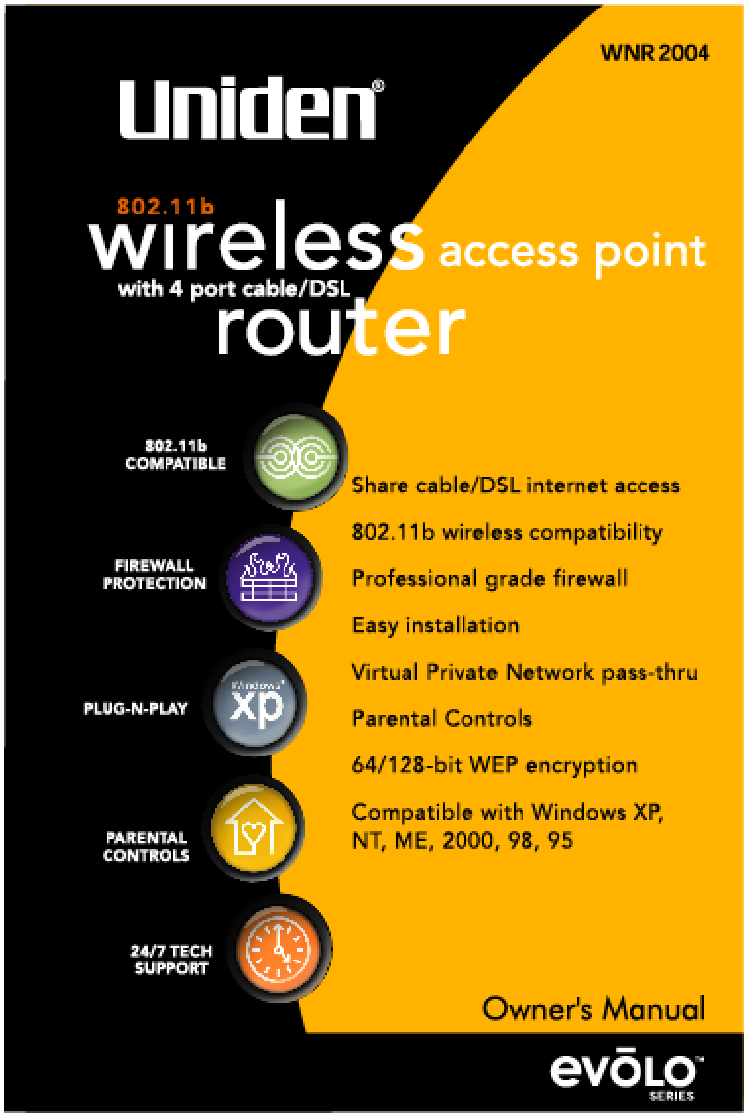


TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

## Welcome

Congratulations on your purchase of the Uniden evōlo™ **WNR2004 802.11b Wireless Access Point (AP) with 4 Port 10/100 Ethernet Cable/DSL Router**. This **Wireless AP/Router** is designed and engineered to exacting standards for reliability, long life and outstanding performance.

With the **WNR2004**, you can share secure high-speed Internet access to multiple computers through a single DSL or Cable modem.

The firewall built into the **WNR2004** is ready to provide secure Internet access to all computers, directly out of the box, (For Cable/DSL users who receive their WAN IP Address automatically from their Internet Service Provider (ISP)). Just follow the hardware installation process and you are ready to surf the web, protected from hackers.

For those wanting to activate other features provided in the **WNR2004**, setup is easy. Follow the instructions and your system will be up and running quickly.

This Owner’s Manual will guide you through the hardware installation and network configuration process.

## WNR2004 Features

The **Uniden WNR2004 802.11b AP/Router** provides many easy-to-use advanced features, described below.

