IP Address	http://192.168.100.1
Password	1234

Firmware Version 1.0
Edition 1, 10/2011

MWR102

Mobile Wireless Router

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the MWR102 using the Web-Based Management Interface. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

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

- Supporting Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.us.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us to help you. Send all User Guide-related comments, questions or suggestions for improvement to the following e-mail address. Thank you!

SUPPORT E-MAIL	WEB SITE
techwriter@zyxel.com	www.zyxel.com

Customer Support

Please have the following information ready when you contact Customer Support:

- Product model and serial number
- Warranty information
- Date that you received or purchased your device
- Brief description of the problem including any steps that you have taken before contacting the ZyXEL Customer Support representative

Support Email	support@zyxel.com
Toll-Free	1-800-978-7222
Website	www.us.zyxel.com
Postal mail	ZyXEL Communications Inc. 1130 N. Miller Street, Anaheim, CA 92806-2001 U.S.A.

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 MWR102 may be referred to as the "MWR102", 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 MWR102 icon is not an exact representation of your device.

MWR102 	Computer 	Notebook computer 
Server 	Modem 	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 leave the device exposed to a heat source or in a high-temperature location such as in the sun or in an unattended vehicle. To prevent damage, remove the device from the vehicle or store it out of direct sunlight
- When storing the device for an extended time, store within the following temperature range: from 32° to 77°F
- Do not operate the device beyond the range of 32° to 104° F
- Do not operate or store the device outside of the above temperature range
- Contact your local waste disposal department to dispose of the device/battery in accordance with applicable local laws and regulations.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do Not keep the unit power on while putting it into suite case, closed box, luggage, computer bag and any closed storage, do turn the device power off before storage.
- 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 power adaptor or cord provided by the manufacturer 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 and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Battery Warnings

Please follow the safety guidelines described in the safety warning and battery warning. Failing to do so may shorten the lifespan of the internal lithium ion battery or may present a risk of damage to the unit, fire, chemical burn, electrolyte leak and/or injury.

- Do not leave unit exposed to a heat source or in a location that may become hot, such as a parked vehicle or in direct sunlight. Do not leave in a glove box, trunk or other location that may become hot.
- Do not puncture or incinerate the device or battery.
- When/if you dispose of the battery, be certain to follow ordinances from local waste disposal agencies.
- Keep the battery away from small children or pets
- Never use a knife, screwdriver or other sharp object to remove the battery.
- Do not attempt to open the battery.
- Use only the provided recharger to recharge the battery.
- Only replace the battery with the correct replacement battery. Failure to do so may result in fire or explosion. Contac ZyXEL to obtain the correct replacement battery.

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

Part I: Introduction

1 Getting to Know Your MWR102

1.1 Overview

The MWR102 is a mobile wireless router with 1T1R MIMO technology. It complies with IEEE 802.11n standards, with Wireless N data rates of up to 150 Mbps, and IEEE 802.11b/g with Wireless B/G data rates of 54 Mbps. It is also backward compatable with all 11/54 Mbps wireless (802.11b/g) products.

The router allows multiple users to share one broadband connection, as well as secures your private network. LAN users can share files, printers, or play network games all at high speeds over the same network.

The MWR102 supports advanced security encryption: WPA, WPA2, open shared key, and pair-wise key authentication services, giving you vital network security. Moreover, this router supports energy efficient Ethernet and saves power.

1.2 Applications

You can create the following networks using the MWR102:

- **Wired**. You can connect a network device via the Ethernet port of the MWR102 so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the MWR102 to access network resources.
- **Land line WAN**. Connect to a broadband modem/router for Internet access.

1.3 Good Habits for Managing the MWR102

Do the following things regularly to make the MWR102 more secure and to manage the MWR102 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 MWR102 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the MWR102. You could simply restore your last configuration.

1.4 The Front Panel

Figure 1 The front panel of the Wireless Router

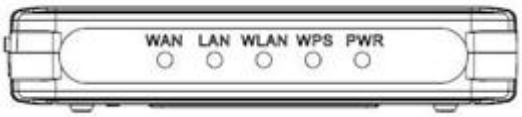
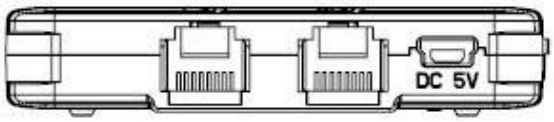


Table 1 Front Panel LEDs

Name	Status	Indication
PWR	Green	Power on
	Dark	Power off
WPS	Blink green one time	System reboot
	Blink green	WPS connecting
	Dark	System stable
WLAN	Off	The wireless function is disabled.
	Flashing	The wireless function is enabled.
	Flashing fast	Sending or receiving data over wireless.
WAN / LAN	Off	There is no device linked to the corresponding port or the connection is dropping off.
	On	There are devices linked to the corresponding ports but no data transmitted or received.
	Flashing	Sending or receiving data over corresponding port.

1.5 The Rear Panel

Figure 2 The rear panel of the Wireless Router.



- **LAN:** Through this port, you can connect the router to your PCs and the other Ethernet network devices.
- **WAN:** This WAN port is where you will connect the cable/DSL Modem, or Ethernet.
- **DC IN:** Plug the end of the cable firmly into the rear panel of the router, and plug the other end into a USB outlet to power the system.
- **WPS/Reset Button:** Located on the underside of the device. Click this button to start PBC configuration method for easy WPS setup.Hold the reset button for 5 seconds or more to reset the system to factory defaults. The system will then reboot, and approximately 60 seconds later will be ready for further use. The reboot process cannot be interrupted by powering off the device, or the unit will fail. Before performing the reset process, ensure the system will be able to finish rebooting!

Warning: Incomplete factory setting recovery procedure will cause the Wireless Router to malfunction! If you are in this situation, do not try to repair it by yourself. Consult your local distributor for help!

2 Web-Based Management

2.1 Overview

This chapter describes how to access the MWR102 Web-Based Management Interface and provides an overview of its screens.

The Web-Based Management Interface is an HTML-based management interface that allows easy setup and management of the MWR102 via Internet browser. Use Internet Explorer 7.0 and later or Firefox 3.0 and later versions or Safari 4.0 or later versions. The recommended screen resolution is 1024 by 768 pixels or higher. In order to use the Web-Based Management Interface 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 (Chapter 16) to see how to make sure these functions are allowed in Internet Explorer.

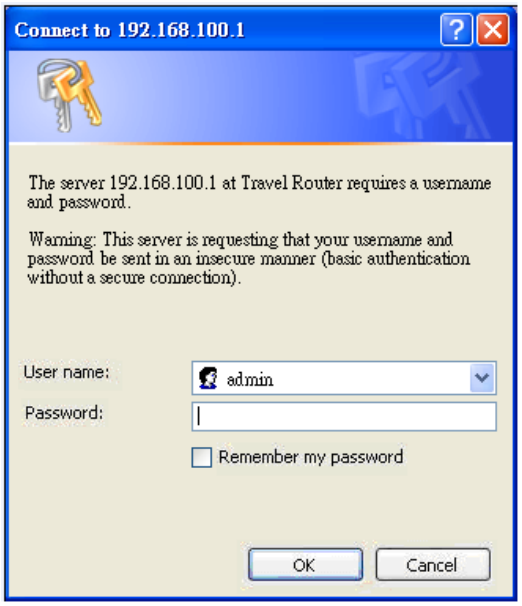
2.2 Accessing the Web-Based Management Interface

1. Make sure your MWR102 hardware is properly connected and prepare your computer or computer network to connect to the MWR102 (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.100.1" as the website address. Your computer must be in the same subnet in order to access this website address.

2.2.1 Login Screen

The Web-Based Management Interface initially displays the following login screen.

Figure 3 Login Screen



The following table describes the labels in this screen.

LABEL	DESCRIPTION
User Name	Type “admin” (default) as the User name.
Password	Type “1234” (default) as the password.

2.3 Resetting the MWR102

If you forget your password or IP address, or you cannot access the Web-Based Management Interface, you will need to use the **RESET** button at the back of the MWR102 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 “192.168.100.1”.

2.3.1 Procedure to Use the Reset Button

1 Make sure the power LED is on.

2 Press the **RESET** button for longer than one second to restart/reboot the MWR102.

3 Press the **RESET** button for longer than five seconds to set the MWR102 back to its factory-default configurations. The Power LED will start to blink to indicate that the default configuration is being loaded.

3 MWR102 Modes

3.1 Overview

This chapter introduces the different modes available on your MWR102.

3.1.1 Device Modes

This refers to the operating mode of the MWR102, which can act as a:

- **Router**. This is the default device mode of the MWR102. Use this mode to connect the local network to another network, like the Internet.
- **Access Point**. Use this mode if you want to extend your network by allowing network devices to connect to the MWR102 wirelessly. Go to AP view the **Status** screen in this mode.

4 Router Mode

4.1 Overview

The MWR102 is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet).

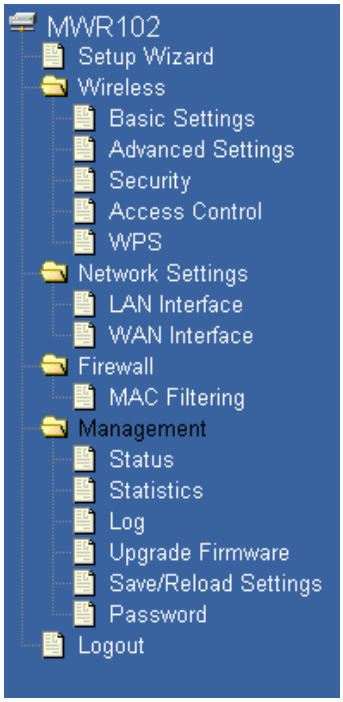
4.2 What You Can Do

Use the **Status** screen to view read-only information about your MWR102.

4.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure MWR102 features.

Figure 4 Navigation Panel



The following table describes the sub-menus.

Table 2 Navigation Panel: Router Mode

LINK	FUNCTION
Setup Wizard	This screen guides you through the setup of the MWR102.
Wireless	
Basic Settings	Use this screen to change the basic wireless settings of the MWR102
Advanced Settings	Use this screen to configure advanced wireless settings
Security	Use this screen to change Wireless Security settings.
Access Control	This page allows control over what devices are allowed to access the router.
WPS	This screen allows you to change the Wi-Fi Protected Setup settings for the MWR102
Network Settings	
LAN Interface	This screen allows you to configure the parameters for your Local Area Network.
WAN Interface	This screen allows you to configure WAN settings.
Firewall	
MAC Filtering	This screen allows you to deny access to specific devices on your network.
Management	

Status	Shows the current status and basic settings of the travel router
Statistics	Shows packet counts for wired and wireless Ethernet connections.
Log	Set remote log server parameters and view the system log.
Upgrade Firmware	Upgrade the travel router firmware.
Save/Reload Settings	Save the current settings to a backup file, or reload the setting from a previously saved file.
Password	Set or change the travel router ADMINISTRATOR user name and password.
Logout	

5 Access Point Mode

5.1 Overview

Use your MWR102 as an access point (AP) if you already have a router or gateway on your network. In this mode your MWR102 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet.

5.2 What You Can Do

- Use the **Status** screen to view read-only information about your MWR102.
- Use the **LAN** screen to set the IP address for your MWR102 acting as an access point.

5.2.1 Setting your MWR102 to AP Mode

1 Flip the switch on the side of the device from “Router” to “AP.”

5.2.2 Accessing the Web-Based Management Interface in Access Point Mode

Log in to the Web-Based Management Interface in Access Point mode, do the following:

1 Connect your computer to the LAN port of the MWR102.

2 The default IP address of the MWR102 is “192.168.100.1”. In this case, your computer must have an IP address in the range between “192.168.100.2” and “192.168.100.254”.

3 Click **Start > Run** on your computer in Windows. Type “cmd” in the dialog box. Enter “ipconfig” to show your computer’s IP address. If your computer’s IP address is not in the correct range then see Appendix C for information on changing your computer’s IP address.

4 After you’ve set your computer’s IP address, open a web browser such as Internet Explorer and type “192.168.100.1” as the web address in your web browser.

5.2.3 Configuring your WLAN and Maintenance Settings

The configuration of wireless and maintenance settings in **Access Point** mode is the same as for **Router Mode**.

- See Chapter 7 for information on the configuring your wireless network.

5.3 AP Mode Status Screen

Click Management > Status to open the Status screen

Table 3 Status Screen: Router Mode

LABEL	DESCRIPTION
System Information	
Uptime	This is the total time the MWR102 has been on.
Firmware Version	This is current firmware version.
Firmware Build Time	This is the date/time the current version of the firmware was released.
Operation Mode	This is the device mode to which the MWR102 is set – **AP Mode**.
Wireless Local Network	
Network Band	We provide six modes for your selection: 2.4GHz (B), 2.4 GHz (G), 2.4 GHz (N), 2.4GHz (B+G), 2.4 GHz (G+N), 2.4 GHz (B+G+N). You may select one type of network band from the dropdown menu.
SSID (Name)	Shows the current name of your wireless network.
Channel Number	This shows the channel number the MWR102 is currently using over Wireless LAN.

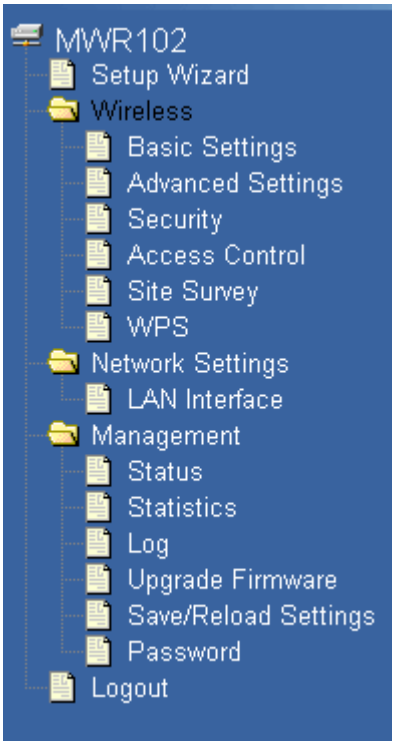
Encryption	This shows the level of wireless security the MWR102 is currently using.
BSSID	This displays the MAC address of the wireless device.
Associated Clients	Displays the number of clients currently associated to the MWR102
Local Network	
Router IP Address	Displays the IP address designated to the MWR102 by your router.
Subnet Mask	Shows what subnet mask the MWR102 is on.
DHCP	This shows the LAN port's DHCP role - **Server** or **None**.
Auto IP Address Diversion	Click the drop down list, you may select "Enabled" to divert the IP Address automatically or select "Disabled" to ban it. When Enabled e, the system will automatically detect conflicts in the WAN and LAN IP. If there are conflicts, the LAN IP and LAN DHCP Range will automatically jump to next subnet to avoid conflicts.
Local MAC Address	This is the MAC address of your MWR102

5.3.1 Navigation Panel

Use the menu in the navigation panel to configure MWR102 features in Access Point mode.

The following screen and table show the features you can configure in Access Point mode.

Figure 5 Navigation Panel



The following table describes the sub-menus.

Table 4 Navigation Panel: Router Mode

LINK	FUNCTION
Setup Wizard	This screen guides you through the setup of the MWR102.
Wireless	
Basic Settings	Use this screen to change the basic wireless settings of the MWR102
Advanced Settings	Use this screen to configure advanced wireless settings
Security	Use this screen to change Wireless Security settings.
Access Control	This page allows control over what devices are allowed to access the

	router.
Site Survey	This page provides a tool to scan the wireless network for nearby routers and APs.
WPS	This screen allows you to change the Wi-Fi Protected Setup settings for the MWR102
Network Settings	
LAN Interface	This screen allows you to configure the parameters for your Local Area Network.
Management	
Status	Shows the current status and basic settings of the travel router
Statistics	Shows packet counts for wired and wireless Ethernet connections.
Log	Set remote log server parameters and view the system log.
Upgrade Firmware	Upgrade the travel router firmware.
Save/Reload Settings	Save the current settings to a backup file, or reload the setting from a previously saved file.
Password	Set or change the travel router ADMINISTRATOR user name and password.
Logout	

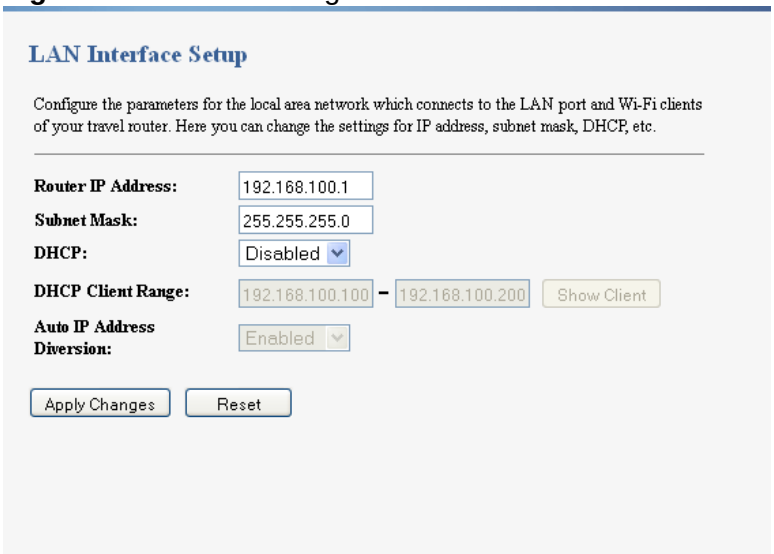
5.4 LAN Screen

Use this section to configure your LAN settings while in **Access Point** mode.

Click **Network Settings > LAN Interface** to see the screen below.

Note: If you change the IP address of the MWR102 in the screen below, you will need to log into the MWR102 again using the new IP address.

Figure 6 Network Settings > LAN Interface



The table below describes the labels in the screen.

Table 5 Network Settings > LAN Interface

LABEL	DESCRIPTION
Router IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.100.2. If you change the IP address you will have to log in again with the new IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your MWR102 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the MWR102.
DHCP	DHCP stands for Dynamic Host Configuration Protocol. It is a protocol for assigning dynamic IP addresses “automatically”.
DHCP Client Range	This field asks you to specify the DHCP Client IP address range (default 100~200). You can also click the “Show Client” button to list those connected DHCP clients. Note: In Router mode, the DHCP Server is enabled by default. However, in AP mode, the DHCP Server disabled by default.
Auto IP Address	Click the drop down list, you may select “Enabled” to divert the IP Address automatically or select “Disabled” to ban it. When Enabled e, the system will

Diversion	automatically detect conflicts in the WAN and LAN IP. If there are conflicts, the LAN IP and LAN DHCP Range will automatically jump to next subnet to avoid conflicts.

6 Tutorials

6.1 Overview

This chapter provides tutorials for your MWR102 as follows:

- Connecting to the Internet from an Access Point
- Configuring Wireless Security Using WPS
- Enabling and configuring wireless security

6.1.1 DSL Modem

If your internet connection comes from a DSL modem you will want to follow these steps to best prepare your modem to connect with the MWR102.

1) Contact your ISP (Internet Service Provider) and ask them to help you “bridge” your DSL modem.

2) Find out from your ISP what the “PPPoE Username and Password” are for your Internet connection.

3) Once the DSL modem has been bridged, connect it (by Ethernet cord) to the WAN port of the MWR102.

4) Open your browser and log into the MWR102. Click on Network Settings > WAN Interface, for the WAN Access Type select “PPPoE” and enter your PPPoE “Username and Password.”

