:55:25 cgd Exp $*/

/*
 * Copyright (c) 1983, 1993
 * The Regents of the University of California. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors.
 * 4. Neither the name of the University nor the names of its contributors
 * may be used to endorse or promote products derived from this software
 * without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS
 * IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
 * TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 * PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
 * BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
 * ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF
 * SUCH DAMAGE.
```

/* tftp-hpa: \$Id\$ */

/* \$OpenBSD: tftpsubs.c,v 1.2 1996/06/26 05:40:36 deraadt Exp \$*/

/* \$NetBSD: tftpsubs.c,v 1.3 1994/12/08 09:51:31 jtc Exp \$*/

/*

* Copyright (c) 1983, 1993

*The Regents of the University of California. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:

* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:

*This product includes software developed by the University of
*California, Berkeley and its contributors.

* 4. Neither the name of the University nor the names of its contributors
* may be used to endorse or promote products derived from this software
* without specific prior written permission.

*

* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS
* IS'' AND

* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
* TO, THE

* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
* PARTICULAR PURPOSE

* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
* BE LIABLE

* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL

* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
* SUBSTITUTE GOODS

* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
* INTERRUPTION)

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
* CONTRACT, STRICT

* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
* ANY WAY

* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
* POSSIBILITY OF

* SUCH DAMAGE.

/* \$Id\$ */

/* \$OpenBSD: tftpsubs.h,v 1.2 1996/06/26 05:40:37 deraadt Exp \$*/

/* \$NetBSD: tftpsubs.h,v 1.2 1994/12/08 09:51:32 jtc Exp \$*/

/*

* Copyright (c) 1993

*The Regents of the University of California. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:

* 1. Redistributions of source code must retain the above copyright

- * notice, this list of conditions and the following disclaimer.
- * 2. Redistributions in binary form must reproduce the above copyright
- * notice, this list of conditions and the following disclaimer in the
- * documentation and/or other materials provided with the distribution.
- * 3. All advertising materials mentioning features or use of this software
- * must display the following acknowledgement:
- *This product includes software developed by the University of
- *California, Berkeley and its contributors.
- * 4. Neither the name of the University nor the names of its contributors
- * may be used to endorse or promote products derived from this software
- * without specific prior written permission.
- *
- * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS
- IS" AND
- * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
- TO, THE
- * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
- PARTICULAR PURPOSE
- * ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS
- BE LIABLE
- * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
- CONSEQUENTIAL
- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
- SUBSTITUTE GOODS
- * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
- INTERRUPTION)
- * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
- CONTRACT, STRICT
- * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
- ANY WAY
- * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
- POSSIBILITY OF
- * SUCH DAMAGE.

This Product includes pptp 1.3.1 software under below license.

License

PPTP Client is licensed under the GNU General Public License (GPL) version 2 or later. PPTP Client was known as pptp-linux and was written by C. Scott Ananian. There have been many contributions by users of PPTP Client. PPP 2.4.2 and later contains MPPE support, added by Frank Cusack and others, that is licensed under a BSD without advertising clause license. The older and deprecated PPP-MPPE 2.4.0 and 2.4.1 contain MS-CHAP-v2 and MPPE support that was added to PPP by Paul Cadach (paul@odt.east.telecom.kz). Two functions from OpenSSL were copied. Because of this, we must say for PPP-MPPE 2.4.0 and 2.4.1 that "this product includes cryptographic software written by Eric A. Young (eay@cryptsoft.com)" and "this product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)."

This Product includes pppd 2.4.2 software under below license.

ppp-2.4, a package which implements the Point-to-Point Protocol (PPP) to provide Internet connections over serial lines.

Copyrights:

All of the code can be freely used and redistributed. The individual source files each have their own copyright and permission notice.

Pppd, pppstats and pppdump are under BSD-style notices. Some of the pppd plugins are GPL'd. Chat is public domain.

pppd - Point-to-Point Protocol Daemon

Authors

Paul Mackerras (paulus@samba.org), based on earlier work by Drew Perkins, Brad Clements, Karl Fox, Greg Christy, and Brad Parker.