INTERNET ACCESS FEATURES

- **DSL & Cable Modem Compatible:** Allows you to connect to either DSL or Cable modems with Ethernet supported.
- **Share High-Speed Internet Access:** Your ISP gives you a single WAN IP Address that can be shared among all computers connected to the LAN. This is known as a *Private Network*. The computers connected to the router (LAN) are hidden from the Internet. This process is called Network Address Translation or *NAT*.
- **PPPoE Support:** The WNR2004 supports Point-to-Point Protocol over Ethernet or *PPPoE*. If you use a cable modem or DSL to connect to the Internet, you may need this feature enabled.
- **Keep-Alive:** When you use a PPPoE account, your ISP may disconnect your PC if it remains inactive for a long period of time. The keep-alive feature sends a data packet over the connection at a designated time interval to make sure the Internet connection remains active.
- **Dial-on-Demand:** For PPPoE accounts, this feature activates the Internet connection during the boot-up stage, or only when using the applications which require Internet access, such as Internet Explorer.
- **Static or Dynamic IP Address:** Supports both Static and Dynamic IP Addresses provided by your ISP.

WIRELESS FEATURES

- **802.11b Compliant:** The Wireless Cable/DSL Router complies with the IEEE 802.11b specifications for Wireless LANS.
- **WEP/Wireless Security:** Supports both 64-bit and 128-bit Wired Equivalent Privacy (WEP) for secure wireless connections.
- **Access Control:** Allows to you to control who you allow or block access to your wireless network.
- **Easy Configuration:** The default settings can be quickly and easily changed.

LAN FEATURES

- **Four 10/100 Ethernet Ports:** 4-port dual-speed (10/100 Mbps) fast Ethernet switch allows you to create or extend your LAN.
- **Auto MDI/MDI-X:** Accepts both straight-through and crossover networking cables, avoiding the confusion of which type of cable is necessary.

ROUTER/SECURITY FEATURES

- **DHCP Server:** Dynamic Host Configuration Protocol (DHCP) automatically issues LAN IP Addresses to PCs and other Internet devices on your LAN.
- **NAT Protection:** Network Address Translation (NAT) allows all LAN computers to share a single WAN IP Address while hiding all LAN computers from external sources.
- **Stateful Packet Inspection:** All Stateful Internet Sessions (i.e. TCP) are monitored for malicious and

erroneous packets, protecting your network from hackers.

- **DoS Protection:** Denial of Service (DoS) attacks overload your router with invalid packets and connection requests, using so many resources that your router crashes and Internet access is no longer available. The WNR2004 protects against DoS attacks.

## CONFIGURATION & MANAGEMENT FEATURES

- **Web-Based Configuration**: No software installation is required to configure the Router
- **Remote Management**: Any computer on the LAN can connect and configure the WNR2004.
- **Password Protected Configuration Utility:** The configuration utility is password protected, preventing unauthorized users from modifying the feature settings.

## PARENTAL CONTROL FEATURES

- **Internet Access Control:** Allows you to enable or disable any computer on the LAN from accessing the Internet; you can also determine when and how long individual computers have access to the Internet.
- **Key Word Filtering:** Allows you to include or exclude a list of key words specified for a web address (URL) and/or that reside on the web site.

## ADVANCED ROUTER FEATURES

- **VPN Support:** The router passes through Virtual Private Networking (VPN) connections, so it can support VPNs that use IPSec, L2TP and PPTP without any user configuration.
- **Online Conferencing Support:** Supports Internet Telephony and Conferencing programs.
- **DMZ:** Allows the Internet unrestricted access to one computer within your LAN. This allows you to run programs that are incompatible with firewalls.
- **Port Mapping:** Allows Internet users to access Internet servers on your LAN. This allows you to support a web server or other host from within the firewall.
- **LAN Activity Log:** Keeps track of all activity and attacks on your network. This activity log can be sent to you via e-mail hourly, daily, weekly or however you want to review your LAN activity.
- **DNS Server:** Supports 2 Domain Name Service (DNS) Servers to relay DNS entries. This speeds up Internet connections.

## Package Contents

The following items are included with the WNR2004:

- One **WNR2004** unit with stand.
- One 7.5V DC power adapter.
- One Easy-Start Installation Guide.
- Owner's Manual on CD-ROM.
- One Cat-5 cable with RJ-45 connectors.