6.1.2 Cable Modem

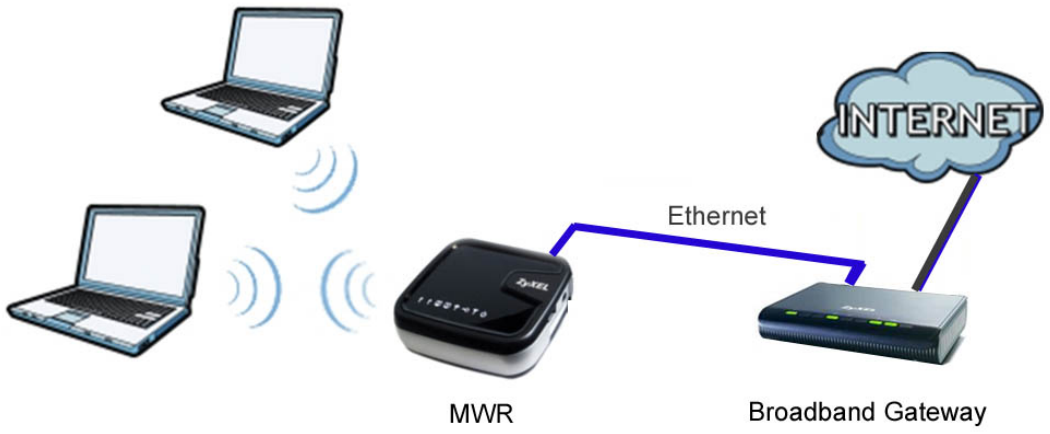
- Connect the cable modem to your MWR102 on the WAN port. Unplug the power to your cable modem. Depending on your cable modem, it may also have a backup battery inside. Remove this battery and completely power down the cable modem. Let it sit from 2 to 3 minutes and then reconnect the battery and power to the cable modem.

- If the router is set with its default settings it should automatically connect to the Internet.

6.2 Connecting to Internet from an Access Point

This section gives you an example of how to set up an access point (**AP**) and wireless client (a notebook (**B**), in this example) for wireless communication. **B** can access the Internet through the access point wirelessly. When the MWR is configured in AP mode, it has to connect to a broadband gateway (wired or wireless router with broadband connection). Local computer(s) can get IP via wireless connection passed by MWR from the broadband gateway, then gain Internet access.

Figure 7 Wireless Access Point mode



6.3 Configuring Wireless Security Using WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the MWR102 as the AP and NWD210N as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the MWR102's interface. This is the more secure method, since one device can authenticate the other.

6.3.1 Push Button Configuration (PBC)

1. Make sure that your MWR102 is turned on and that it is within range of your computer.
2. Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
4. Log into MWR102's Web-Based Management Interface and press the **Start PBC** button in the **Wireless** > **WPS** screen.

Note: Your MWR102 has a WPS button located on its bottom panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The MWR102 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the MWR102 securely.

6.3.2 PIN Configuration

When you use the PIN configuration method, you need to use both MWR102's configuration interface and the client's utilities.

1. Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
2. Enter the PIN number to the **PIN** field in the **Wireless** > **WPS** screen on the MWR102.
3. Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the MWR102's **WPS Station** screen within two minutes.

The MWR102 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the MWR102 securely.

6.4 Enabling and Configuring Wireless Security (No WPS)

Follow the steps below to configure the wireless settings on your MWR102.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web-Based Management Interface through your LAN connection.

1 Open the **Wireless > Security** screen in the AP's Web-Based Management Interface.

2 Choose a Pre-Shared Key format. (Passphrase or Hex)

3 Enter your desired key, then click the **Apply Changes** button.

Figure 8 Tutorial: Wireless > Security

6.5 Configure Your Notebook

Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

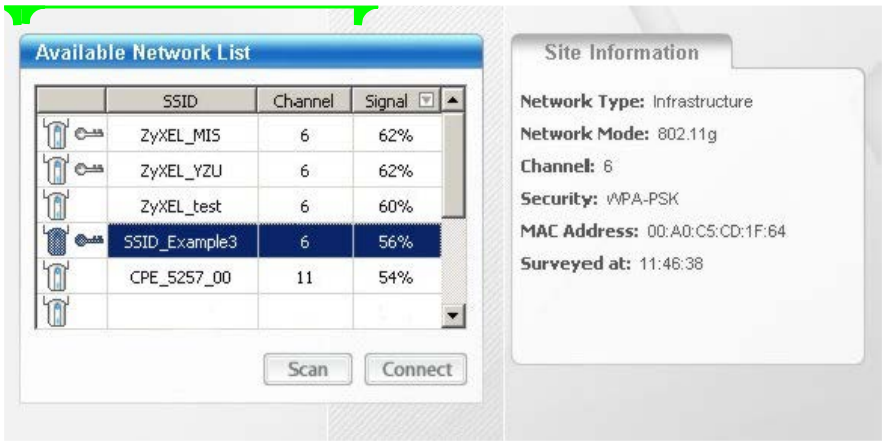
1. The MWR102 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2. Wireless adapters come with software sometimes called a “utility” that you install on your computer. See your wireless adapter’s User’s Guide for information on how to do that.

3. After you’ve installed the utility, open it. If you cannot see your utility’s icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

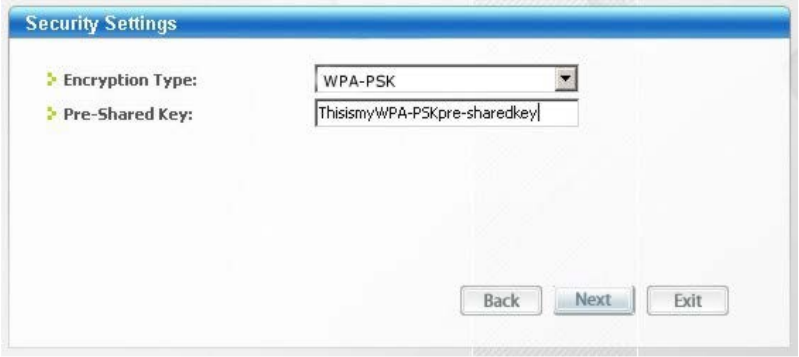
4. Select the MWR102’s SSID and click **Connect**.

Figure 9 Connecting a Wireless Client to a Wireless Network



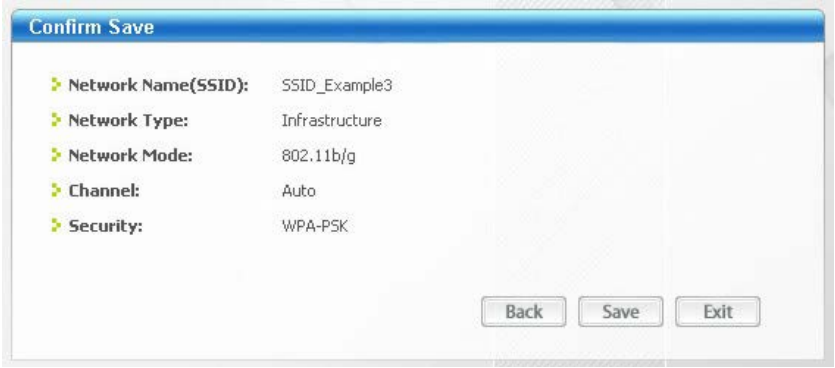
5. Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 10 Security Settings



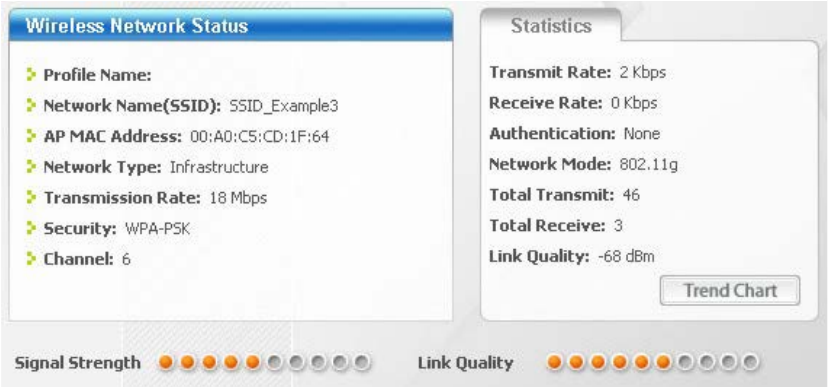
6. The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 11 Confirm Save



7. Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 12 Link Status



If your connection is successful, open your Internet browser and enter http://us.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

Part II: Wireless

7 Wireless

7.1 Overview

This chapter discusses how to configure the wireless network settings in your MWR102. See the appendices for more detailed information about wireless networks.

7.2 What You Can Do

- Use the **Basic Settings** screen to enable the Wireless LAN, enter the SSID and select the channel width.
- Use the **Advanced Settings** screen to set RF output power and set the RTS Threshold.
- Use the **Security** screen to set encryption type and passphrase.
- Use the **Access Control** screen to whitelist and blacklist devices on your network.
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually.

7.3 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.

7.3.1 Wireless Security Overview

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

7.3.1.1 SSID

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

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

7.3.1.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

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

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

7.3.1.3 Encryption

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

The types of encryption you can choose depend on the type of user authentication.

---

[1]Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2]Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

Table 6 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION
Weakest	No Security
↕	WEP
	WPA-Personal (TKIP) WPA-Enterprise
Strongest	WPA2-Personal (AES) WPA2-Enterprise

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA-PSK. Therefore, you should set up **WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-Personal/Enterprise** or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

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

7.3.1.4 WPS

Wi-Fi Protected Setup (WPS) is an industry standard specification, defined by the Wi-Fi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you 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.

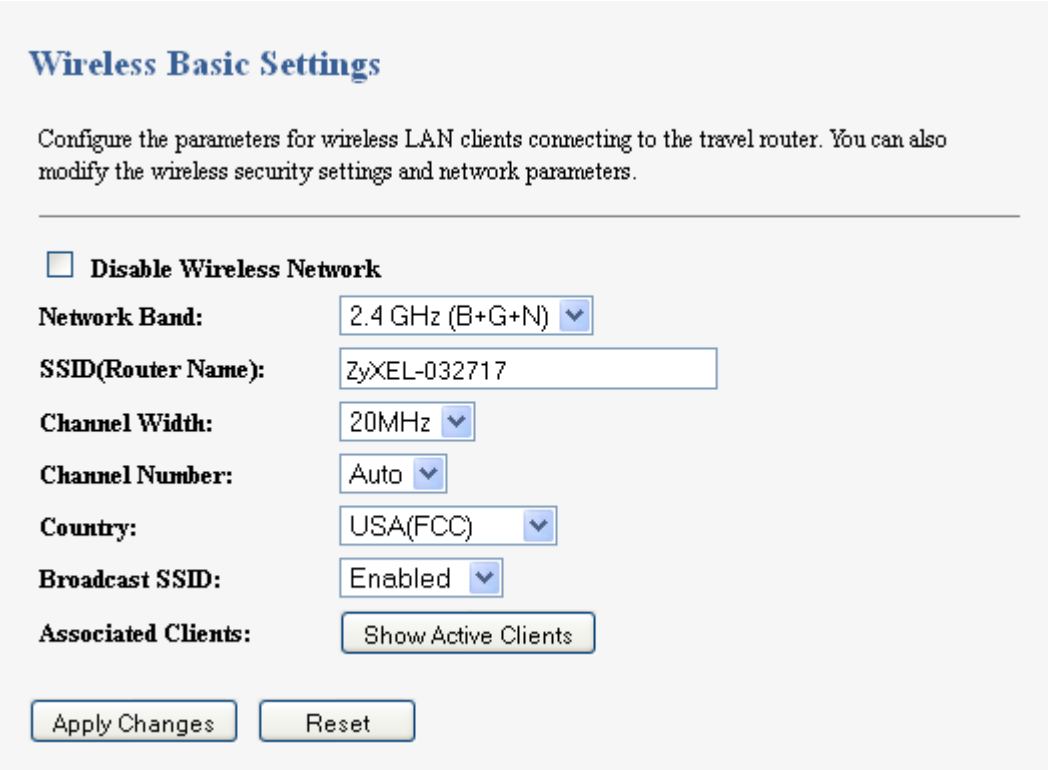
7.4 General Wireless LAN Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the channel.

Note: If you are configuring the MWR102 from a computer connected to the wireless LAN and you change the MWR102's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the MWR102's new settings.

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

Figure 13 Wireless > Basic Settings



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

Table 7 Wireless > Basic Settings

LABEL	DESCRIPTION
Wireless Basic Settings	

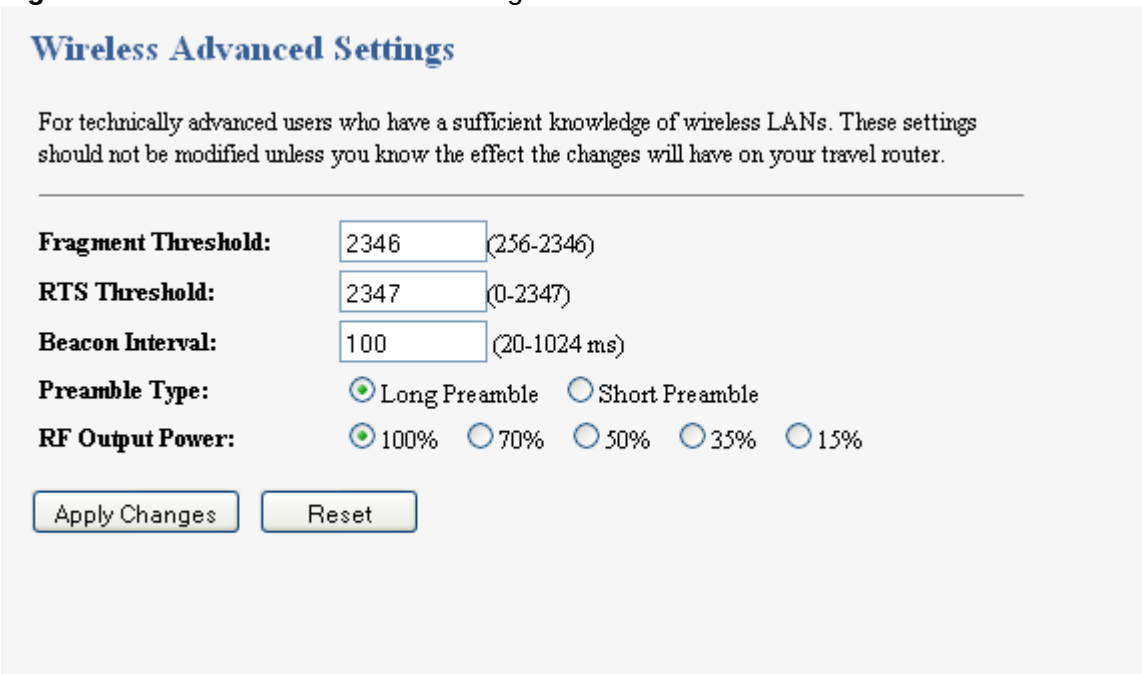
Network Band	Allows you to choose between Wireless B/G/N functionality.
Channel Width	Allows you to choose between the 20MHz and 40MHz channel.
Channel Number	This displays the channel the MWR102 is currently using.
Country	Allows you to set your country**.**
Broadcast SSID	Set whether or not the MWR102 is discoverable.
Associated Clients	The Show Clients button shows all clients associated with the MWR102.

7.5 Wireless LAN Advanced Settings

Use this screen to allow wireless advanced features, such as setting output power and the RTS Threshold

Click **Wireless** > **Advanced Settings**. The screen appears as shown.

Figure 14 Wireless > Advanced Settings



The following table describes the labels in this screen.

Table 8 Wireless > Advanced Settings

LABEL	DESCRIPTION
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.
RTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100ms) is recommended.
Preamble Type	The length of CRC blocks in the frames during the wireless communication.

Output Power	Set the output power of the MWR102 in this field. If there is a high density of APs in an area, decrease the output power of the MWR102 to reduce interference with other APs. Select one of the following **100%**, **70%**, **50%**, **35%**, or **15%**. See the product specifications for more information on your MWR102's output power.
Apply Changes	Click **Apply Changes** to save your changes back to the MWR102.
Reset	Click **Reset** to reload the previous configuration for this screen.

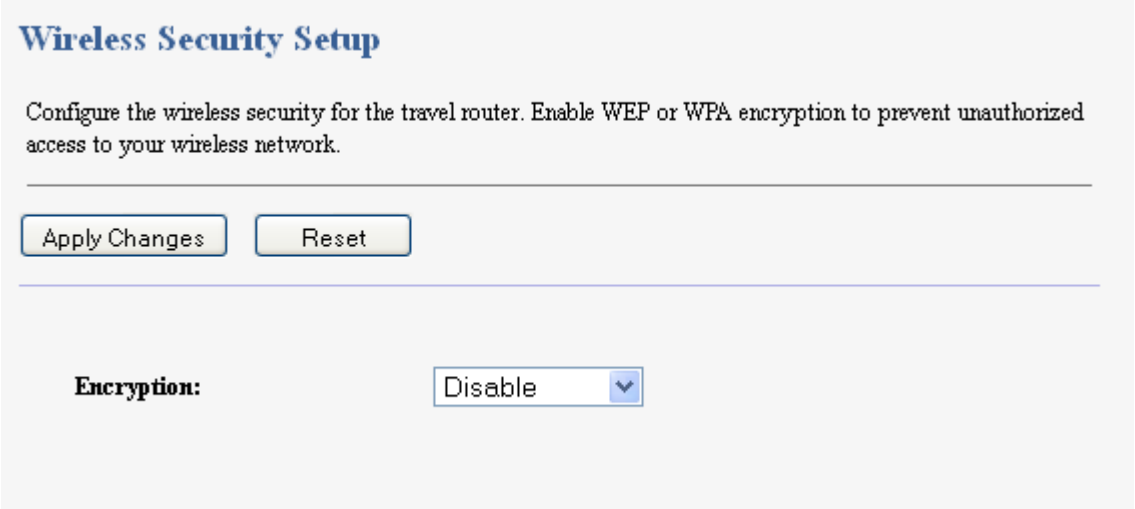
7.6 Security

7.6.1 Disabling Security

Select **Disable** to allow wireless stations to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your MWR102, your network is accessible to any wireless networking device that is within range.

Figure 15 Wireless > Security

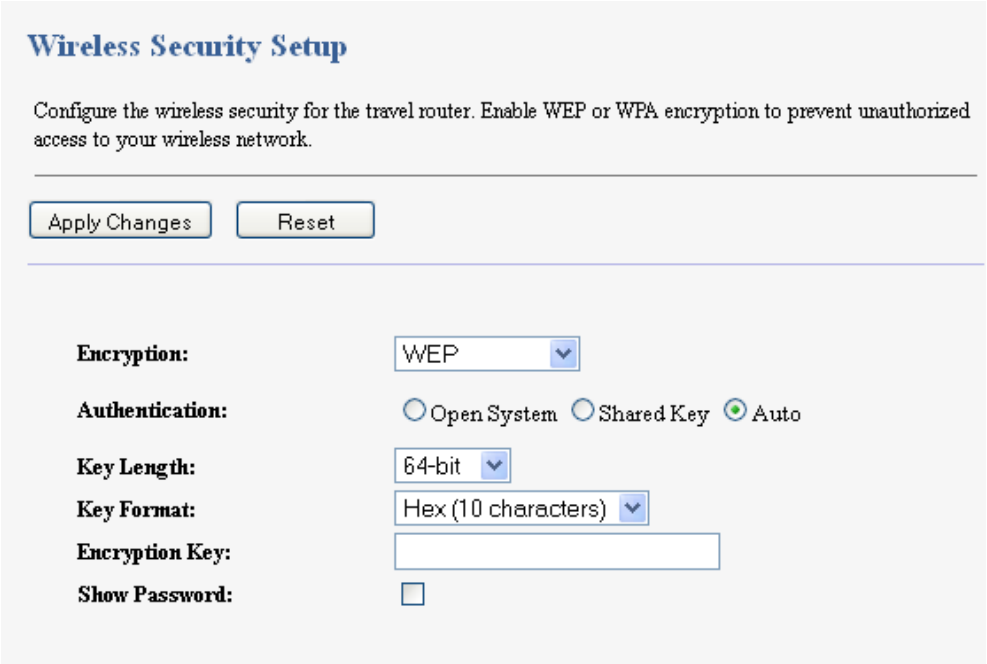


7.6.2 WEP Encryption

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.