Copyright

Pppd is copyrighted and made available under conditions which provide that it may be copied and used in source or binary forms provided that the conditions listed below are met. Portions of pppd are covered by the following copyright notices:

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

Copyright (c) 1993-2004 Paul Mackerras. All rights reserved.

Copyright (c) 1995 Pedro Roque Marques. All rights reserved.

Copyright (c) 1995 Eric Rosenquist. All rights reserved.

Copyright (c) 1999 Tommi Komulainen. All rights reserved.

Copyright (C) Andrew Tridgell 1999

Copyright (c) 2000 by Sun Microsystems, Inc. All rights reserved.

Copyright (c) 2001 by Sun Microsystems, Inc. All rights reserved.

Copyright (c) 2002 Google, Inc. All rights reserved.

The copyright notices contain the following statements.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

Office of Technology Transfer

Carnegie Mellon University

5000 Forbes Avenue

Pittsburgh, PA 15213-3890

(412) 268-4387, fax: (412) 268-7395

tech-transfer@andrew.cmu.edu

3b. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.

4. Redistributions of any form whatsoever must retain the following acknowledgments:

"This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)."

"This product includes software developed by Paul Mackerras <paulus@samba.org>".

"This product includes software developed by Pedro Roque Marques <pedro_m@yahoo.com>".

"This product includes software developed by Tommi Komulainen <Tommi.Komulainen@iki.fi>".
CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

This Product includes igmpproxy 0.1 software under below license.

igmpproxy - IGMP proxy based multicast router
Copyright (C) 2005 Johnny Egeland <johnny@rlo.org>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

This software is derived work from the following software. The original source code has been modified from it's original state by the author of igmpproxy.

smcroute 0.92 - Copyright (C) 2001 Carsten Schill <carsten@cschill.de>
- Licensed under the GNU General Public License, version 2

mrouted 3.9-beta3 - COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.
- Original license can be found in the Stanford.txt file.

This Product includes Goahead Web Server 2.1.1 software under below license.

License Agreement

THIS LICENSE ALLOWS ONLY THE LIMITED USE OF GO AHEAD SOFTWARE, INC. PROPRIETARY CODE. PLEASE CAREFULLY READ THIS AGREEMENT AS IT PERTAINS TO THIS LICENSE, YOU CERTIFY THAT YOU WILL USE THE SOFTWARE ONLY IN THE MANNER PERMITTED HEREIN.

1. Definitions.

1.1 "Documentation" means any documentation GoAhead includes with the Original Code.

1.2 "GoAhead" means Go Ahead Software, Inc.

1.3 "Intellectual Property Rights" means all rights, whether now existing or hereinafter acquired, in and to trade secrets, patents, copyrights, trademarks, know-how, as well as moral rights and similar rights of any type under the laws of any governmental authority, domestic or foreign, including rights in and to all applications and registrations relating to any of the foregoing.

1.4 "License" or "Agreement" means this document.

1.5 "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications.

1.6 "Original Code" means the Source Code to GoAhead * proprietary computer software entitled GoAhead WebServer.

1.7 "Response Header" means the first portion of the response message output by the GoAhead WebServer, containing but not limited to, header fields for date, content-type, server identification and cache control.

1.8 "Server Identification Field" means the field in the Response Header which contains the text "Server: GoAhead-Webs".

1.9 "You" means an individual or a legal entity exercising rights under, and complying with all of the terms of, this license or a future version of this license. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1 Limited Source Code Grant.

GoAhead hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims, to use, reproduce, modify, copy and distribute the Original Code.

2.2 Binary Code.

GoAhead hereby grants You a world-wide, royalty-free, non-exclusive license to copy and distribute the binary code versions of the Original Code together with Your Modifications.

2.3 License Back to GoAhead.

You hereby grant in both source code and binary code to GoAhead a world-wide, royalty-free, non-exclusive license to copy, modify, display, use and sublicense any Modifications You make that are distributed or planned for distribution. Within 30

days of either such event, You agree to ship to GoAhead a file containing the Modifications (in a media to be determined by the parties), including any programmers' notes and other programmers' materials. Additionally, You will provide to GoAhead a complete description of the product, the product code or model number, the date on which the product is initially shipped, and a contact name, phone number and e-mail address for future correspondence. GoAhead will keep confidential all data specifically marked as such.