If any of these items are missing or damaged, immediately contact your place of purchase or Uniden Customer Service at: (800) 775-9060, Monday-Sunday, 24/7.

## Front View Details

**Table 1 LED Indicators**

| **Label/LED Indications** | **Activity** | **Description** |
|---|---|---|
| Wirless LAN Link/Activity | ON<br>OFF | Wireless client connected<br>No wireless clients are connected |
| Wired LAN Link/Activity<br>Ports 1 - 4 | Green<br>Amber<br>Blinking | The port is connected at 100 Mb/s.<br>The port is connected at 10 Mb/s.<br>Data is being transmitted/received. |
| WAN<br>Link/Activity | Green<br>Amber<br>Blinking | The port is connected at 100 Mb/s.<br>The port is connected at 10 Mb/s.<br>Data is being transmitted/received. |
| Test | Amber<br>OFF | The router is undergoing a power-on self-test (POST). If the light remains on, the router failed the POST.<br>The router passed the POST. |
| Power | ON<br>OFF | Power is on<br>Power is off |

## Rear View Details

- **Wireless Antenna:** For better performance, place the AP/Router at a high location. Placing the unit under a desk reduces performance.
- **Reset Button:** Pressing this button once performs a soft reboot, similar to turning the power on and off. However, if you press and hold the button for approximately 10 seconds, the device will reset to the factory default settings, erasing any configuration changes you have made (including the password).
- **Ports 1 through 4:** These auto-sensing 10/100 Ethernet RJ-45 jack ports automatically detect the speed of any attached Ethernet device and provide a the correct Ethernet connection. All of these ports are configured with auto MDI/MDI-X, so they support either straight or crossover cables, (Cat 5 UTP). Each port supports a maximum cable length of 100 meters over category 5 twisted pair cable.
- **WAN Port:** RJ-45 Interface connects to either the DSL or Cable modem.
- **7.5V Power Jack:** Connects to the Uniden supplied external power adapter to the power jack.

## Quick Installation Process

There are three steps to install your AP/Router and create a your own Local Area Network (LAN).

1. **Hardware Installation:** Through this process you will physically connect your computers to your router.
2. **PC Configuration:** For each computer, you will need to make sure they have the same LAN IP Address (The LAN IP Address is similar to an area code for making telephone calls. In order for all the computers to talk to each other, they must reside in the same area code).
3. **Basic Router Configuration:** Within this step you can set your Parental Controls, Passwords, and other features of your AP/Router.

### STEP 1: HARDWARE INSTALLATION

**NOTE: During the hardware installation process, please make sure all computers and the router are turned off until the installation process is complete.**

Before installing the **WNR2004** you will need the following:

- One external DSL or Cable modem with an Ethernet Port.
- Network Cables with RJ-45 connectors (UTP CAT 5).
- TCP/IP network protocols installed on all PCs. (See page 91 if you need assistance)

INSTALLING THE HARDWARE

1. **Connect to the DSL/Cable Modem:** Connect one end of the supplied CAT 5 network cable to the DSL/Cable Modem. Insert the other end into the **WNR2004** port labeled ***WAN***.
2. **Connect to the PC's:** Using standard CAT 5 network cables, connect any one of the four available LAN ports (labeled ***1*** through ***4***) to your PC's network card or Ethernet connection (RJ-45 jack). For wireless connections, you will need 802.11b clients (PCMCIA, PCI and/or USB) installed for your computers.
3. **Power on the Router:** Plug the power adapter into an AC power outlet and connect the power supply to the power jack on the rear of the **WNR2004**. The power LED should immediately turn on.

**NOTE: The WNR2004 has no "on" switch. It will power on as soon as the power adapter is connected.**

4. **Observe the Power-On Self Test:** When the WNR2004 powers on, it conducts a series of hardware diagnostics called Power-On-Self-Test (POST). While the POST is running, watch the front panel of the router. The Test LED should stay ON during the POST. If router passes the POST, the Test LED will turn off. If the Test LED stays on, then the router has failed the test.