In order to configure and enable WEP encryption, click **Wireless** > **Security** to display the **Security** screen. Select **WEP** from the **Encryption** list.

Figure 16 Wireless > Security: WEP



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

Table 9 Wireless > Security: WEP

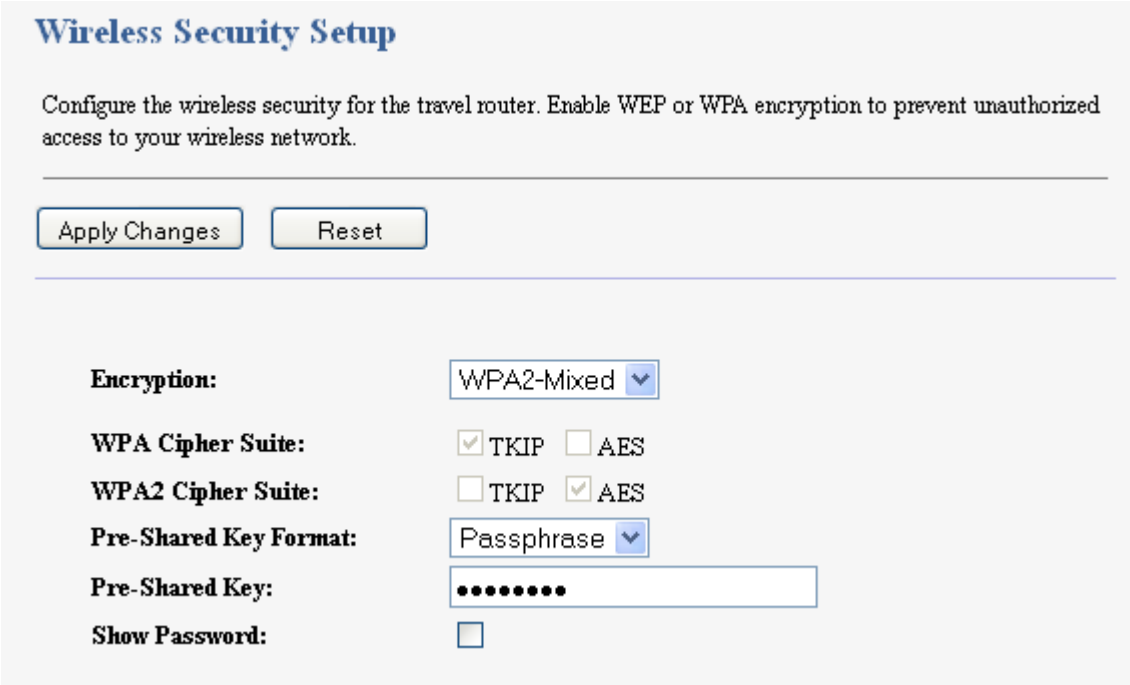
LABEL	DESCRIPTION
Encryption	Select **Static WEP** to enable data encryption.
Authentication Method	Select Open **System, Auto,** or **Shared Key**. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.

Key Length	Select **64-bit** or **128-bit**. This dictates the length of the security key that the network is going to use.
Key Format	Select ASCII (5 Characters) or Hex (10 Characters) from the dropdown menu.
Encryption Key	Enter a Passphrase. A passphrase functions like a password. In WEP security mode, it is further converted by the MWR102 into a complicated string that is referred to as the “key”. This key is requested from all devices wishing to connect to a wireless network.
Apply Changes	Click **Apply** to save your changes back to the MWR102.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.6.3 WPA-PSK/WPA2-PSK/WPA2-Mixed

Click **Wireless** > **Security** to display the **Security** screen. Select **WPA-PSK, WPA2-PSK,** or **WPA2-Mixed** from the **Security Mode** list.

Figure 17 Wireless > Security: WPA-PSK/WPA2-PSK/WPA2-Mixed



The following table describes the labels in this screen.

Table 10 Wireless > Security: WPA-PSK/WPA2-PSK/WPA2-Mixed

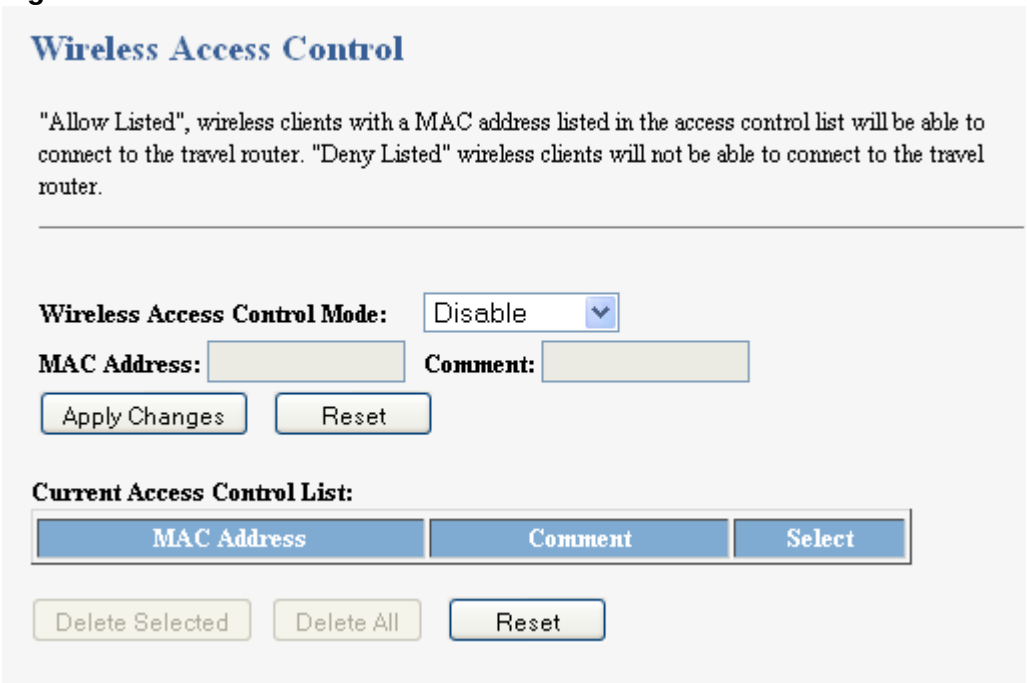
LABEL	DESCRIPTION
Encryption	Select **WPA-PSK, WPA2-PSK** or **WPA2-Mixed** to enable data encryption.
Pre-shared Key Format	This field allows you to choose between a passphrase and HEX as your Sre-Shared Key Format.
Pre-Shared Key	**WPA-PSK/WPA2-PSK/WPA2-Mixed** use a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Apply Changes	Click **Apply Changes** to save your changes back to the MWR102.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.7 Access Control

The Access Control screen allows you to configure the MWR102 to give exclusive access to devices (Allow) or exclude devices from accessing the MWR102 (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your MWR102's MAC filter settings, click **Wireless** > **Access Control**. The screen appears as shown.

Figure 18 Wireless > Access Control



The following table describes the labels in this menu.

Table 11 Wireless > Access Control

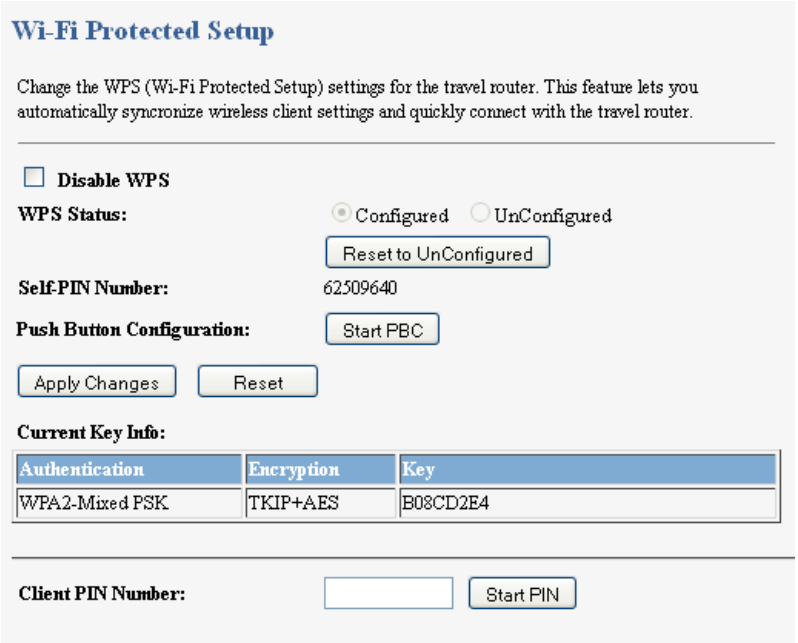
LABEL	DESCRIPTION
Wireless Access Control Mode	Define whether entered MAC addresses will be whitelisted or blacklisted.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the MWR102 in this field. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. Click **Apply Changes**.
Comment	Enter any notes about the device being black/whitelisted in this field.
Delete Selected	Delete single MAC addresses from the list.
Delete All	Delete all MAC addresses from the list.

Apply Changes	Click **Apply** to save your changes back to the MWR102.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.8 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Wireless** > **WPS**.

Figure 19 Wireless > WPS



The following table describes the labels in this screen.

Table 12 Network > Wireless LAN > WPS

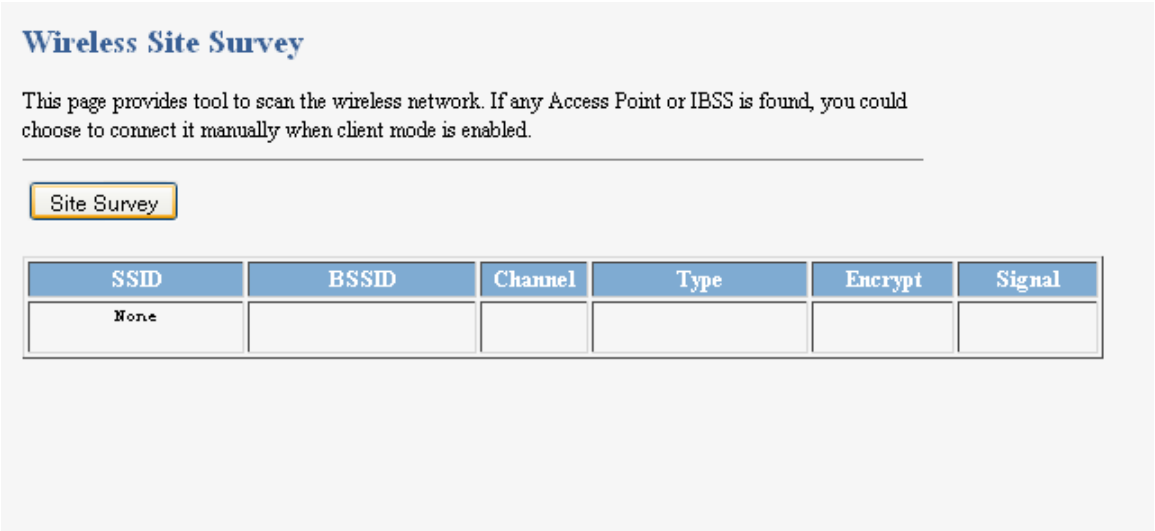
LABEL	DESCRIPTION
Wi-Fi Protected Setup	
Disable WPS	Select this to disable the WPS feature.

Status	This displays **Configured** when the MWR102 has connected to a wireless network using WPS. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the MWR102 or you click **Reset to Unconfigured** to remove the configured wireless and wireless security settings.
Self-PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
Reset to Unconfigured	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the MWR102.
Push Button Configuration	Press this button to begin the PBC process.
Current Key Info	The authentication type, encryption type, and key are displayed here if security settings are configured.
Client PIN number	This is where the PIN is displayed when using PIN setup. To generate a PIN, press the **Start PIN** button.
Apply	Click **Apply** to save your changes back to the MWR102.
Refresh	Click **Refresh** to get this screen information afresh.

7.9 Wireless Site Survey (AP Mode Only)

Use this screen to view nearby wireless networks. Go to **Wireless > Site Survey** to open the following screen.

Figure 20 Wireless > Site Survey



The following table describes the labels in this screen.

Table 13 Wireless > Site Survey

LABEL	DESCRIPTION
Wireless Site Survey	
SSID	This displays the Network Name (SSID) of the wireless networks close to you.
BSSID	This displays the MAC address of the wireless device listed.
Channel	This displays the wireless channel used by the wireless network.
Type	This displays the network type being used by the wireless network.
Encrypt	This displays the encryption type used by the wireless network.
Signal	This displays the strength of the wireless network signal.

8 Network Settings

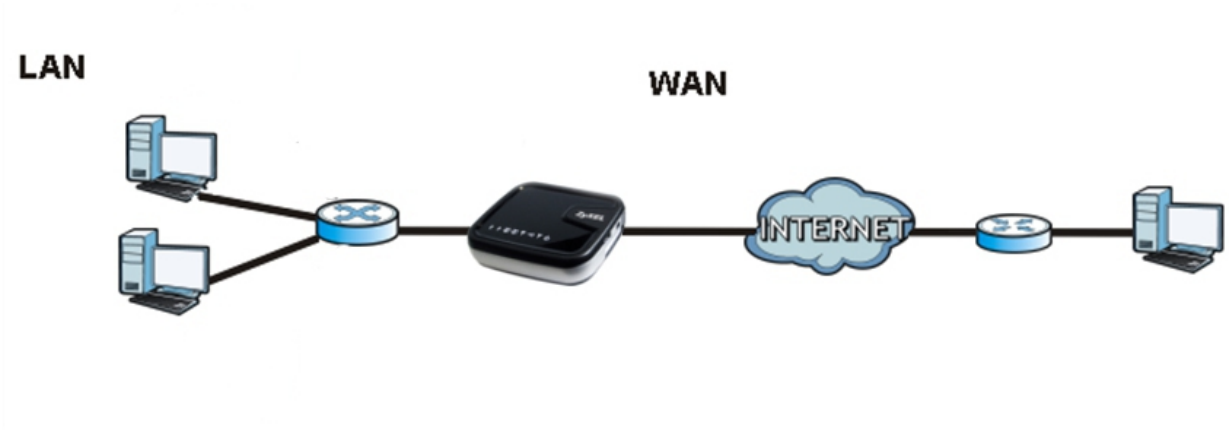
8.1 Overview

This chapter discusses the MWR102's **Network Settings** screens. Use these screens to configure your LAN and WAN 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.

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.

Figure 21 LAN and WAN



8.2 What You Can Do

- Use the **LAN Interface Setup** screen to modify your router's IP address, DHCP Settings, and Subnet Mask
- Use the **WAN Interface Setup** screen to modify your DHCP access type (DHCP client, Static IP, or PPoE), MTU Size, DNS Settings, and MAC address.

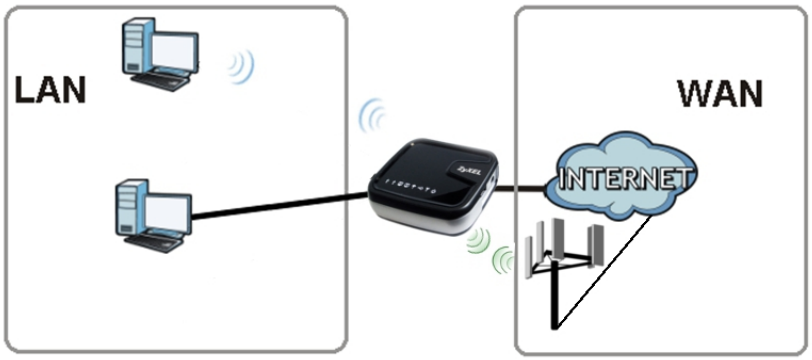
8.3 What You Need To Know

The information in this section can help you configure the screens for your WAN and LAN connections.

8.3.1 Configuring Your Internet Connection

The actual physical connection determines whether the MWR102 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 22 LAN and WAN IP Addresses (implies wired WAN connection)



The LAN parameters of the MWR102 are preset in the factory with the following values:

- IP address of 192.168.100.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.100.33.

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

8.3.2 WAN MAC Address

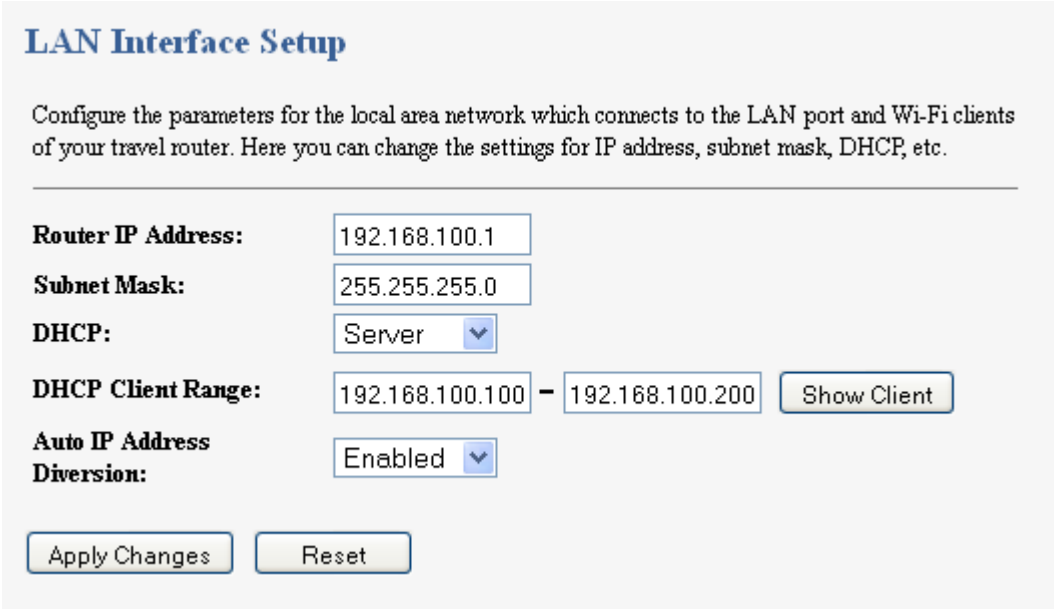
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

8.4 LAN Interface

The LAN Interface Setup screen allows you to set up your LAN interface, the private IP of your router's LAN port, and the subnet mask of your LAN segment. Go to **Network > LAN Interface** to access the following screen.

Figure 23 Network > LAN Interface



The following table describes the labels in this screen.