2.4 Restrictions on Use.

You may sublicense Modifications to third parties such as subcontractors or OEM's provided that You enter into license agreements with such third parties that bind such third parties to all the obligations under this Agreement applicable to you and that are otherwise substantially similar in scope and application to this Agreement.

3. Term.

This Agreement and license are effective from the time You accept the terms of this Agreement until this Agreement is terminated. You may terminate this Agreement at any time by uninstalling or destroying all copies of the Original Code including any and all binary versions and removing any Modifications to the Original Code existing in any products. This Agreement will terminate immediately and without further notice if You fail to comply with any provision of this Agreement. All restrictions on use, and all other provisions that may reasonably be interpreted to survive termination of this Agreement, will survive termination of this Agreement for any reason. Upon termination, You agree to uninstall or destroy all copies of the Original Code, Modifications, and Documentation.

4. Trademarks and Brand.

4.1 License and Use.

GoAhead hereby grants to You a limited world-wide, royalty-free, non-exclusive license to use the GoAhead trade names, trademarks, logos, service marks and product designations posted in Exhibit A (collectively, the "GoAhead Marks") in connection with the activities by You under this Agreement. Additionally, GoAhead grants You a license under the terms above to such GoAhead trademarks as shall be identified at a URL (the "URL") provided by GoAhead. The use by You of GoAhead Marks shall be in accordance with GoAhead's trademark policies regarding trademark usage as established at the web site designated by the URL, or as otherwise communicated to You by GoAhead at its sole discretion. You understand and agree that any use of GoAhead Marks in connection with this Agreement shall not create any right, title or interest in or to such GoAhead Marks and that all such use and goodwill associated with GoAhead Marks will inure to the benefit of GoAhead.

4.2 Promotion by You of GoAhead WebServer Mark.

In consideration for the licenses granted by GoAhead to You herein, You agree to notify GoAhead when You incorporate the GoAhead WebServer in Your product and to inform GoAhead when such product begins to ship. You agree to promote the Original Code by prominently and visibly displaying a graphic of the GoAhead WebServer mark on the initial web page of Your product that is displayed each time a user connects to it. You also agree that GoAhead may identify your company as a user of the GoAhead WebServer in conjunction with its own marketing efforts. You may further promote the Original Code by displaying the GoAhead WebServer mark in marketing and promotional materials such as the home page of your web site or web pages promoting the product.

4.3 Placement of Copyright Notice by You.

You agree to include copies of the following notice (the "Notice") regarding proprietary rights in all copies of the products that You distribute, as follows: (i) embedded in the object code; and (ii) on the title pages of all documentation. Furthermore, You agree to use commercially reasonable efforts to cause any licensees of your products to embed the Notice in object code and on the title pages or relevant documentation. The Notice is as follows: Copyright (c) 20xx GoAhead Software, Inc. All Rights Reserved. Unless GoAhead otherwise instructs, the year 20xx is to be replaced with the year during which the release of the Original Code containing the notice is issued by GoAhead. If this year is not supplied with Documentation, GoAhead will supply it upon request.

4.4 No Modifications to Server Identification Field.

You agree not to remove or modify the Server identification Field contained in the Response Header as defined in Section 1.6 and 1.7.

5. Warranty Disclaimers.

THE ORIGINAL CODE, THE DOCUMENTATION AND THE MEDIA UPON WHICH THE ORIGINAL CODE IS RECORDED (IF ANY) ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EXPRESS, STATUTORY OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The entire risk as to the quality and performance of the Original Code (including any Modifications You make) and the Documentation is with You. Should the Original Code or the Documentation prove defective, You (and not GoAhead or its distributors, licensors or dealers) assume the entire cost of all necessary servicing or repair. GoAhead does not warrant that the functions contained in the Original Code will meet your requirements or operate in the combination that You may select for use, that the operation of the Original Code will be uninterrupted or error free, or that defects in the Original Code will be corrected. No oral or written statement by GoAhead or by a representative of GoAhead shall create a warranty or increase the scope of this warranty.