The hardware installation is complete. Continue to Step 2: PC Configuration on page 16.

## STEP 2: PC CONFIGURATION

In order for your computer to communicate with the WNR2004, both devices must be on the same LAN, i.e. the first three parts of their IP addresses must be the same:

The default IP address of the WNR2004 Router is **192.168.1.1**. As a result, your PC's IP address must start with **192.168.1** as well. Fill in the last digit with some number other than **1** to distinguish your computer from the router.

To verify and/or change your PC's IP address so it is on the same network, please see the instructions specifically for your Microsoft operating system: Windows 95, 98, ME, NT, 2000 or XP.

**NOTES:**

- **If you are using the default WNR2004 settings and the default Windows "Obtain an IP address automatically" (DHCP) settings, no changes are required.**
- **By default, the AP/Router will act as a DHCP Server, automatically providing an IP Address and other related information to each PC on the LAN when that PC boots up.**
- **If you receive a Static (Fixed) IP address from your Cable/DSL provider, write it down along with your DNS Server information when prompted through the steps below. You will need to enter the Static IP address later during the IP Sharing Section of the Owner's Manual.**

FOR WINDOWS 95, 98, AND ME

1. Click on **Start**, **Settings**, **Control Panel**. Double click on **Network**.
2. In **“The following network components are installed”** box, select the TCP/IP associated with your network adapter. (If you have only one network adapter installed, you will only see one TCP/IP listed.) Highlight it and click the **Properties** button.
3. In the “**TCP/IP Properties**” window, select the “**IP Address**” tab. If the “**Obtain an IP address automatically**” is checked, this computer is ready to communicate with the **WNR2004**. If it is not, proceed to step 4.
4. If there is an IP address listed, ***WRITE DOWN*** this IP address on the memo page of this manual (page 115).
5. Select the **DNS configuration** tab. If there is an IP address listed on this tab, ***WRITE DOWN*** this IP address on the memo page of this manual (page 115).

**NOTE: After you’ve configured your PC to communicate with the WNR2004, you might need to enter these IP addresses into the router in order to share your internet access through your Cable or DSL modem.**

6. Select **Obtain an IP address automatically**.
7. Click the **OK** button in the “**TCP/IP Properties**” window, and click **OK** in the “**Network**” window.
8. Restart the computer if asked.

Repeat for each PC on your network. When all of your PCs are configured, continue to Step 3: Basic Router Configuration on page 21.

FOR WINDOWS 2000

1. Click on **Start, Settings, Control Panel**. Double click on **Network and Dial-up Connections**.
2. Right click on the **Local Area Connection** that is associated with the network adapter you are using and select the **Properties** option.
3. In the “**Components checked are used by this connection**” box, highlight Internet Protocol (TCP/IP), and click the “**Properties**” button. If the “**Obtain an IP address automatically**” is checked, this computer is ready to communicate with the WNR2004. If it is not, proceed to step 4.
4. If there are any IP addresses listed on this screen, ***WRITE DOWN*** these IP addresses on the memo page of this manual (page 115). There may be an IP address listed under **Use the Following IP Address** and one under **Use the Following DNS Server Addresses**. Be sure to make a note of ***BOTH*** IP addresses.

**NOTE: After you’ve configured your PC to communicate with the WNR2004, you might need to enter these IP addresses into the router in order to share your Internet access through your Cable or DSL modem.**

5. Select **Obtain an IP address automatically**.
6. Click the **OK** button in the **Internet Protocol (TCP/IP) Properties** window, and click the **OK** button in the **Local Area Connection Properties** window.
7. Restart the computer if asked.

Repeat for each PC on your network. When all of your PCs are configured, continue to Step 3: Basic Router Configuration on page 21.