Table 14 Network > LAN Interface

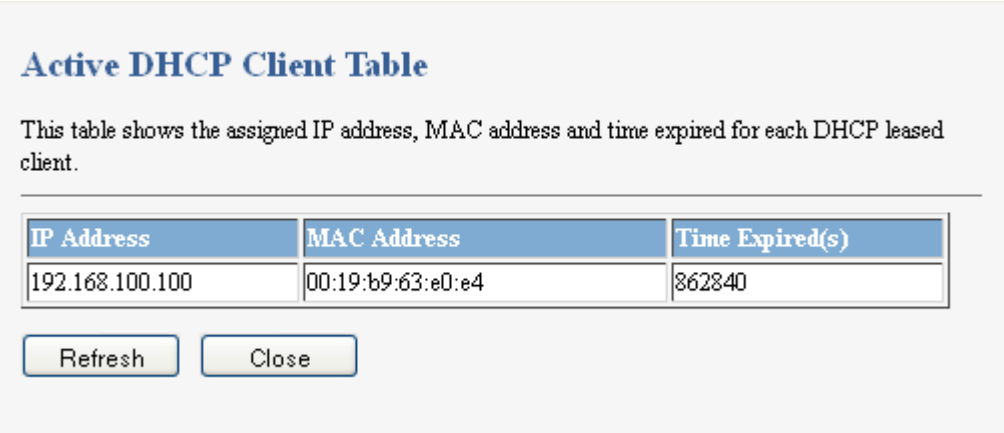
Items	Information
Router IP Address	The IP of your Router LAN port (default 192.168.100.1).
Subnet Mask	Subnet Mask of you LAN (default 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.
DHCP	DHCP stands for Dynamic Host Configuration Protocol. It is a protocol for assigning dynamic IP addresses "automatically".
DHCP Client Range	This field asks you to specify the DHCP Client IP address range (default 100~200). You can also click the "Show Client" button to list those connected DHCP clients. **Note**: In Router mode, the DHCP Server is enabled by default. However, in AP mode, the DHCP Server disabled by

	default.
Auto IP Address Diversion	Click the drop down list, you may select “Enabled” to divert the IP Address automatically or select “Disabled” to ban it. When Enabled, the system will automatically detect conflicts in the WAN and LAN IP. If there are conflicts, the LAN IP and LAN DHCP Range will automatically jump to next subnet to avoid conflicts.

8.4.1 Active DHCP Client List

This window pops up after clicking the **Show Client** button.

Figure 24 Network > LAN Interface > Show Client



The following table describes the labels in this screen.

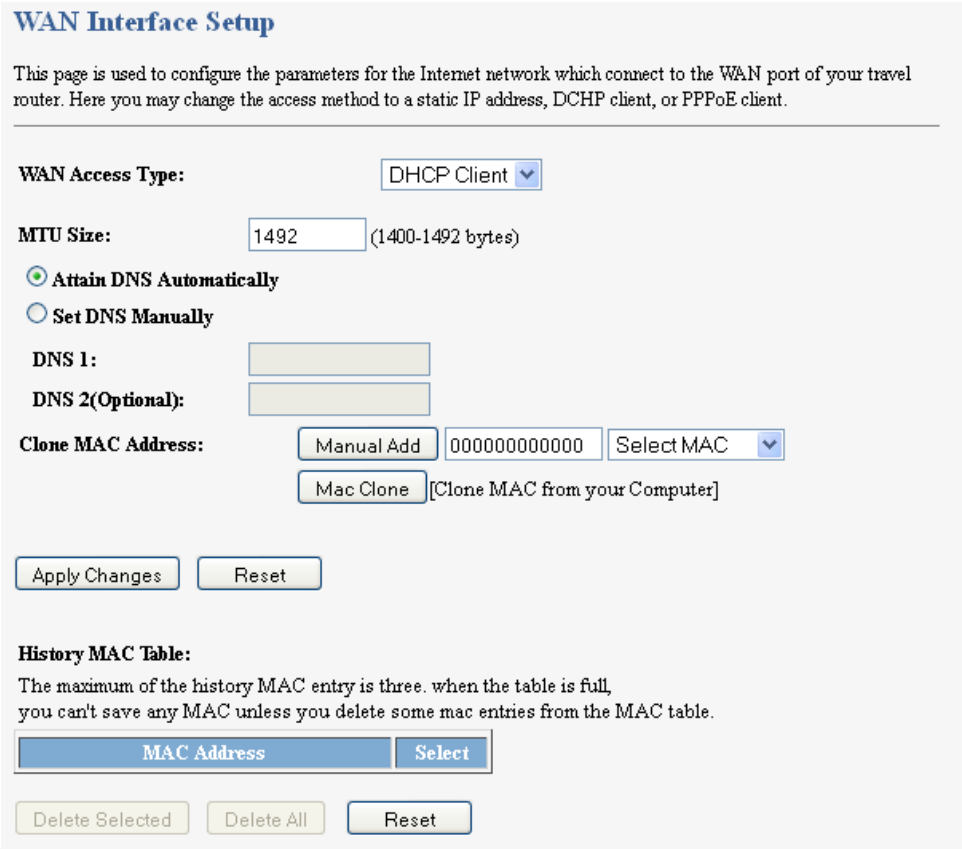
Table 15 Network > LAN Interface > Show Client

Items	Information
IP Address	The IP of the connected client.
MAC Address	The MAC Address of the connected client.
Time Expired	The amount of seconds the client has been connected.
Refresh	This button refreshes the list with the most recent information.
Close	Closes the Active DHCP Client Table.

8.5 WAN Interface

This page allows users to configure WAN settings. You may select the Internet connection type from the drop down list next to “WAN Access Type” and configure the parameters for each mode. Go to **Network Settings > WAN Interface** to open the following screen.

Figure 25 Network > WAN Interface



The following table describes the labels in this screen.

Table 16 Network > WAN Interface

Items	Information
WAN Access Type	Select to access the WAN as Static, DHCP Client or PPPoE.
Internet IP Address	The IP address provided by your Internet Service Provider (ISP).
Subnet Mask	The Subnet Mask provided by your Internet Service Provider (ISP).
Default Gateway	The Default Gateway provided by your Internet Service

	Provider (ISP).
MTU Size	The Maximum packet size the router will transmit. Any packet over the specified size will be chopped into a smaller size before sending. Larger packet size will enhance performance. Enter the MTU number in the blank to set the limitation.
Clone MAC Address	There are two ways to clone a MAC address. One way is to directly input a MAC address into the text box. To store a MAC address, click the 'Manual Add' button and add it to the “History MAC Table.” The second way is to click the 'MAC Clone' button. This will copy the MAC address from your network card. Note: The 'History MAC Table' can save a maximum of three MAC Addresses.
History MAC Table	To Delete MAC Addresses you have added before, mark the check box on the right hand and click “Delete Selected.” If you want to delete all saved MAC Addresses, click “Delete All.”

Part III: Security

MAC Filtering

9 MAC Filtering

9.1 Overview

This chapter shows you how to enable and configure MAC address filtering that allows your MWR102 to permit and deny access to specific devices on your network.

Enable MAC Filtering to restrict the passage of certain types of data packets from your local network to the Internet through the travel router. Use of such filters can be helpful in securing or restricting your local network.

By default the firewall allows all traffic that originates from your LAN computers to go to all networks.

9.2 What You Can Do

- Use the **MAC Filtering** screen to enable or disable MAC Filtering, and modify what devices are restricted to the local network.

9.3 What You Need To Know

The MWR102's MAC Filtering feature physically separates the LAN and the WAN of selected devices, and acts as a secure gateway to keep selected devices from having access to the WAN.

The MWR102 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a gateway for all data passing between the Internet and the LAN.

The MWR102 has one Ethernet WAN port and one Ethernet LAN port, 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. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web unless their MAC address is blocked by the MWR102.

9.4 MAC Filtering

This page allows users to restrict data from passing onto the internet from certain devices. Go to **Firewall > MAC Filtering** to open the following screen.

Figure 26 Firewall > MAC Filtering

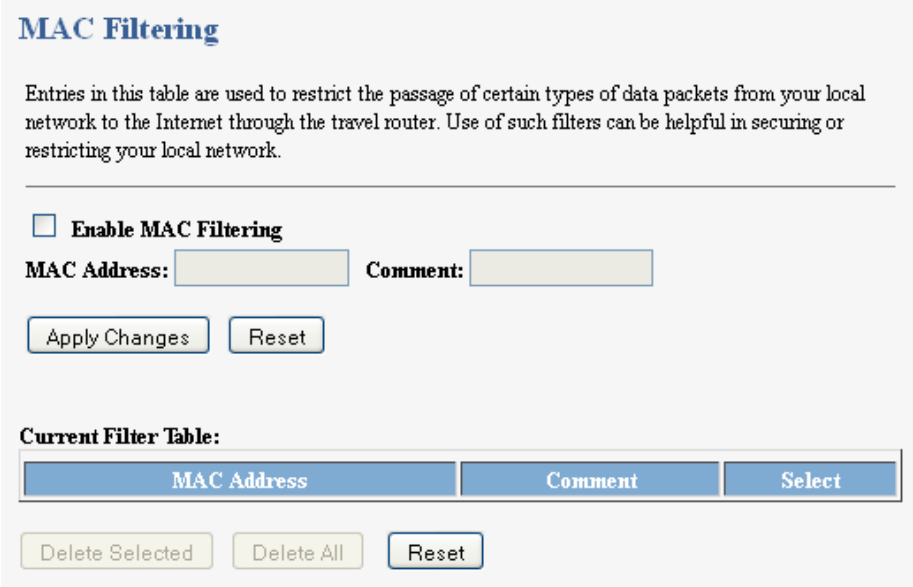


Table 17 Firewall > MAC Filtering

Items	Information
Enable MAC Filtering	Mark to enable MAC Filtering, and clear to disable.
MAC Address	Fill in the MAC address of wireless stations you want to forbid Internet access to.
Comment	Input any text to describe the name of the device, reason for filtering, etc.
Current Filter Table	Lists MAC Filter Settings you have added before. To delete settings on the list, click the check box next to the item and click “Delete Selected.” If you want to delete all saved MAC addresses, click “Delete All.”
Enable MAC Filtering	Mark to enable MAC Filtering, and clear to disable.
MAC Address	Fill in the MAC address of wireless stations you want to forbid Internet access to.
Comment	Input any text to describe the name of the device, reason for filtering, etc.

Part IV: Management

10 Status

10.1 Overview

This chapter discusses how to access and interpret information about the MWR102.

10.2 What You Can Do

- Use the **Status** screen to view the current status and basic settings of the device.

10.3 Status Screen

This information page shows the current status and basic settings of this device.

Click **Management** > **Status** to open the Status screen.

Figure 27 Management > Status

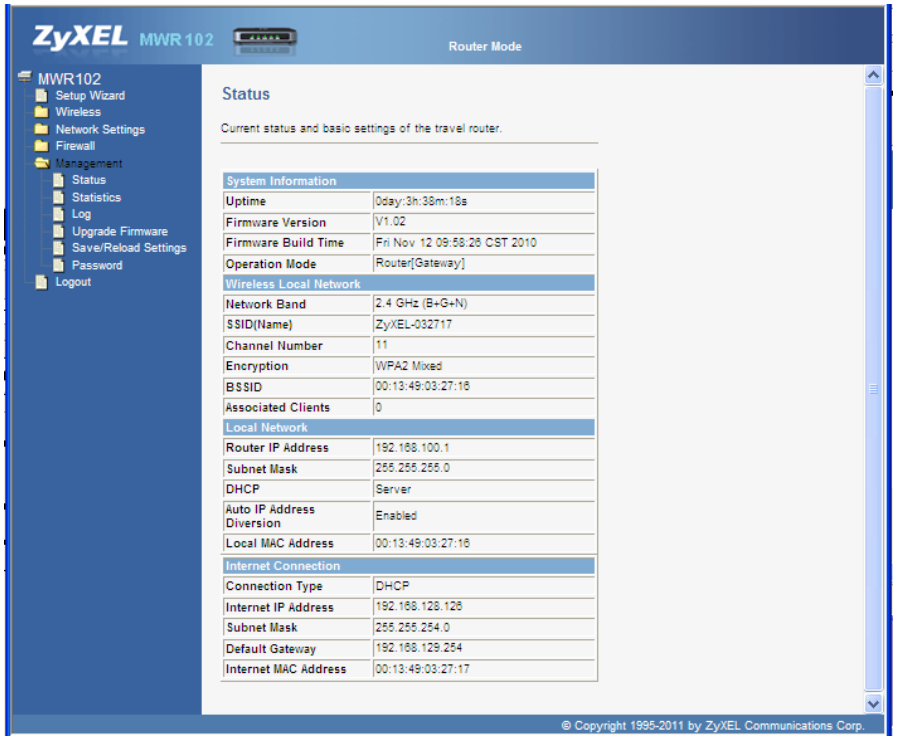


Table 18 Management > Status

LABEL	DESCRIPTION
System Information	
Uptime	This is the total time the MWR102 has been on.
Firmware Build Time	This is the date/time the current version of the firmware was released.
Operation Mode	This is the device mode to which the MWR102 is set – **Router Mode**.
Wireless Local Network	
Network Band	We provide six modes for your selection: 2.4GHz (B), 2.4 GHz (G), 2.4 GHz (N), 2.4GHz (B+G), 2.4 GHz (G+N), 2.4 GHz (B+G+N). You may select one type of network band from the dropdown menu.
SSID (Name)	Shows the current name of your wireless network.
Channel Number	This shows the channel number the MWR102 is currently using over Wireless LAN.
Encryption	This shows the level of wireless security the MWR102 is currently using.
BSSID	This displays the MAC address of the wireless device.
Associated Clients	Displays the number of clients currently associated to the MWR102
Local Network	
Router IP Address	Displays the IP address designated to the MWR102 by your router.
Subnet Mask	Shows what subnet mask the MWR102 is on.
DHCP	This shows the LAN port's DHCP role - **Server** or **None**.
Internet Connection	
Connection Type	Shows connection type: Static, DHCP Client or PPPoE.

Internet IP Address	The IP address provided by your Internet Service Provider (ISP).
Subnet Mask	The Subnet Mask provided by your Internet Service Provider (ISP).
Default Gateway	The Default Gateway provided by your Internet Service Provider (ISP).
Internet MAC Address	MAC Address of the device on the internet.

11 Statistics

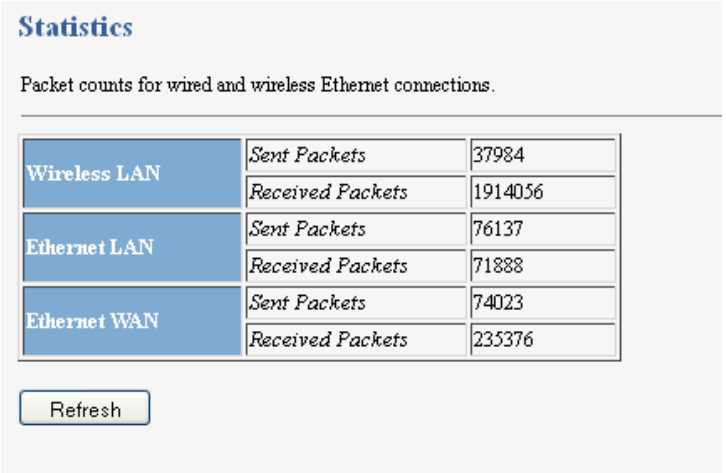
11.1 Overview

This page shows users data transfer information, and monitors packets sent and received

11.2 Statistics Screen

. Click **Management > Statistics** to access the Statistics screen.

Figure 28 Management > Statistics



The following table describes the labels in this screen.

Table 19 Management > Statistics

LABEL	DESCRIPTION
Wireless LAN	This table shows the number of packets sent over the Wireless LAN.
	This table shows the number of packets received over the Wireless LAN.
Ethernet LAN	This table shows the number of packets sent over Ethernet LAN.

	This table shows the number of packets received over Ethernet LAN.
Ethernet WAN	This table shows the number of packets sent over the Ethernet WAN.
	This table shows the number of packets received over the Ethernet WAN.
Refresh	This button updates the Statistics screen to show the current number of packets sent and received.
Clear	This button clears the system log.

12 Log

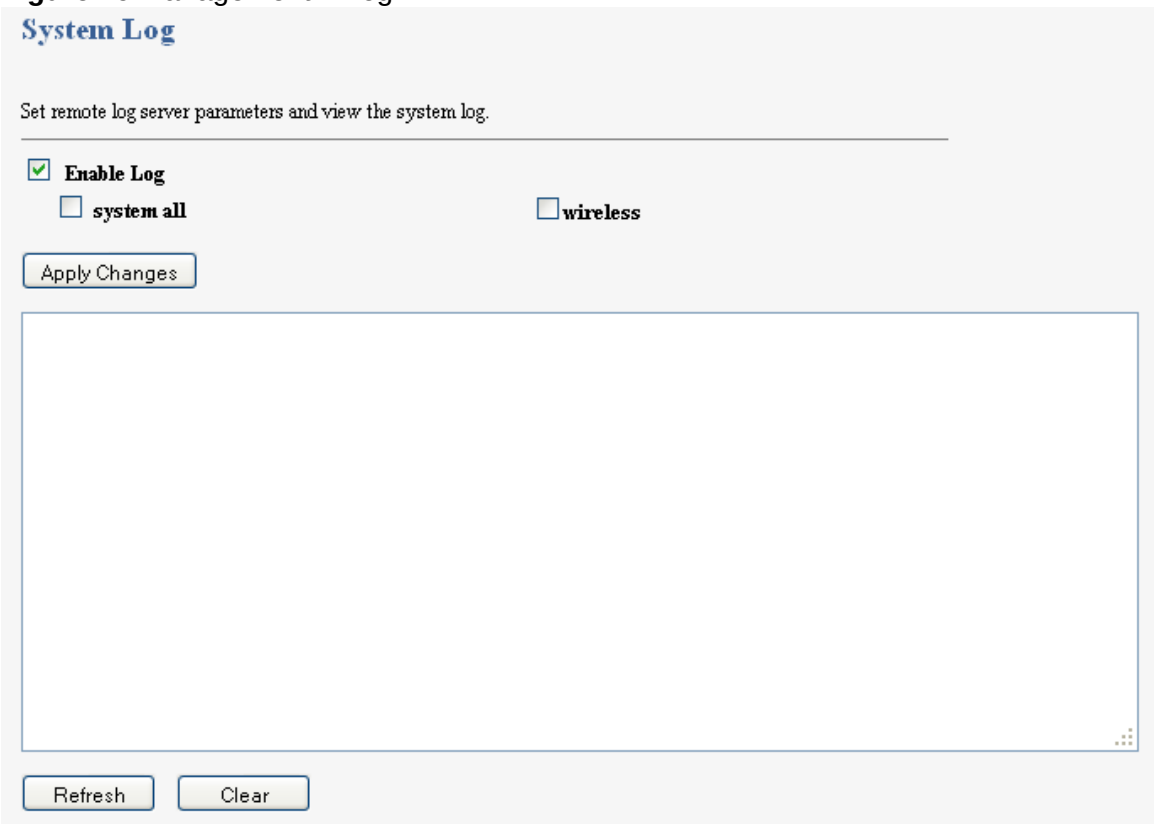
12.1 Overview

This page shows current activity on the router, and allows you to set what information the router logs.

12.2 Log Screen

Click **Management > Log** to access the Log screen.

Figure 29 Management > Log



The following table describes the labels in this screen.

Table 20 Management > Log

LABEL	DESCRIPTION
Enable Log	Checking this box enables system log functionality.
System All	Checking this box shows all logged information passing through the device.
Wireless	Checking this box shows only the information passing through the wireless network.
Apply Changes	This button applies the changes made above. The MWR102 must reboot in order for these changes to take affect.
Refresh	This button updates the System Log to show the most recent information to pass through the device.
Clear	This button clears the system log.