GOAHEAD DOES NOT WARRANT THE ORIGINAL CODE AGAINST INFRINGEMENT OR THE LIKE WITH RESPECT TO ANY COPYRIGHT, PATENT, TRADE SECRET, TRADEMARK OR OTHER PROPRIETARY RIGHT OF ANY THIRD PARTY AND DOES NOT WARRANT THAT THE ORIGINAL CODE DOES NOT INCLUDE ANY VIRUS, SOFTWARE ROUTINE OR OTHER SOFTWARE DESIGNED TO PERMIT UNAUTHORIZED ACCESS, TO DISABLE, ERASE OR OTHERWISE HARM SOFTWARE, HARDWARE OR DATA, OR TO PERFORM ANY OTHER SUCH ACTIONS.

Any warranties that by law survive the foregoing disclaimers shall terminate ninety (90) days from the date You received the Original Code.

6. Limitation of Liability.

YOUR SOLE REMEDIES AND GOAHEAD'S ENTIRE LIABILITY ARE SET FORTH ABOVE. IN NO EVENT WILL GOAHEAD OR ITS DISTRIBUTORS OR DEALERS BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE ORIGINAL CODE, THE INABILITY TO USE THE ORIGINAL CODE, OR ANY DEFECT IN THE ORIGINAL CODE, INCLUDING ANY LOST PROFITS, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

You agree that GoAhead and its distributors and dealers will not be LIABLE for defense or indemnity with respect to any claim against You by any third party arising from your possession or use of the Original Code or the Documentation.

In no event will GoAhead's total liability to You for all damages, losses, and causes of action (whether in contract, tort, including negligence, or otherwise) exceed the amount You paid for this product.

SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, AND SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

7. Indemnification by You.

You agree to indemnify and hold GoAhead harmless against any and all claims, losses, damages and costs (including legal expenses and reasonable counsel fees) arising out of any claim of a third party with respect to the contents of the Your products, and any intellectual property rights or other rights or interests related thereto.

8. High Risk Activities.

The Original Code is not fault-tolerant and is not designed, manufactured or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines or weapons systems, in which the failure of the Original Code could lead directly to death, personal injury, or severe physical or environmental damage. GoAhead and its suppliers specifically disclaim any express or implied warranty of fitness for any high risk uses listed above.

9. Government Restricted Rights.

For units of the Department of Defense, use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Contractor/manufacturer is GoAhead Software, Inc., 10900 N.E. 8th Street, Suite 750, Bellevue, Washington 98004.

If the Commercial Computer Software Restricted rights clause at FAR 52.227-19 or its successors apply, the Software and Documentation constitute restricted computer software as defined in that clause and the Government shall not have the license for published software set forth in subparagraph (c)(3) of that clause.

The Original Code (i) was developed at private expense, and no part of it was developed with governmental funds; (ii) is a trade secret of GoAhead (or its licensor(s)) for all purposes of the Freedom of Information Act; (iii) is "restricted computer software" subject to limited utilization as provided in the contract between the vendor and the governmental entity; and (iv) in all respects is proprietary data belonging solely to GoAhead (or its licensor(s)).

10. Governing Law and Interpretation.

This Agreement shall be interpreted under and governed by the laws of the State of Washington, without regard to its rules governing the conflict of laws. If any provision of this Agreement is held illegal or unenforceable by a court or tribunal of competent jurisdiction, the remaining provisions of this Agreement shall remain in effect and the

invalid provision deemed modified to the least degree necessary to remedy such invalidity.

11. Entire Agreement.

This Agreement is the complete agreement between GoAhead and You and supersedes all prior agreements, oral or written, with respect to the subject matter hereof.

If You have any questions concerning this Agreement, You may write to GoAhead Software, Inc., 10900 N.E. 8th Street, Suite 750, Bellevue, Washington 98004 or send e-mail to info@goahead.com.

BY CLICKING ON THE "Register" BUTTON ON THE REGISTRATION FORM, YOU ACCEPT AND AGREE TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. IF YOU DO NOT WISH TO ACCEPT THIS LICENSE OR YOU DO NOT QUALIFY FOR A LICENSE BASED ON THE TERMS SET FORTH ABOVE, YOU MUST NOT CLICK THE "Register" BUTTON.

Exhibit A
GoAhead Trademarks, Logos, and Product Designation Information
01/28/00