FOR WINDOWS NT 4.0

1. Click on **Start, Settings, Control Panel**. Double click on **Network**.
2. Select the **Protocol** tab, and double click on **TCP/IP Protocol**.
3. When the window appears, select the correct adapter for your network adapter. If the **Obtain an IP address from a DHCP Server** is checked, this computer is ready to communicate with the WNR2004. If it is not, proceed to step 4.
4. If there is an IP address listed, ***WRITE DOWN*** this IP address on the memo page of this manual (page 115).
5. Select the **DNS configuration** tab. If there is an IP address listed on this tab, ***WRITE DOWN*** this IP address on the memo page of this manual (page 115).

**NOTE: After you've configured your PC to communicate with the WNR2004, you might need to enter these IP addresses into the router in order to share your Internet access through your Cable or DSL modem.**

4. Select **Obtain an IP address from a DHCP Server**.
5. Click the **OK** button in the **TCP/IP Properties** window, and click **OK** in the "**Network**" window.
6. Restart the computer if asked.

Repeat for each PC on your network. When all of your PCs are configured, continue to Step 3: Basic Router Configuration on page 21.

FOR WINDOWS XP

1. Click on **Start**, **Settings**. If your view is already **Classic View**, proceed to step 2. Otherwise, switch your view to **Classic View** by right clicking your mouse while the cursor is over the **Start** button.
2. Double click on **Network Connections**.
3. Right click on the **Local Area Connection** that is associated with the network adapter you are using, and select the **Properties** option.
4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button. If the **Obtain an IP address automatically** is checked, this computer is ready to communicate with the WNR2004. If it is not, proceed to step 5.
5. If there is an IP address listed, ***WRITE DOWN*** this IP address on the memo page of this manual (page 115).
6. Select the **DNS configuration** tab. If there is an IP address listed on this tab, ***WRITE DOWN*** this IP address on the memo page of this manual (page 115).

**NOTE: After you've configured your PC to communicate with the WNR2004, you might need to enter these IP addresses into the router in order to share your Internet access through your Cable or DSL modem.**

7. Select **Obtain an IP address from a DHCP Server**.
8. Click the **OK** button in the **Internet Protocol (TCP/IP) Properties** window. Click the **OK** button in the **Local Area Connection Properties** window.
9. Restart your computer if asked.

Repeat for each PC on your network. When all of your PCs are configured, continue to Step 3: Basic Router Configuration below.

## STEP 3: BASIC ROUTER CONFIGURATION

The **WNR2004 802.11b AP/Router** uses a browser-based management/configuration interface. Although the router's default settings allow most users to connect with no further configuration, you will need to set the password, time zone, and any desired parental access control rules. In some cases, you may have to change a few of the communications settings to connect to your ISP.

Your router will require more advanced configuration if any of the following conditions apply:

- Your ISP gives you a static IP address to use for your computer.
- Your ISP requires PPPoE support.
- Your ISP requires you to have a specific MAC or hardware address to connect to the network (MAC address spoofing).
- You want to make sure a particular PC (e.g., a mail server or a web host) always gets the same IP address (fixed IP address function).
- You need to run an Internet server or a web host from within the firewall (port mapping or DMZ functions).
- You want to use the Universal Plug and Play feature (UPnP).
- You want to block an external PC from communicating with your network (MAC address blocking function).
- You need to configure the router's DHCP settings or configure the router to operate within a LAN that has an existing DHCP server.
- You want to route or block data based on information in each individual data packet (packet filtering feature).
- You want to link your router to a dynamic DNS service.

If none of these conditions apply to you, then the basic configuration should be all you need. Even if you do need advanced configuration, you will need to perform the basic configuration as the first steps of an advanced configuration.