13 Upgrade Firmware

13.1 Overview

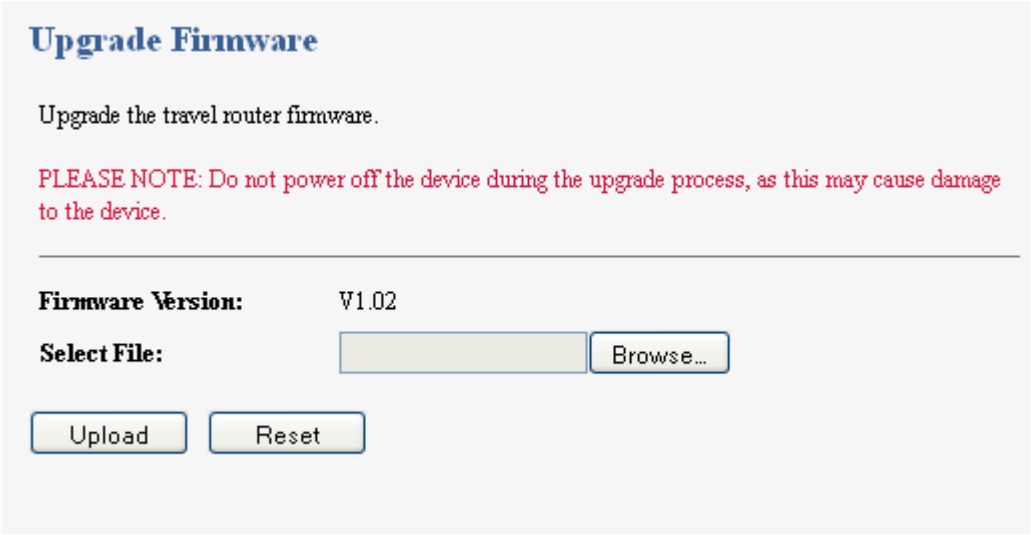
Occasionally, a firmware upgrade may be issued to address bugs or add functionality. This chapter discusses how to upgrade to the MWR102's most recent firmware.

Find firmware at http://us.zyxel.com/Support/Download-Library.aspx. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

13.2 Upgrade Firmware Screen

Click **Management > Upgrade Firmware**. Follow the instructions in this screen to upload firmware to your MWR102.

Figure 30 Management > Upgrade Firmware



The following table describes the labels in this screen.

Table 21 Management > Upgrade Firmware

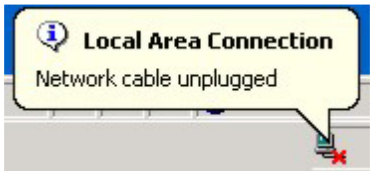
LABEL	DESCRIPTION
Select File	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click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

Note: Do not turn off the MWR102 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the MWR102 again.

The MWR102 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 31 Network Temporarily Disconnected



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

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware** screen.

14 Save/Reload Settings

14.1 Overview

This chapter shows you how to backup, restore and reset your MWR102.

14.2 What You Can Do

Save Settings to File allows you to back up (save) the MWR102's current configuration to a file on your computer. Once your MWR102 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.

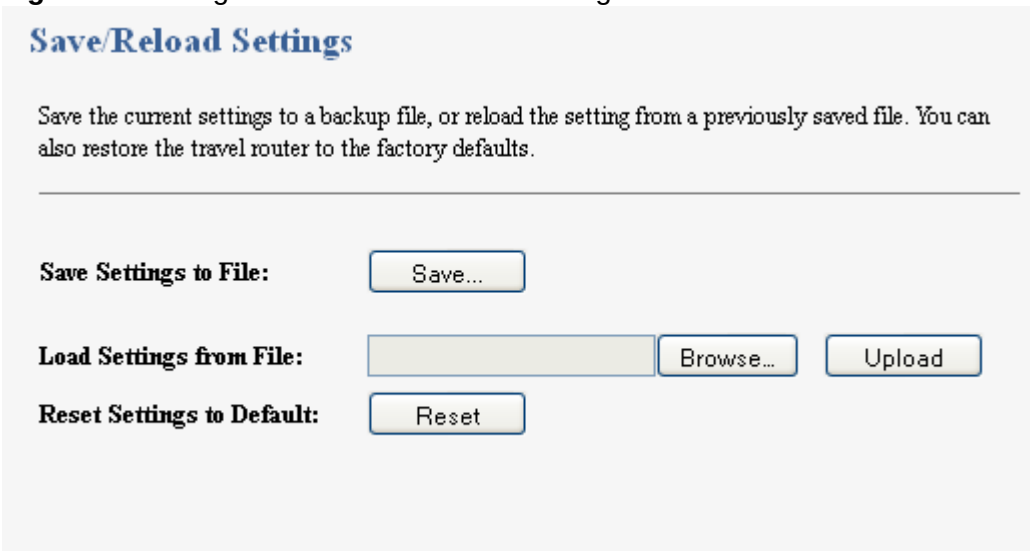
Load Settings from File allows you to upload a new or previously saved configuration file from your computer to your MWR102.

Reset Settings to Default allows you to restore the configuration to factory default.

14.3 Save/Reload Settings Screen

Click **Management > Save/Reload Settings**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 32 Management > Save/Reload Settings



The following table describes the labels in this screen.

Table 22 Management > Save/Reload Settings

LABEL	DESCRIPTION
Save…	Click **Save…** to save the MWR102's current configuration to your computer.
Load Settings from File	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the MWR102 while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the MWR102 again. The MWR102 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.

Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the MWR102 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your MWR102. Refer to the Web-Based Management Interface Chapter for more information on the **RESET** button.

Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default MWR102 IP address (192.168.100.1). See Appendix C for details on how to set up your computer's IP address.

15 Password

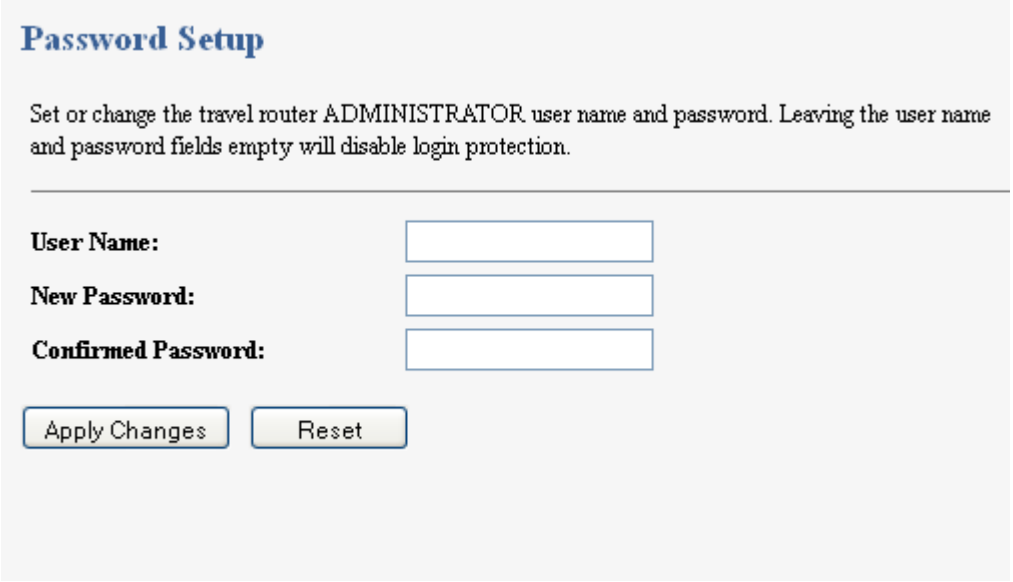
15.1 Overview

This chapter discusses management of the MWR102's Administrator user name and password. These are the User name and Password used to access the Web-based Management interface and make changes to your router.

15.2 Password Screen

Click **Management** > **Password**.

Figure 33 Management > Password



The following table describes the labels in this screen.

Table 23 Management > Password

LABEL	DESCRIPTION
User Name	Type the user name you wish to use to log into the MWR102.
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.
Confirmed Password	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the MWR102.
Reset	Click **Reset** to begin configuring this screen afresh.

Part V: Troubleshooting

16 Troubleshooting

16.1 Overview

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

- Power, Hardware Connections, and LEDs
- Internet Access
- Resetting MWR102
- Wireless Router/AP Troubleshooting

16.2 Power, Hardware Connections, and LEDs

The MWR102 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the MWR102.
2. Make sure the power adaptor or cord is connected to the MWR102 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the MWR102.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.4.
2. Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor to the MWR102.

5 If the problem continues, contact the vendor.

16.3 MWR102 Access and Login

I don't know the IP address of my MWR102.

1 The default IP address is **192.168.100.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the MWR102 by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the MWR102 (it depends on the network), so enter this IP address in your Internet browser. Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Local Network** table in the **Status** screen. Your MWR102's IP address is available in the **Local Network** table.

- If the **DHCP** setting under **Local Network** is **None**, your device has a fixed IP address.
- If the **DHCP** setting under **Local Network** is **Client**, then your device receives an IP address from a DHCP server on the network.

3 If your MWR102 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your MWR102 to change all settings back to their default. This means your current settings are lost. See Resetting MWR102 in the **Troubleshooting** section for information on resetting your MWR102.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Resetting MWR102.

I cannot see or access the **Login** screen in the Web-Based Configuration Utility.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.100.1.
- If you changed the IP address (Chapter 5), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for “I don’t know the IP address of my MWR102”

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix A.

4 Make sure your computer is in the same subnet as the MWR102. (If you know that there are routers between your computer and the MWR102, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address.
- If there is no DHCP server on your network, make sure your computer’s IP address is in the same subnet as the MWR102. See Appendix B.

5 Reset the device to its factory defaults, and try to access the MWR102 with the default IP address.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestion

I can see the **Login** screen, but I cannot log in to the MWR102.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

3 Disconnect and re-connect the power adaptor or cord to the MWR102.

4 If this does not work, you have to reset the device to its factory defaults. See Resetting MWR102.

16.4 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 Check your System Operation Mode setting.

- Select **Router** if your device routes traffic between a local network and another network such as the Internet.
- Select **Access Point** if your device bridges traffic between clients on the same network.

6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the MWR102), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4.

2 Reboot the MWR102.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.4. If the MWR102 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving the MWR102 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Reboot the MWR102.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.
- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

16.5 Resetting MWR102 to Factory Defaults

If you reset the MWR102, you lose all of the changes you have made. The MWR102 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the MWR102,

1. Make sure the power LED is on.
2. Press the **RESET** button for longer than 1 second to restart/reboot the MWR102.
3. Press the **RESET** button for longer than five seconds to set the MWR102 back to its factory-default configurations.

If the MWR102 restarts automatically, wait for the MWR102 to finish restarting, and log in to the Web-Based Configuration Interface. The password is “1234”.

If the MWR102 does not restart automatically, disconnect and reconnect the MWR102’s power. Then, follow the directions above again.

16.6 Wireless Router/AP Troubleshooting

I cannot access the MWR102 or ping any computer from the WLAN (wireless AP or router).

1. Make sure the wireless LAN is enabled on the MWR102
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the MWR102.

4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the MWR102.

5. Check that both the MWR102 and your wireless station are using the same wireless and wireless security settings.

6. Make sure you allow the MWR102 to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.

I can't access the Web -Based Configuration Interface after switching to AP mode.

When you change from router mode to AP mode, your computer must have an IP address in the range between "192.168.100.3" and "192.168.100.254".

Refer to Appendix C for instructions on how to change your computer's IP address.

The following tables summarize the MWR102's hardware and firmware features.

17 Product Specifications

The following tables summarize the MWR102's hardware and firmware features.

Table 24 Hardware Features

Dimensions (W x D x H)	162 mm x 115 mm x 33 mm
Weight	252 g
Power Specification	Input: 100~240 V AC, 50~60 Hz Output: 5V DC 2A
Ethernet ports	Auto-negotiating: 10 Mbps, 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
LEDs	PWR, LAN, WAN, WLAN, WPS
Reset Button	The reset button is built into the bottom panel. Use this button to restore the MWR102 to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Operation Environment	Temperature: 0º C ~ 40º C / 32ºF ~ 104ºF Humidity: 10% ~ 90%
Storage Environment	Temperature: -20º C ~ 70º C / -4ºF ~ 158ºF Humidity: 20% ~ 70%

Table 25 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.100.1 (router) 192.168.100.2. (AP)
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.100.33 to 192.168.100.64
Wireless Interface	Wireless LAN
Default Wireless SSID	ZyXEL
Default Wireless DHCP Pool Size	Wireless LAN: Same as LAN (32 from 192.168.100.33 to 192.168.100.64)
Device Management	Use the Web-Based Configuration Interface to easily configure the rich range of features on the MWR102.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the MWR102 wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The MWR102 may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web-Based Configuration Interface to put it on the MWR102. Note: Only install firmware for your specific model!
Save/Reload Settings	Make a copy of the MWR102's configuration and put it back on the MWR102 later if you decide you want to revert back to an earlier configuration.

DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the MWR102 assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
Logging	Use logs for troubleshooting. You can view logs in the Web-Based Configuration Utility.
PPPoE	PPPoE mimics a dial-up Internet access connection.

Appendices

Appendix A

Pop-up Windows, JavaScripts and Java Permissions

In order to use the Web-Based Management Interface 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

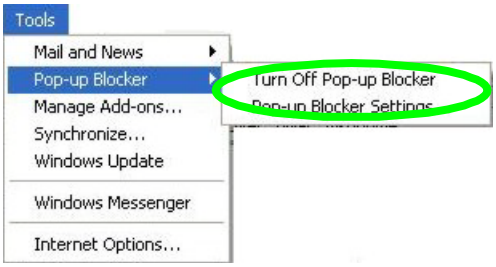
You may have to disable pop-up blocking to log into your device.

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**.

Figure 34 Pop-up Blocker

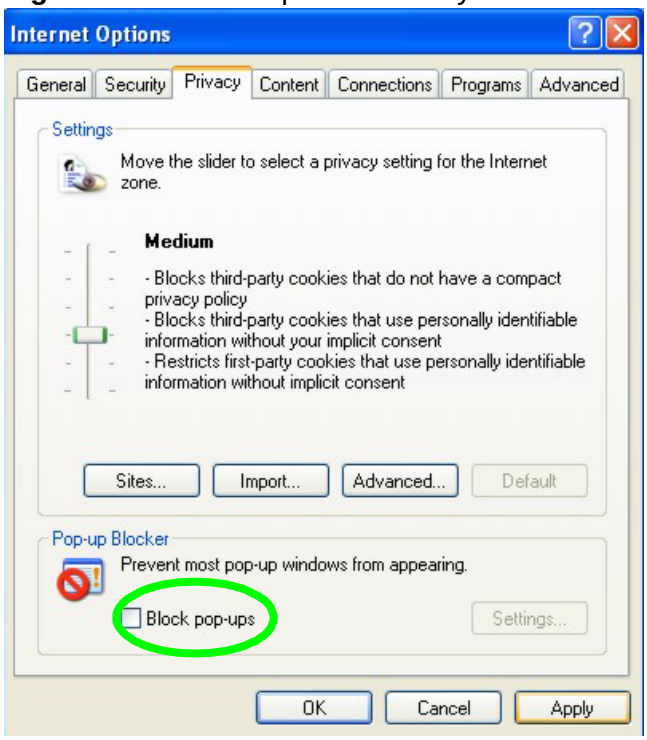


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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

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

Figure 35 Internet Options: Privacy



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

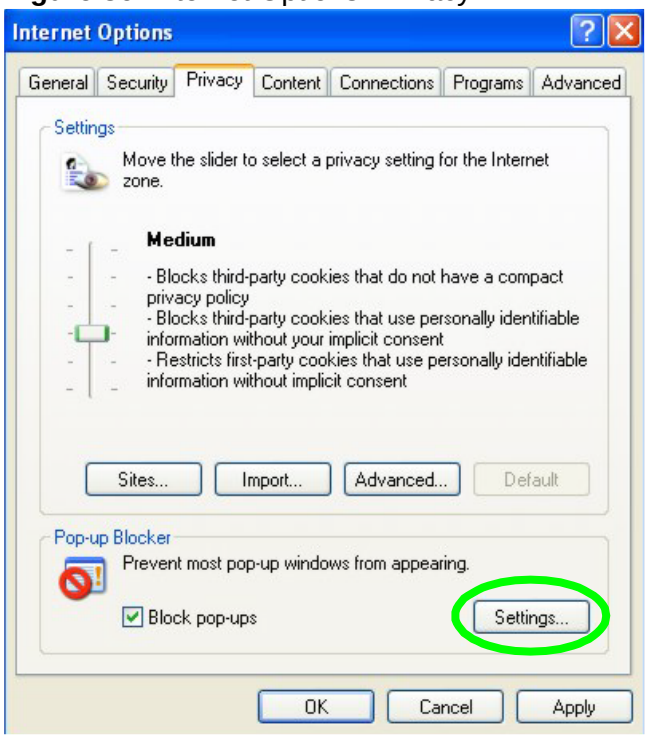
Enable pop-up Blockers with Exceptions

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.

Figure 36 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**.

Figure 37 Pop-up Blocker Settings

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

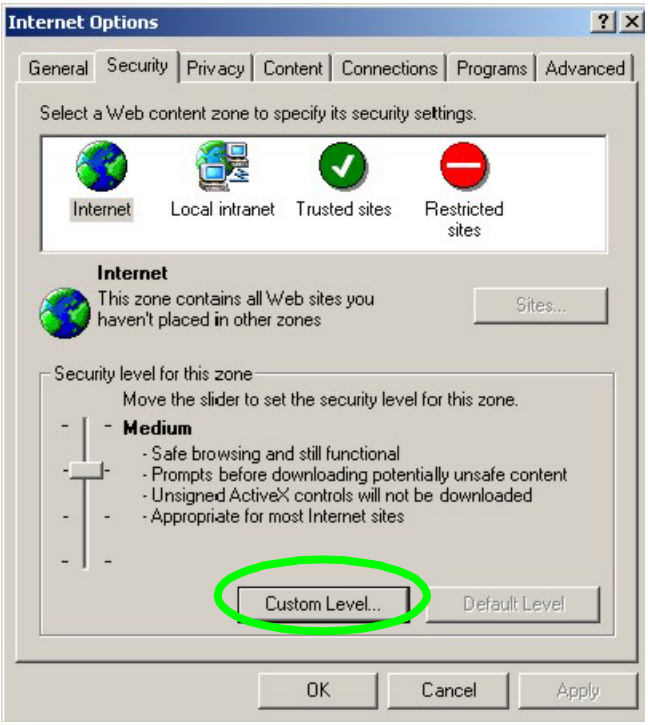
6 Click **Apply** to save this setting.

JavaScripts

If pages of the Web-Based Management Interface do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

Figure 38 Internet Options: Security



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

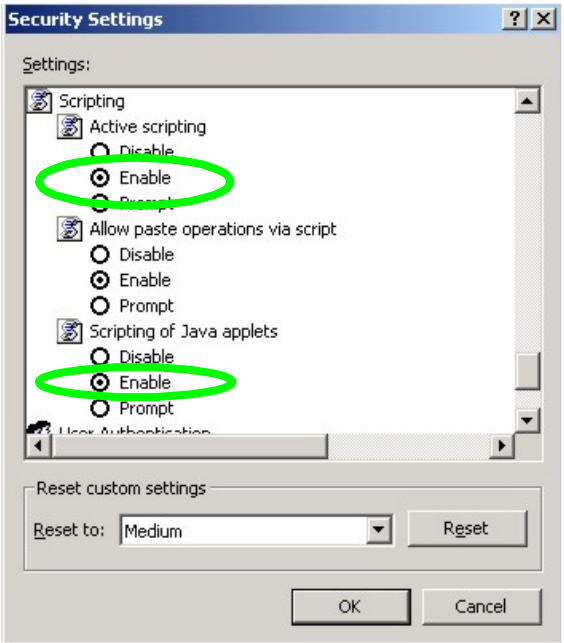
3 Scroll down to **Scripting**.

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.

Figure 39 Security Settings - Java Scripting



Java Permissions

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

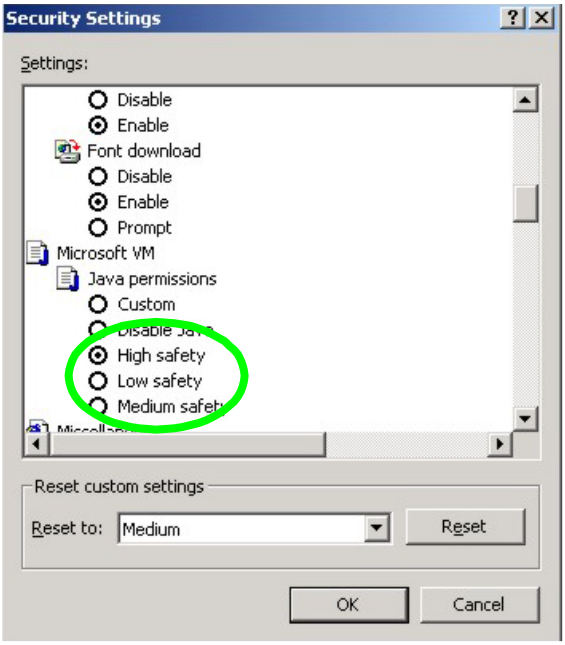
2 Click the **Custom Level...** button.

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.

Figure 40 Security Settings – Java



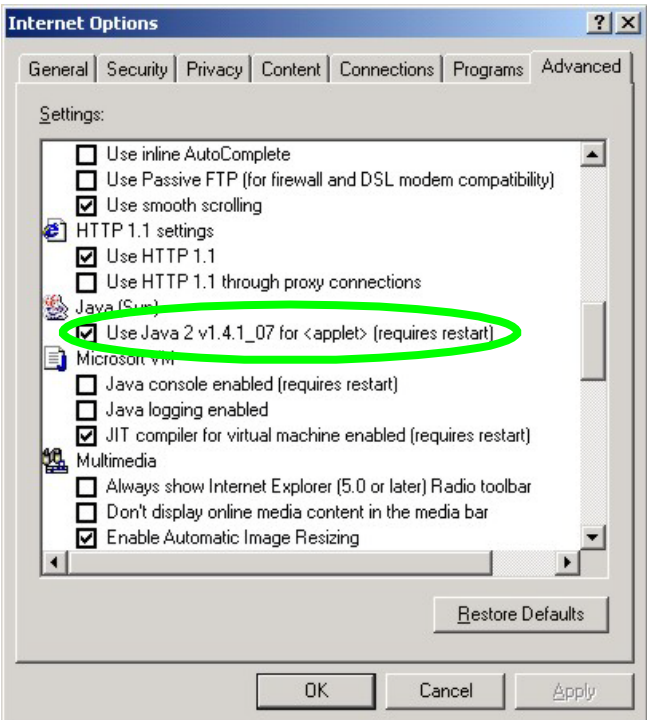
JAVA (Sun)

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.

Figure 41 Java (Sun)



Appendix B

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.

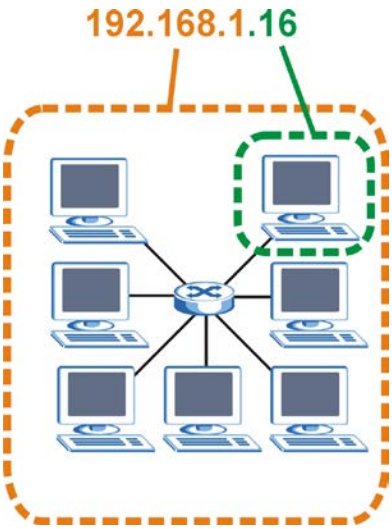
Structure

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.

Figure 42 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).

Table 26 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
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

Table 27 Subnet Masks

	BINARY				**DECIMAL**
	1ST OCTET	**2ND OCTET**	**3RD OCTET**	**4TH OCTET**	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
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:

Table 28 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.

Table 29 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

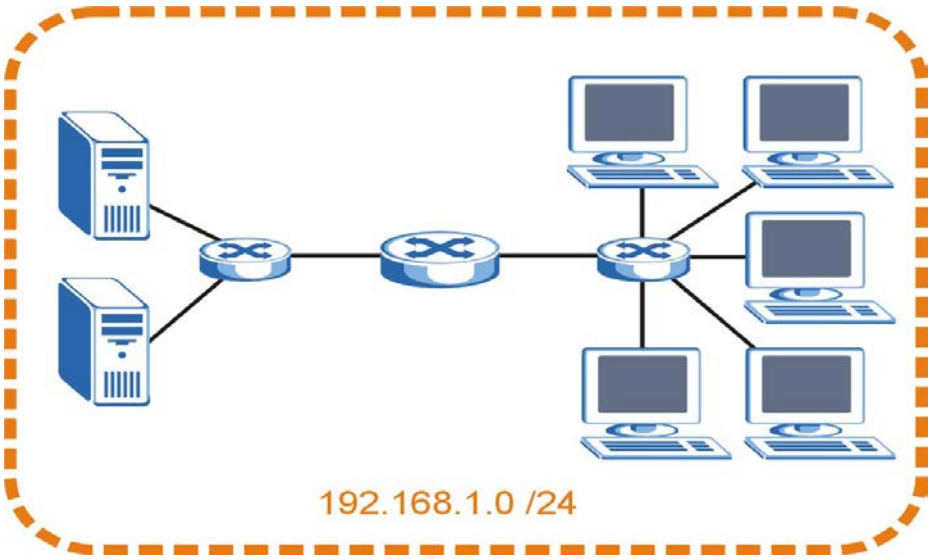
Subnetting

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.

Figure 43 Subnetting Example: Before Subnetting

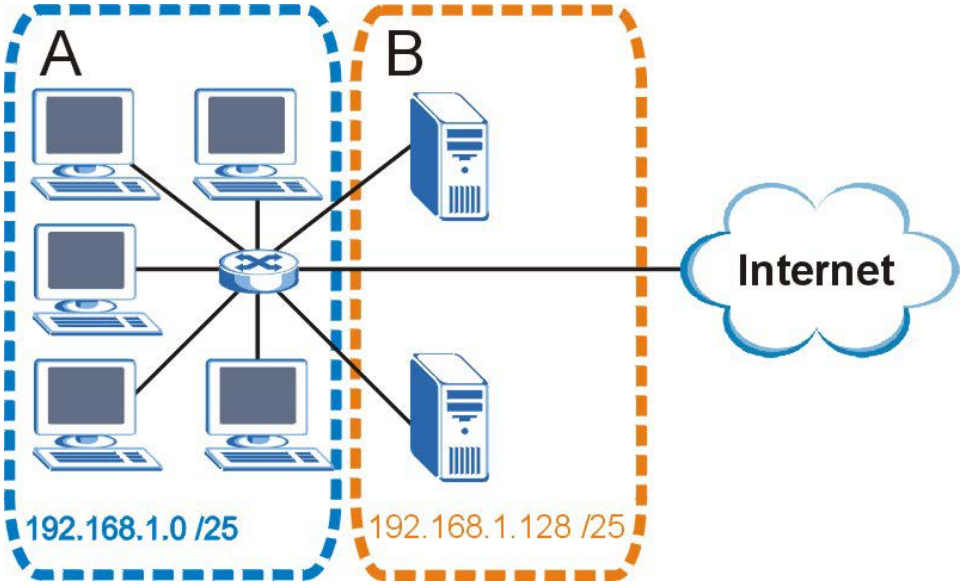


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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**.

Figure 44 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.**11**000000) 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).

Table 30 Subnet 1

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

Table 32 Subnet 2

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

Table 33 Subnet 3

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

Table 34 Subnet 4

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

Example: Eight Subnets

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

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

Table 35 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.

Table 36 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	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

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

Table 37 16-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022

7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

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 MWR102.

Once you have decided on the network number, pick an IP address for your MWR102 that is easy to remember (for instance, 192.168.100.1) 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 MWR102 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 MWR102 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.*

Appendix 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.

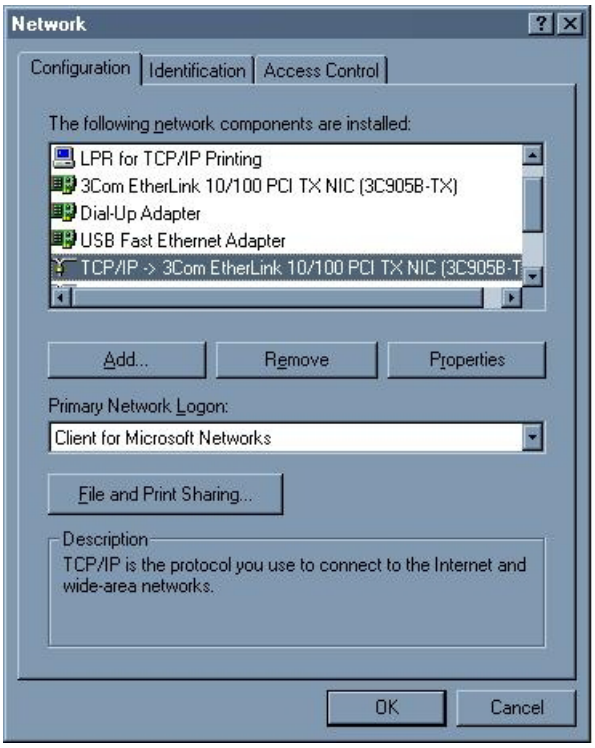
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 Prestige's LAN port.

Windows 95/98/Me

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

Figure 45 Windows 95/98/Me: Network: Configuration



Installing Components

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

If you need the adapter:

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

If you need TCP/IP:

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

If you need Client for Microsoft Networks:

1 Click **Add**.

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

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

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

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

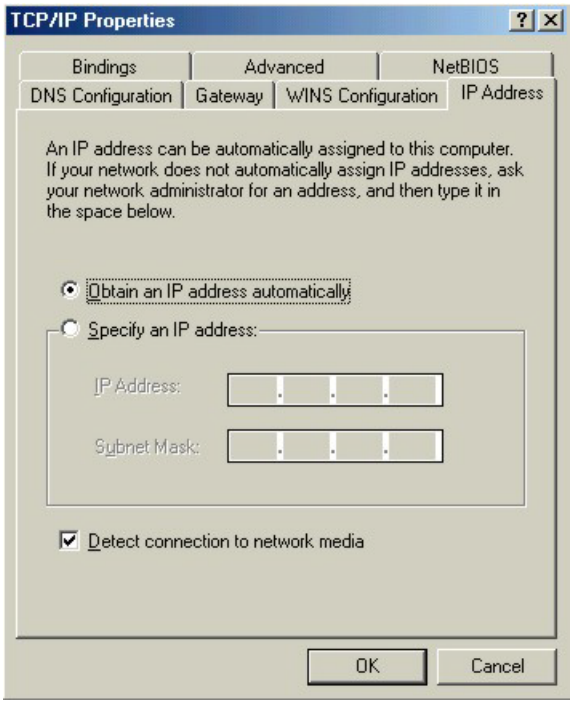
Configuring

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

2 Click the **IP Address** tab.

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

Figure 46 Windows 95/98/Me: TCP/IP Properties: IP Address

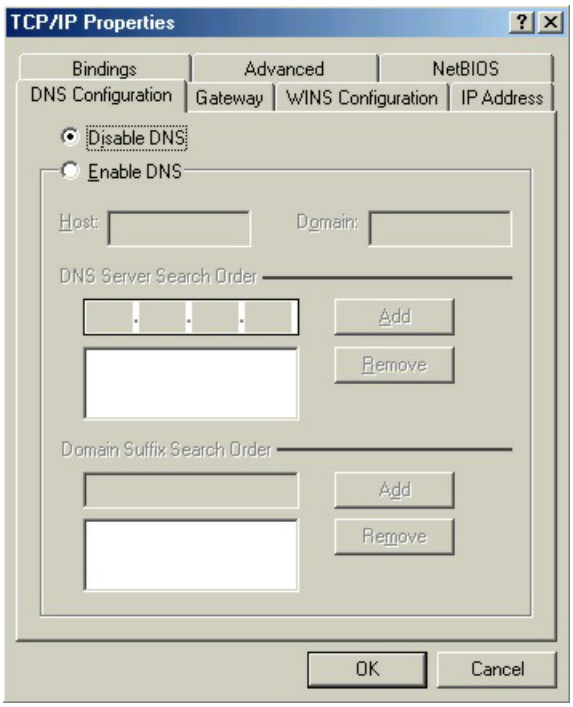


3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.

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

Figure 47 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 router and restart your computer when prompted.

Verifying Settings

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

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

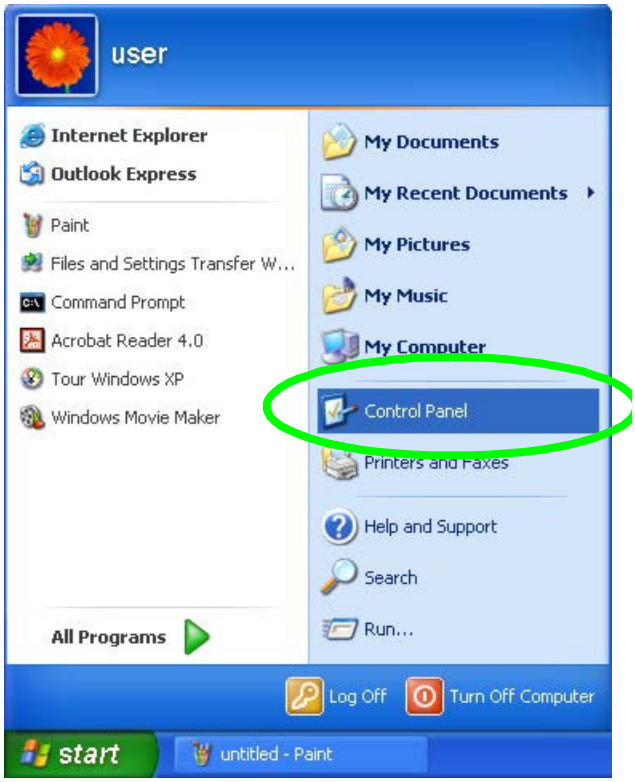
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

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

Figure 48 Windows XP: Start Menu

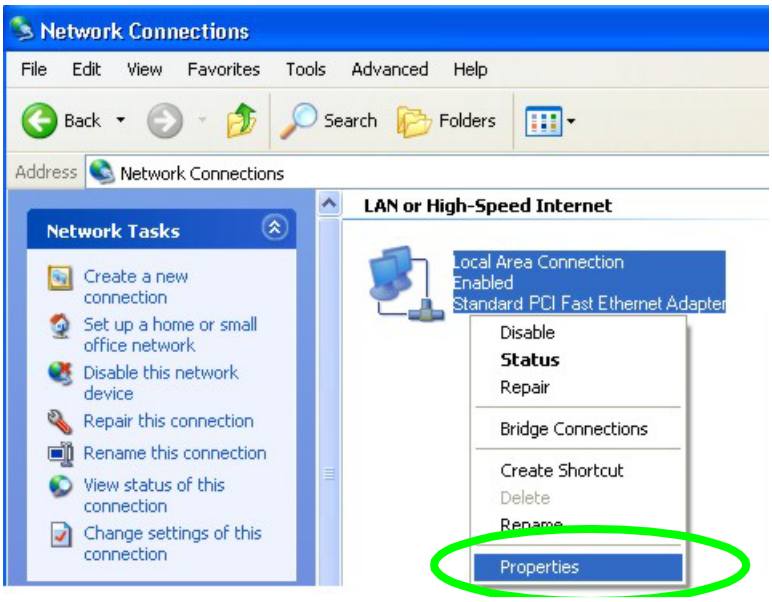


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 49 Windows XP: Control Panel

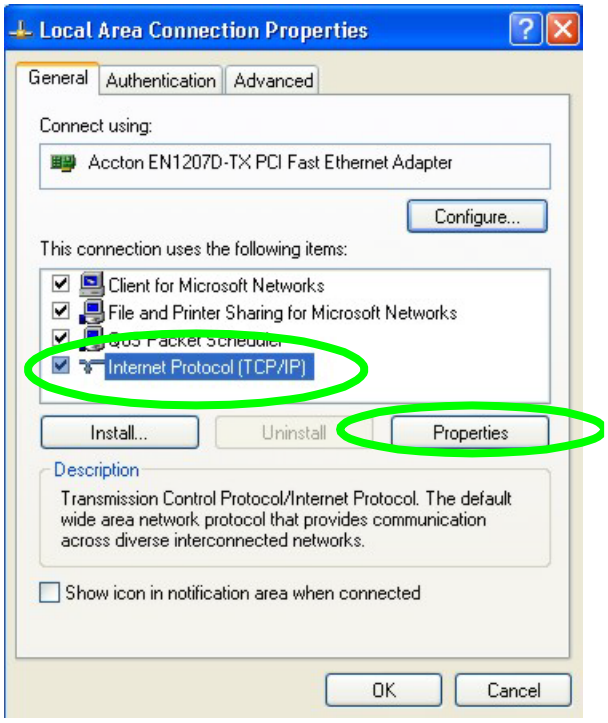
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 50 Windows XP: Control Panel: Network Connections: Properties