### LOGGING IN

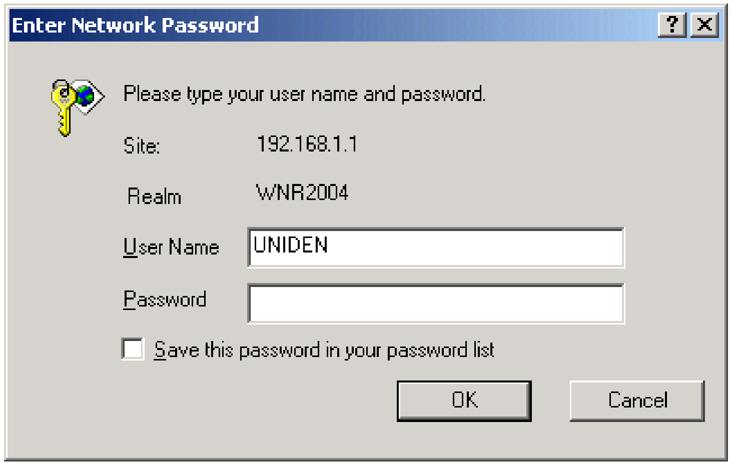
Before starting, be sure your computer is correctly configured to obtain an IP address automatically in the TCP/IP networking setup. If you have any trouble communicating with the WNR2004, see Step 2: PC Configuration on page 16.

1. Open a web browser window, Internet Explorer or Netscape.
2. In the location field at the top of the browser window (where you normally type the web page address), type the following text exactly as shown:

```
http://192.168.1.1
```

3. Hit **Enter**. The router will display the **Enter Network Password** window (see Figure 1).

**NOTE: If the enter password window does not display, double check the hardware setup in Step 1: Hardware Installation on page 14 and Step 2: PC Configuration on page 16.**



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm WNR2004

User Name UNIDEN

Password

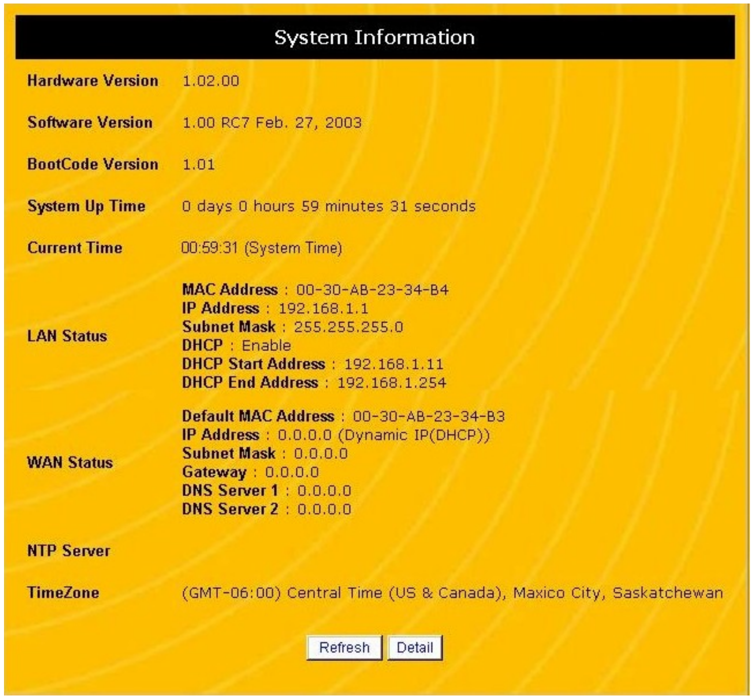
□ Save this password in your password list