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

Figure 51 Windows XP: Local Area Connection Properties

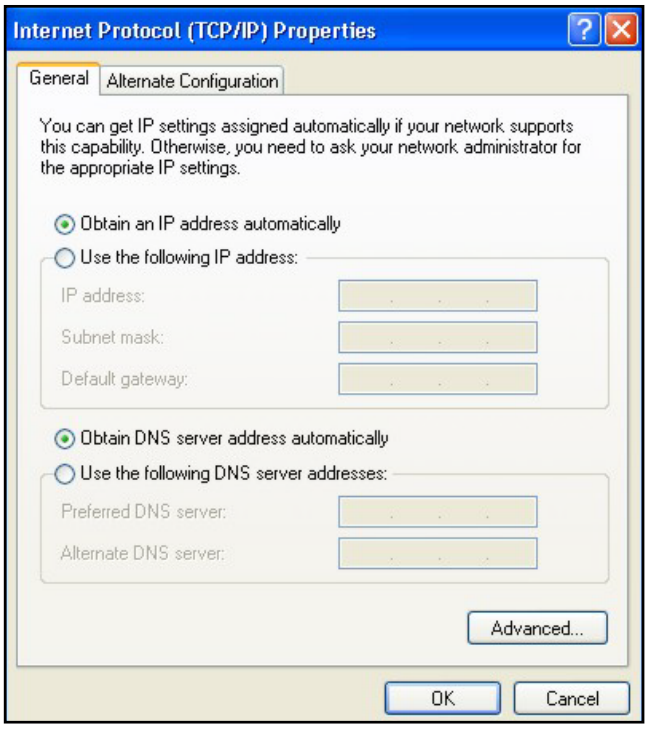


5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

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

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

Figure 52 Windows XP: Internet Protocol (TCP/IP) Properties

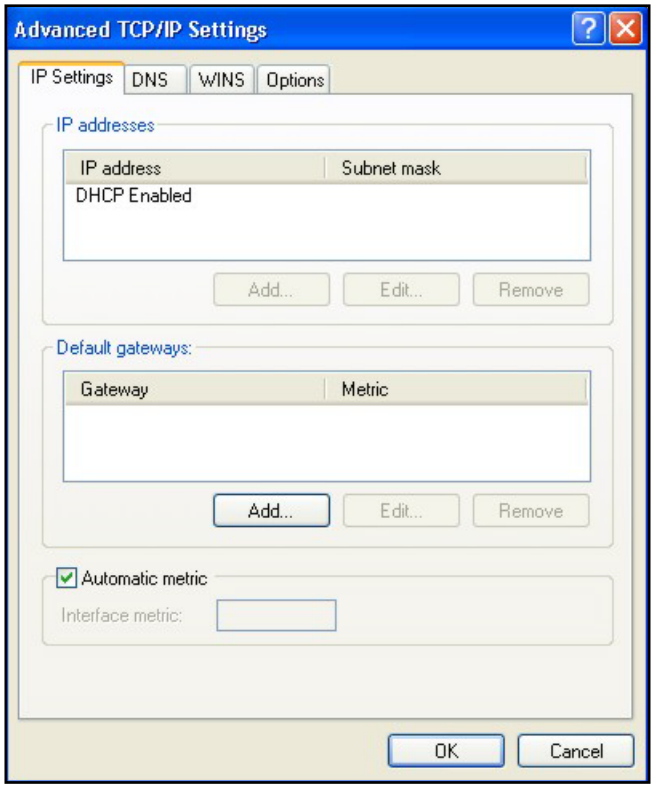


6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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

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

Figure 53 Windows XP: Advanced TCP/IP Properties

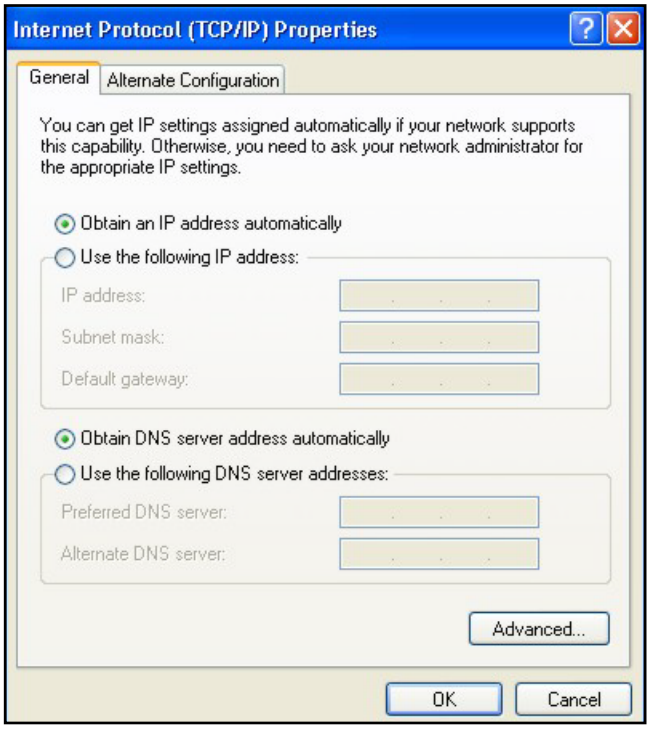


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

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

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

Figure 54 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 router and restart your computer (if prompted).

Verifying Settings

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

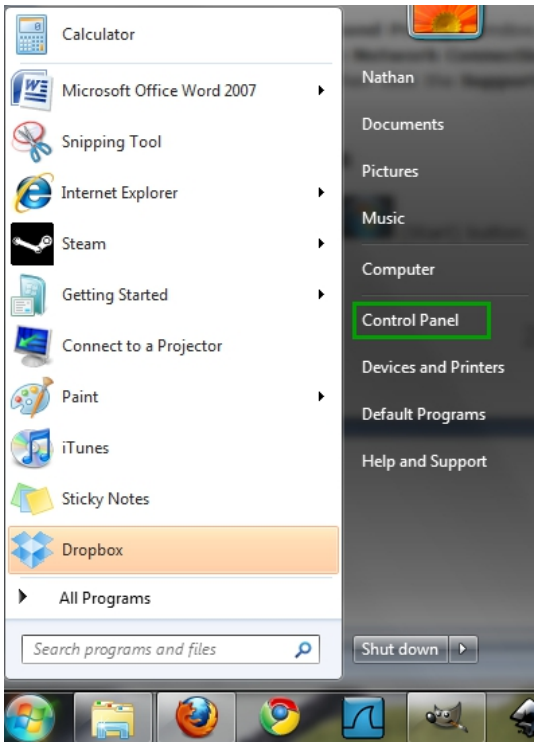
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows 7/Vista

1 Click on the  (**Start**) button.

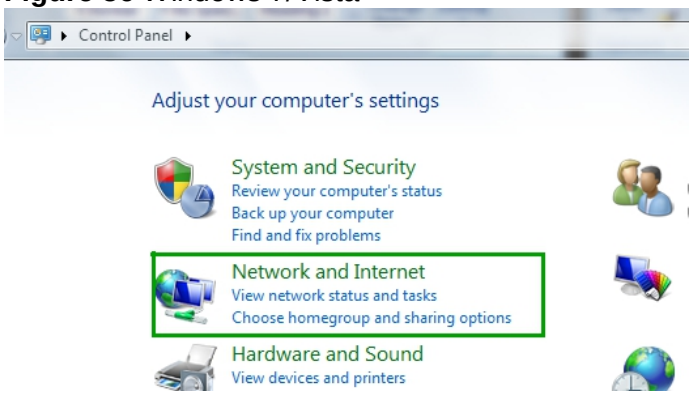
2 Click on **Control Panel.**

Figure 55 Windows 7/Vista



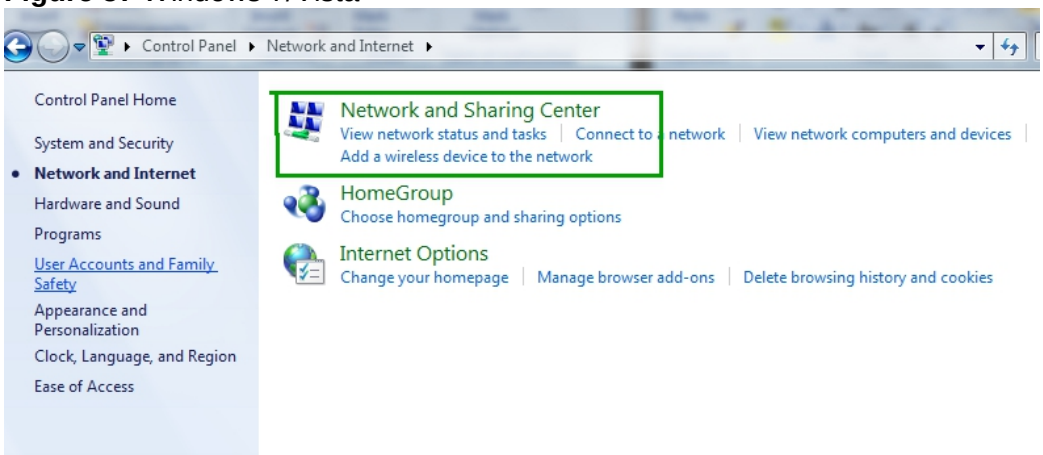
3 Click on **Network and Internet**.

Figure 56 Windows 7/Vista



4 Click on **Network and Sharing Center**

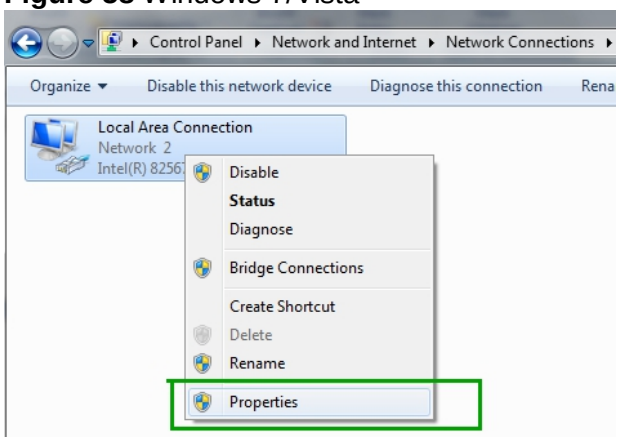
Figure 57 Windows 7/Vista



5 On the left side of the screen click on **Change Adapter Settings** (Windows 7), or **Manage Network Connections** (Vista).

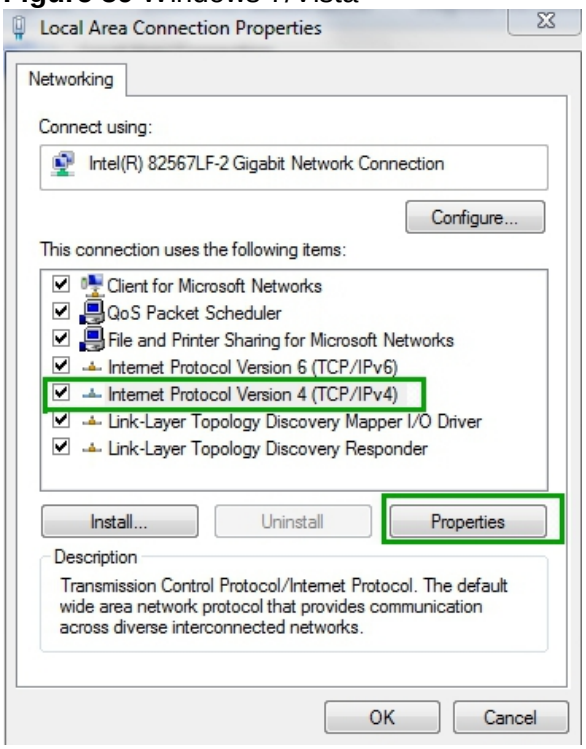
6 Right click on **Local Area Connection** and select **Properties**.

Figure 58 Windows 7/Vista



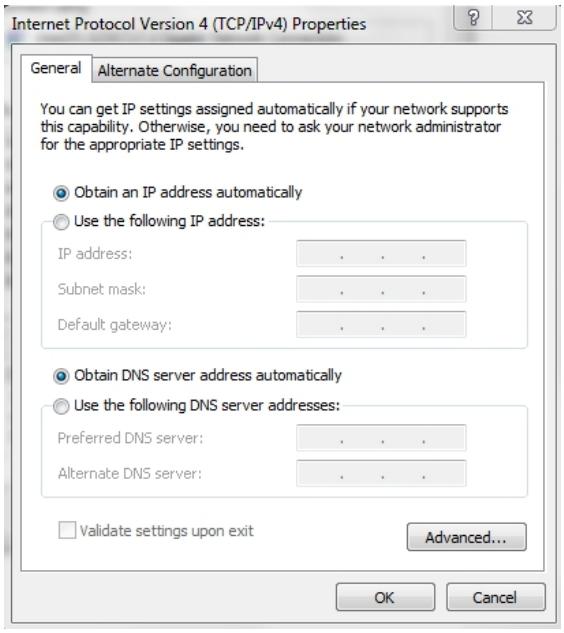
7 Highlight **Internet Protocol Version 4** and click **Properties**.

Figure 59 Windows 7/Vista



8 Select **Use the Following IP Address** and enter your IP address, Subnet Mask, and Default Gateway. Enter your DNS server address (if trying to connect to the internet) and click **OK**.

Figure 60 Windows 7/Vista

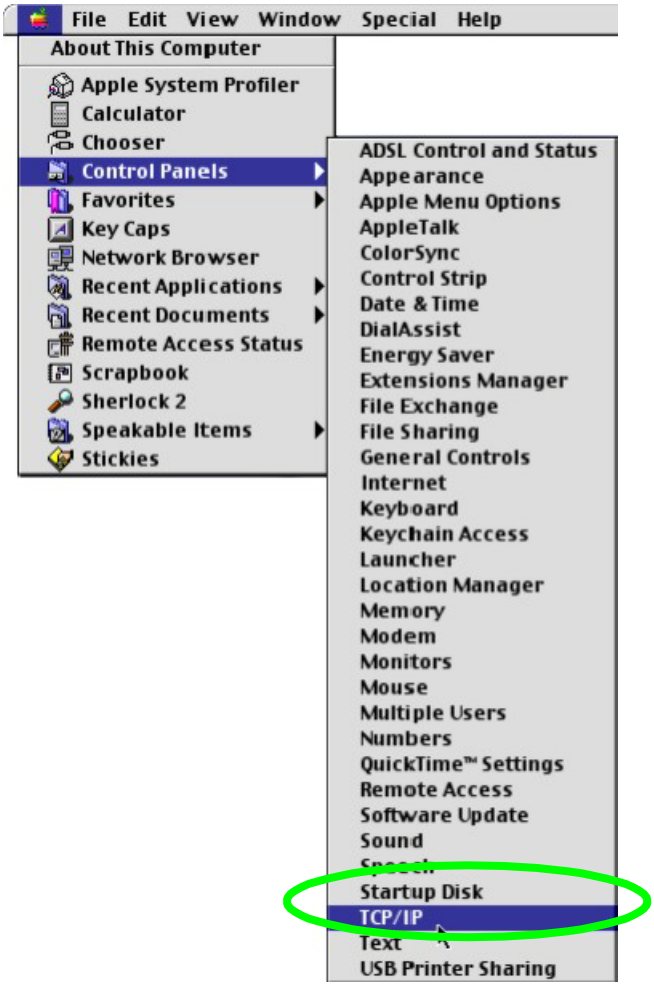


9 Click **OK** or **Close** on the Local Area Connection Properties window to apply the settings.

Macintosh OS 8/9

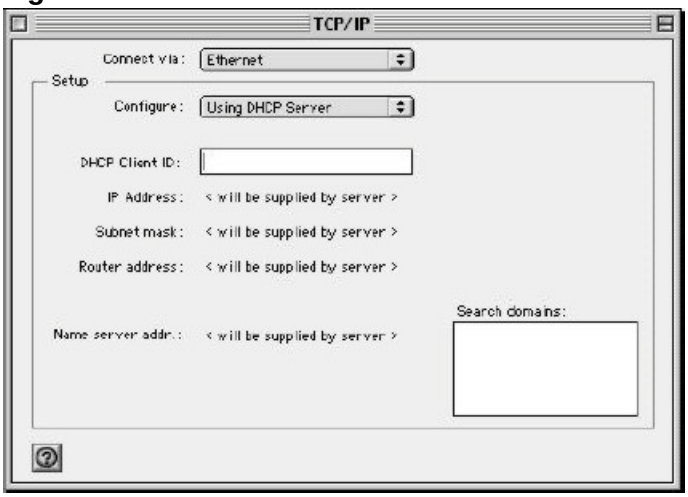
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 61 Macintosh OS 8/9: Apple Menu



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

Figure 62 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 router and restart your computer (if prompted).

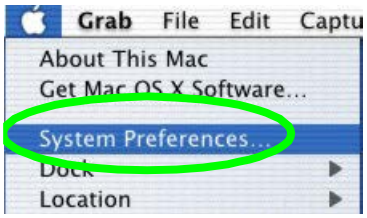
Verifying Settings

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

Macintosh OS X

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

Figure 63 Macintosh OS X: Apple Menu

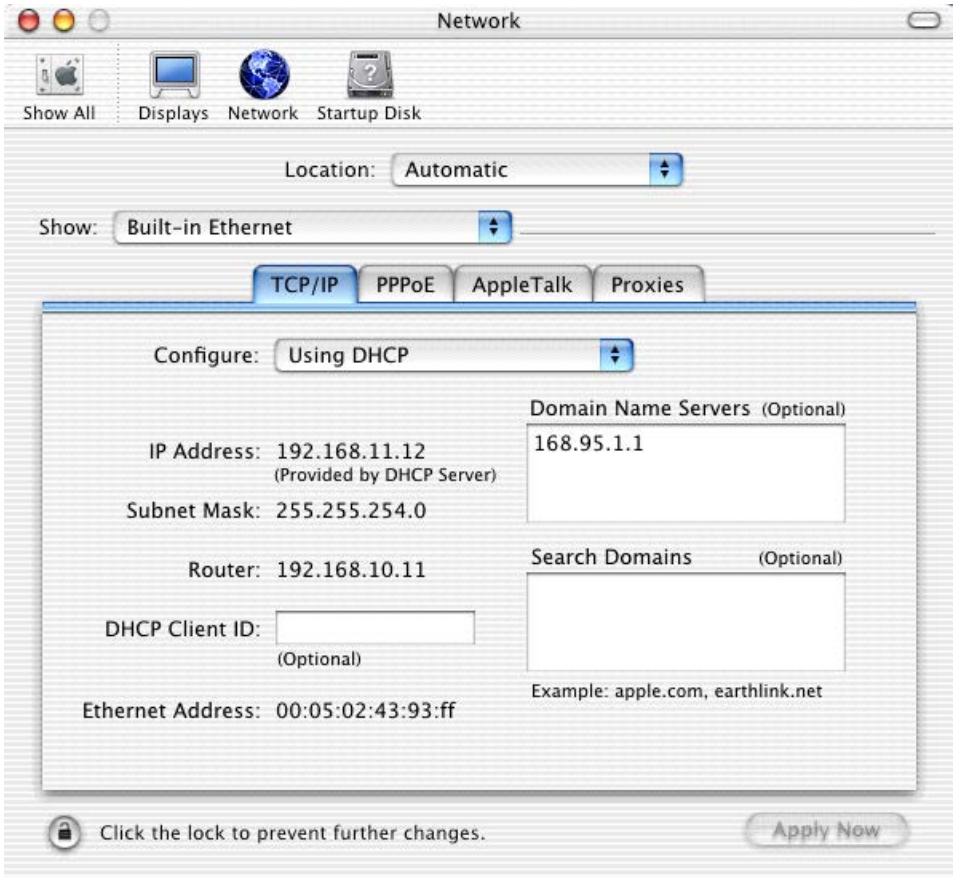


2 Click **Network** in the icon bar.

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

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

Figure 64 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 router 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.

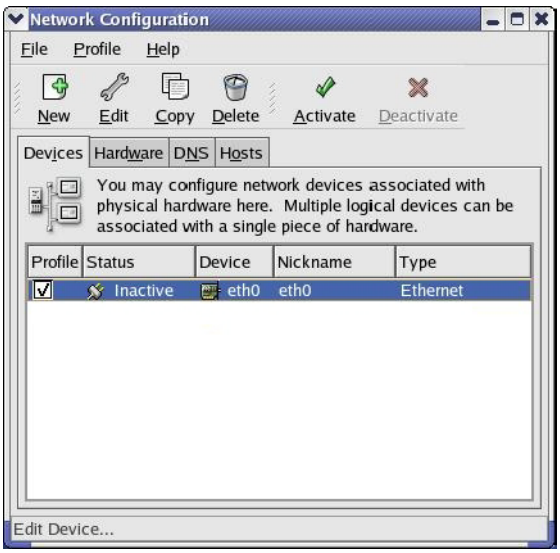
Note: Make sure you are logged in as the root administrator.