Figure 1 Enter Network Password Screen

4. In the **User Name** field, enter the following (in upper case):

   `UNIDEN`

5. Leave the **Password** field blank and click **OK**. The router will display the **System Information** screen.



System Information

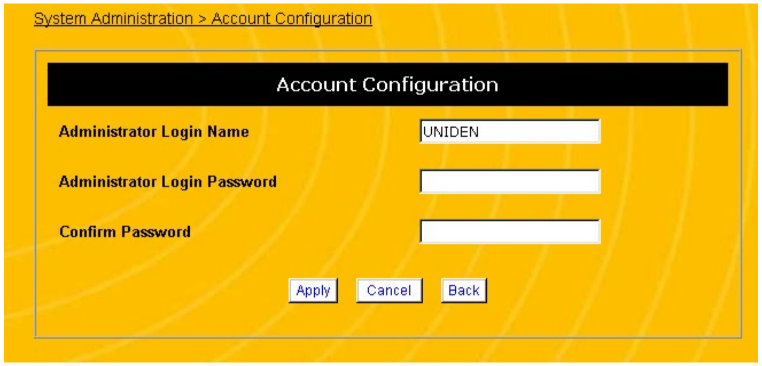
|  |  |
|---|---|
| **Hardware Version** | 1.02.00 |
| **Software Version** | 1.00 RC7 Feb. 27, 2003 |
| **BootCode Version** | 1.01 |
| **System Up Time** | 0 days 0 hours 59 minutes 31 seconds |
| **Current Time** | 00:59:31 (System Time) |
| **LAN Status** | **MAC Address** : 00-30-AB-23-34-B4<br>**IP Address** : 192.168.1.1<br>**Subnet Mask** : 255.255.255.0<br>**DHCP** : Enable<br>**DHCP Start Address** : 192.168.1.11<br>**DHCP End Address** : 192.168.1.254 |
| **WAN Status** | **Default MAC Address** : 00-30-AB-23-34-B3<br>**IP Address** : 0.0.0.0 (Dynamic IP(DHCP))<br>**Subnet Mask** : 0.0.0.0<br>**Gateway** : 0.0.0.0<br>**DNS Server 1** : 0.0.0.0<br>**DNS Server 2** : 0.0.0.0 |
| **NTP Server** |  |
| **TimeZone** | (GMT-06:00) Central Time (US & Canada), Maxico City, Saskatchewan |

Figure 2 System Information Screen

6. On the **System Information** screen (Figure 2), note the hardware version, software version, and boot code version in the memo section of this manual (page 115) for future reference.

## CHANGING THE DEFAULT PASSWORD

1. In the menu on the left of the screen, click on **System Administration**, then **Account Configuration**. This displays the **Account Configuration** screen (see Figure 3).



System Administration > Account Configuration

Account Configuration

Administrator Login Name: UNIDEN

Administrator Login Password:

Confirm Password:

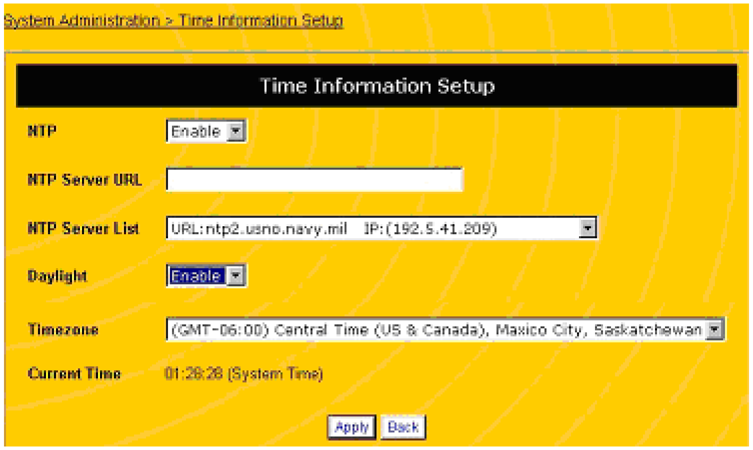
Figure 3 Account Configuration Screen

2. Change the **Administrative Login Name** and **Administrative Password**. Make a note of the login name and password in the memo section of this manual (page 115).
3. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **Cancel**. We will reboot the router after all the changes are made.

**NOTE: The new name and password will take effect when you reboot the router.**

CONFIGURING THE TIME

1. In the menu on the left of the screen, click on **System Administration** and then **Time Information Setup**. This displays the **Time Information Setup** screen (Figure 4).