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**.

Figure 65 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.

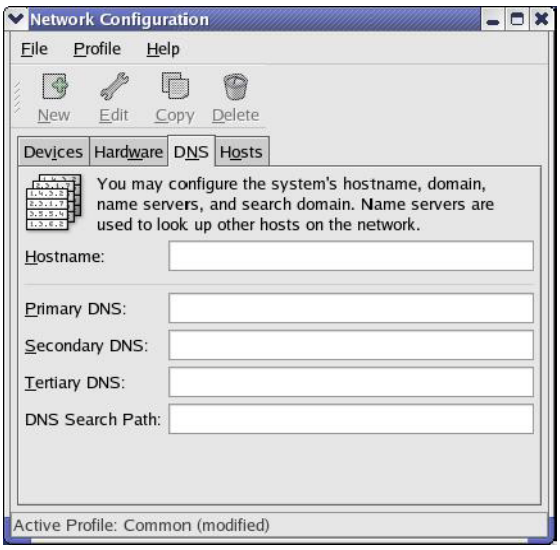
Figure 66 Red Hat 9.0: KDE: Ethernet Device: General

- 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.

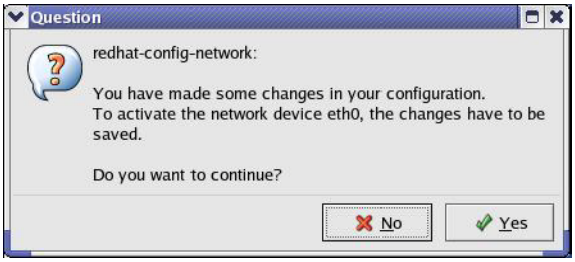
Figure 67 Red Hat 9.0: KDE: Network Configuration: DNS



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.**

Figure 68 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.

Figure 69 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 192.168.100.10 and the subnet mask is 255.255.255.0.

Figure 70 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.100.10
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.

Figure 71 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.

Figure 72 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]
```

34.1.2 Verifying Settings

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

Figure 73 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]#
```

Appendix D

Wireless LANs

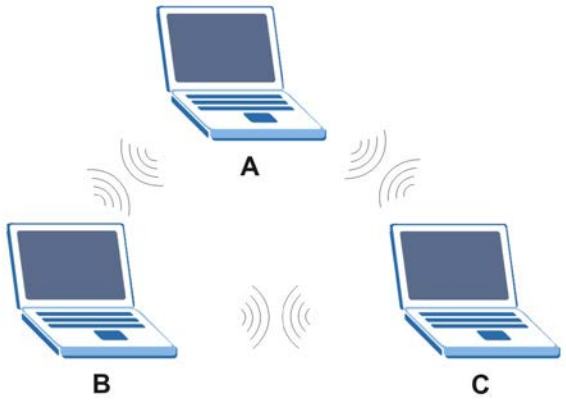
Wireless LAN Topologies

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.

Figure 74 Peer-to-Peer Communication in an Ad-hoc Network

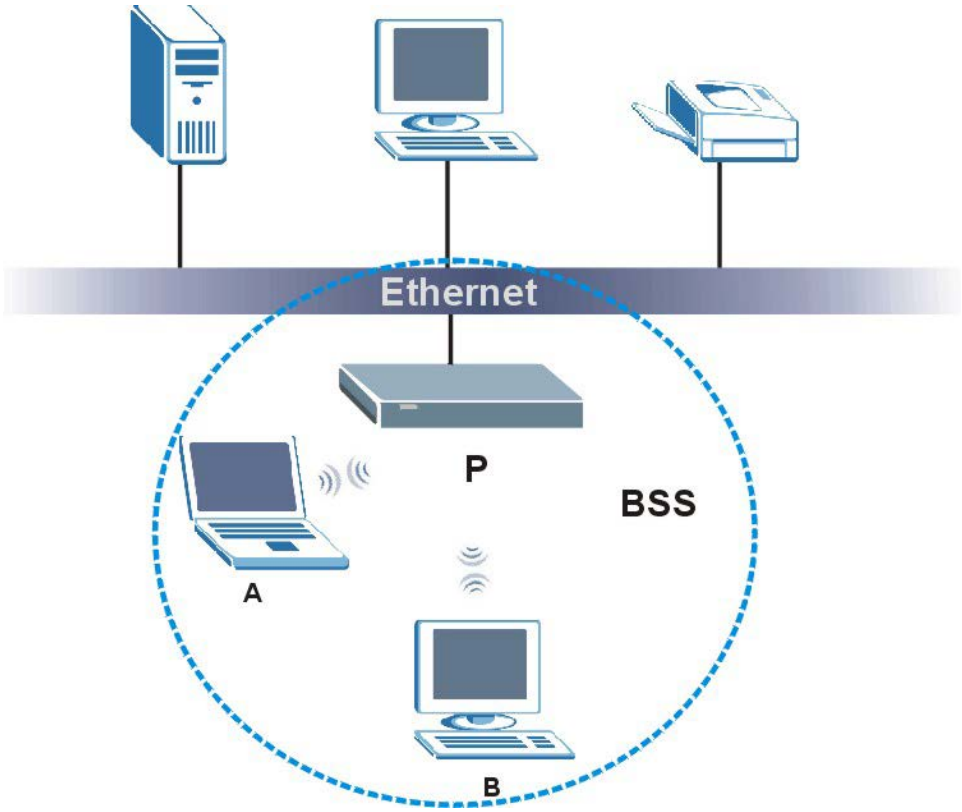


BSS

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.

Figure 75 Basic Service Set



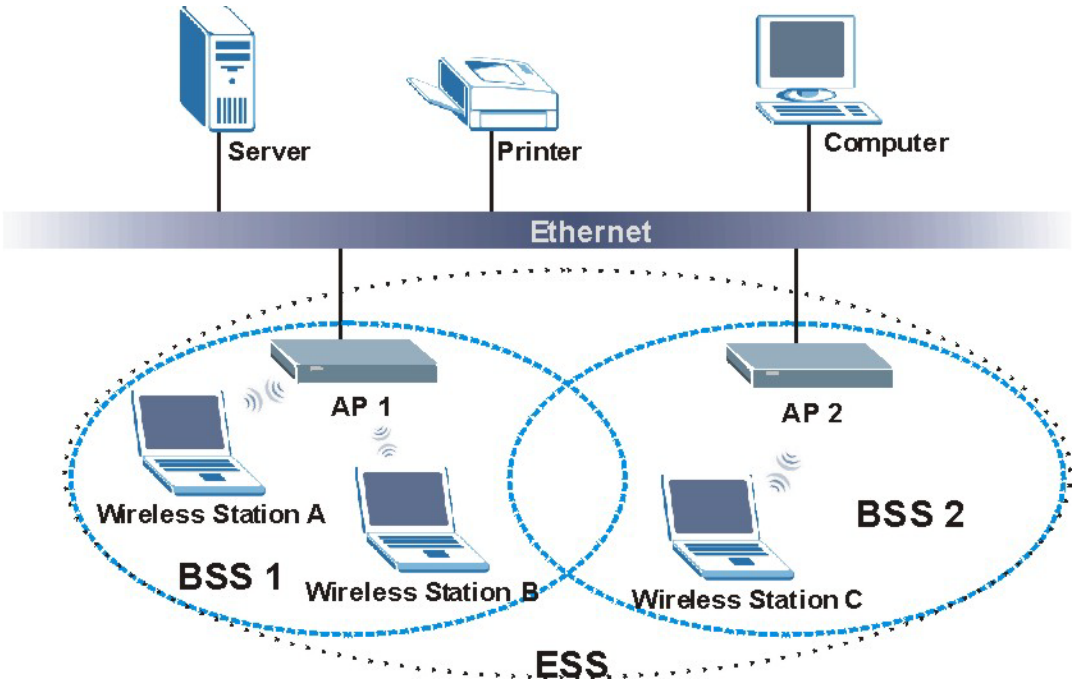
ESS

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.

Figure 76 Infrastructure WLAN



Channel

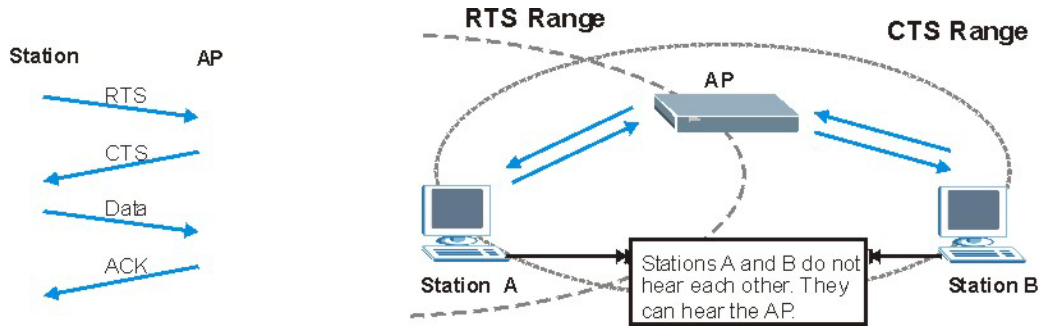
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs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

Figure 77 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:

Table 38 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.

Table 39 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 WPA-PSK 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.

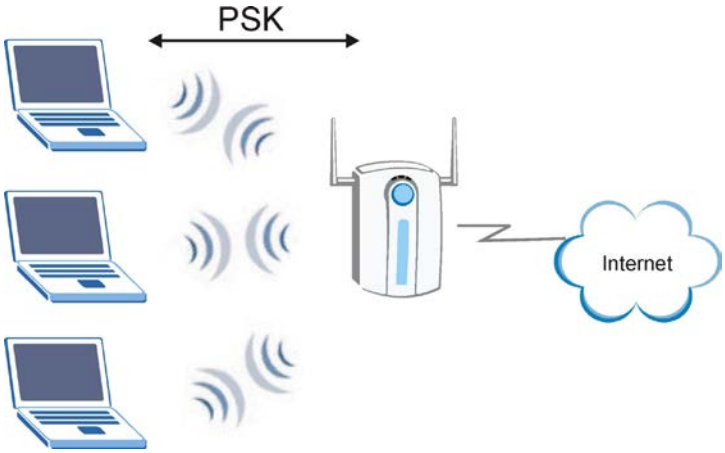
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

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.

Figure 78 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 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.

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.

Table 40 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-Enterprise	TKIP	No	Enable
WPA-Personal	TKIP	Yes	Enable
WPA2-Enterprise	AES	No	Enable
WPA2-Personal	AES	Yes	Enable

Appendix E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **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**. Please refer to RFC 1700 for further information about port numbers.
  - 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.

Table 41 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
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	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example http://us.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.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
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 or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.

IGMP (MULTICAST)	User-Defined	2	Internet Group Management 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.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
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.
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).
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.

RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
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	Simple File Transfer Protocol.
SMTP	TCP	25	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.
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.
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 used for (Terminal Access Controller Access Control System).
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	7000	Another videoconferencing solution.

Appendix F

Legal Information

Copyright

Disclaimer

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

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.

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

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

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1. this device may not cause interference and
2. this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Viewing Certifications

1. Go to http://us.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.

GPL-OSS Software Notice

In our continuing effort to disclose important and useful information with regards to our products, we would like to inform you that certain products you received from ZyXEL Communications Inc. may contain in part some free software (In accordance with this free software, it is licensed in a way that ensures your freedom to run, copy, distribute, study, change and improve the software.).

Also, certain ZyXEL products include software code developed by third parties, including software code subject to the GNU General Public License ("GPL")

Please refer to the following URLs to get more information:

http://us.zyxel.com/opensource

or

http://us.zyxel.com/Support/GPL-OSS/

Appendix G

Open Source Licenses

Article I. End-User License Agreement for “MWR102”

Article II.

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. HOWEVER, CERTAIN ZYXEL’S PRODUCTS MAY CONTAIN–IN PART-SOME THIRD PARTY’S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY’S LICENSES (“OPEN-SOURCED COMPONENTS”). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

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, trade secret law, international treaty provisions, and the applicable national laws of each respective country. 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. 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, you may not market, co-brand, and 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 third party software, and your use of such material is exclusively 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 other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. 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, AND NON-INFRINGEMENT. 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 UNINTERUPTED 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 SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL 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 if the parties agree to a binding arbitration. 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.

Article III.

Article IV. **NOTE:** Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (freesoftware@zyxel.com), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Article V. Notice

Article VI. 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.

Open-Sourced Components

Name	Version	Source	License
GNU/Linux kernel	v2.6.30.9	http://www.kernel.org	GPLv2
bootcode	v1.1e.1	NA	GPLv2
toolchain	v1.3.6 or v1.5.5	http://gcc.gnu.org/	GPLv2
auth	v1.8e	NA	GPLv2
boa	v0.94.14rc21	http://www.boa.org/	GPLv2
bridge-utils	v0.9.5	http://bridge.sourceforge.net/	GPLv2
busybox-1.13	v1.13	http://www.busybox.net/	GPLv2
discover			
dlna_dms	v1.1a	http://ushare.geexbox.org/	GPLv2
dnrd-2.12.1	v2.12.1	http://sourceforge.net/projects/dnrd/	GPLv2
dnsmasq-2.33	v2.33	http://thekelleys.org.uk/dnsmasq/doc.html	GPLv2
dosfstools-2.11	v2.11	http://freshmeat.net/projects/dosfstools	GPLv2
gdb	v6.8	http://www.gnu.org/software/gdb/	GPLv2/3
goahead-2.1.1	v2.1.1	http://www.goahead.com/products/webserver/default.aspx	royalty free licensing terms http://www.goahead.com/products/webserver/licensing.aspx
hostapd-0.6.10	v0.6.10	http://hostapd.sourcearchive.com/	GPLv2/BSD Dual license
hostapd-0.6.9	v0.6.9	http://hostapd.sourcearchive.com/	GPLv2/BSD Dual license
IAPP	v1.7	http://hostap.epitest.fi/wpa_supplicant/devel/dir_5a5c05d102ff4f2b85d1c95aa4590d78.html	GPLv2

igmpproxy	v1.2	http://sourceforge.net/projects/igmpproxy/	GPLv2
iproute2-2.6.29-1	v2.6.19	http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2	GPLv2
iptables-1.4.4	v1.4.4	http://www.netfilter.org/about.html#license http://www.netfilter.org/projects/iptables/downloads.html#iptables-1.4.4	GPLv2
l2tpd	v0.69	http://sourceforge.net/projects/l2tpd/	GPLv2
libnl-1.1	v1.1	http://www.infradead.org/~tgr/libnl/	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1
libusb-0.1.12	v0.1.12	http://www.libusb.org/	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1
lzma465	v4.65	http://sourceforge.net/projects/sevenzip/	Public Domain
mbpk_eject	v0.14	NA	GPLv2
mt-daapd-0.2.4.2	v0.2.4.2	http://sourceforge.net/projects/mt-daapd/	GPLv2
nbserver	v1.5.30	http://us1.samba.org/samba/docs/10years.html http://ftp.samba.org/pub/samba/old-versions/nbserver-1.5.30.tar.gz	GPLv2
ntfs-3g-2010.10.2	v2010.10.2	http://www.tuxera.com/community/ntfs-3g-download/	GPLv2
ntpclient	v2.0	http://doolittle.icarus.com/ntpclient/	GPLv2
ppp-2.4.4	2.4.4	ftp://ftp.samba.org/pub/ppp/	GPLv2
pptp-1.7.2	1.7.2	http://sourceforge.net/projects/pptpclient/	GPLv2
radvd-0.9.1	v0.9.1	http://www.litech.org/radvd/	radvd
samba-3.0.24	v3.0.24	http://samba.org/samba	GPL v2
samba-3.0.37	v3.0.37	http://samba.org/samba	GPL v2
squashfs4.0	v4.0	http://sourceforge.net/projects/squashfs/	GPL v2
udhcp-0.9.9-pre	v0.9.9	udhcp is now a drop-in component for busybox (http://busybox.net)	GPL v2
updatedd-2.5	v2.5	http://updatedd.philipp-benner.de	GPL
usb-modeswitch-1.1.3	v1.1.3	http://www.draisberghof.de/usb_modeswitch	GPL v2
usb-modeswitch-data-20100623	v1.1.3	http://www.draisberghof.de/usb_modeswitch	GPL v2
usbutils-0.86	v0.86	http://sourceforge.net/projects/linux-usb/files/	GPL v2
vsftpd-2.3.2	v2.3.2	http://vsftpd.beasts.org/	GPL v2
wide-dhcpv6	wide-dhcpv6-20070507	http://sourceforge.net/projects/wide-dhcpv6/	Copyright (C) 1998-2004 WIDE Project.
wireless_tools.25	v25	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html	GPL v2
wireless_tools.29	v29	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html	GPL v2
zlib-1.2.3	v1.2.3	http://www.zlib.org	Zlib

Notice

This Product includes GNU/Linux kernel, bootcode, toolchain, auth, boa, bridge-utils, busybox-1.13, discover, dlna_dms, dnrd-2.12.1, dnsmasq-2.33, dosfstools-2.11, gdbunder, hostapd-0.6.10, hostapd-0.6.9, IAPP, igmpproxy, iproute2-2.6.29-1, iptables-1.4.4, l2tpd, mbpk_eject, mt-daapd-0.2.4.2, nbserver, ntfs-3g-2010.10.2, ntpclient, ppp-2.4.4, pptp-1.7.2, samba-3.0.24, samba-3.0.37, squashfs4.0, udhcp-0.9.9-pre, updatedd-2.5, usb-modeswitch-1.1.3, usb-modeswitch-data-20100623, usbutils-0.86, vsftpd-2.3.2, wireless_tools.25, and wireless_tools.29 under the GPL License.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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.

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

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

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. 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 them 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 prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. 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.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those

activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the

work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey 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; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received

by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on

material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License

(including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or

counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If 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 convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU 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 that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version

published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

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.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS 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.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

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 3 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, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an “about box”.

You should also get your employer (if you work as a programmer) or school, if any, to sign a “copyright disclaimer” for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the

library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

This Product includes libnl-1.1, libusb-0.1.12 under the GNU Lesser Public License

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

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. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, 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 and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, 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 library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete 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 distribute a copy of this License along with the Library. 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 Library or any portion of it, thus forming a work based on the Library, 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) The

modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, 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 Library, 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 Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you 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. If distribution of 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 satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the

Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special

exception, the materials to be 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.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library 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.

9. 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 Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library 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 with this License.

11. 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 Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library 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 Library. 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.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library 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.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser 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 Library 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 Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, 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

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "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 LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. 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 LIBRARY 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 LIBRARY (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 LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes hostapd-0.6.10, hostapd-0.6.9 under the BSD License.

BSD

Copyright (c) [dates as appropriate to package]

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:

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

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.

Neither the name of the University nor of the Laboratory 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 Zlib 1.2.3 under the Zlib License.

Zlib License

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.2, October 3rd, 2004

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

ZLIB is third party library and has its own license.

files under src/acdk/vfile/zlib are published under following Copyright and license:

zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.3, July 9th, 1998

Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a

product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds.internic.net/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

This Product includes radvd-0.9.1 under the radvd License.

radvd License

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.
1. All terms of all other applicable copyrights and licenses must be followed.
2. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.
3. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. All advertising materials mentioning features or use of this software must display the following acknowledgement with the name(s) of the authors as specified in the copyright notice(s) substituted where indicated:

   This product includes software developed by the authors which are mentioned at the start of the source files and other contributors.

5. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.