System Administration > Time Information Setup

Time Information Setup

NTP: Enable

NTP Server URL:

NTP Server List: URL:ntp2.usno.navy.mil IP:(192.5.41.209)

Daylight: Enable

Timezone: (GMT-06:00) Central Time (US & Canada), Mexico City, Saskatchewan

Current Time: 01:28:28 (System Time)

Figure 4 Time Information Setup Screen

2. In the **Timezone** field, select the time zone you are in.
3. If you want to enable the *Network Time Protocol* on the router, select **Enable** in the **NTP** field. NTP is an Internet protocol standard that will be used to synchronize Routers clock to an internet based NTP server such as the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO.
4. If you enable NTP, enter the **NTP Server URL**, or select an NTP server from the **NTP Server List**.
5. If you want your router to recognize Daylight Savings Time, select **Enable** in the **Daylight** field.
6. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **Cancel**. We will reboot the router after all the changes are made.

## SETTING PARENTAL CONTROLS

Parental controls allow you to control Internet access for the network as a whole or for each PC using its *MAC address* (a hardware identification number assigned to an individual PC).

To access parental control features, in the menu on the left of the screen, click on **Firewall/Security** and then **Parental Controls**. This displays the **Parental Controls** screen (see Figure 5).

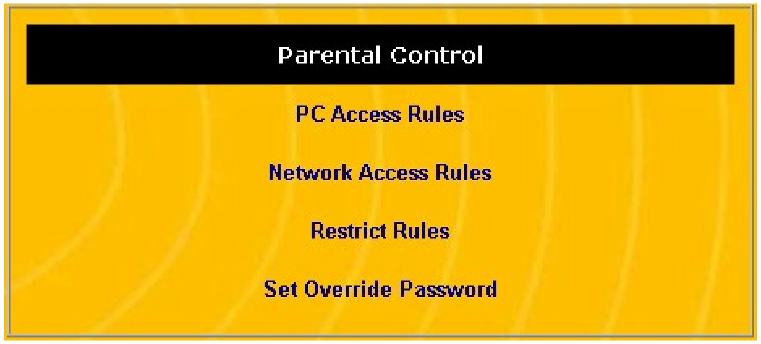
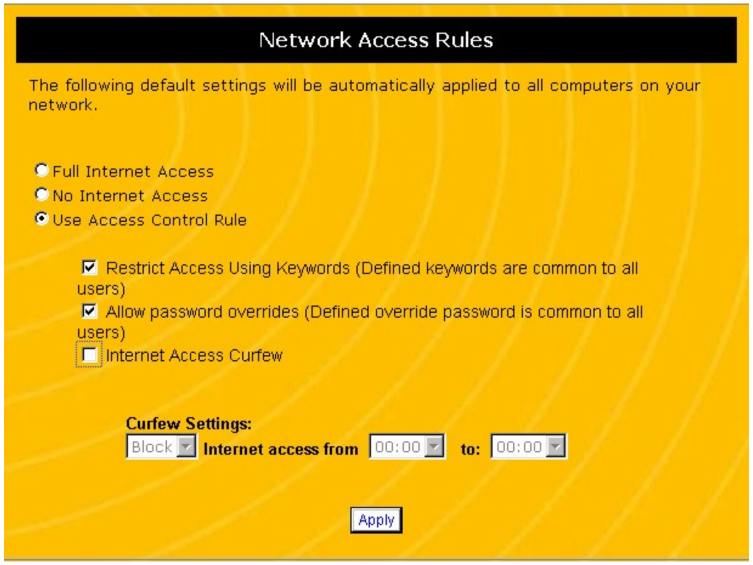


**Figure 5 Parental Controls Screen**

## NETWORK-LEVEL CONTROL

If you want to set access control for the whole network, click Network Access Rules. This displays the **Network Access Rules** screen (see Figure 6).

**NOTE: All settings on this screen apply to all computers connected to the router.**



Network Access Rules

The following default settings will be automatically applied to all computers on your network.

○ Full Internet Access
○ No Internet Access
● Use Access Control Rule

☑ Restrict Access Using Keywords (Defined keywords are common to all users)
☑ Allow password overrides (Defined override password is common to all users)
□ Internet Access Curfew

Curfew Settings:
Block Internet access from 00:00 to: 00:00

**Figure 6 Network Access Rules Screen**

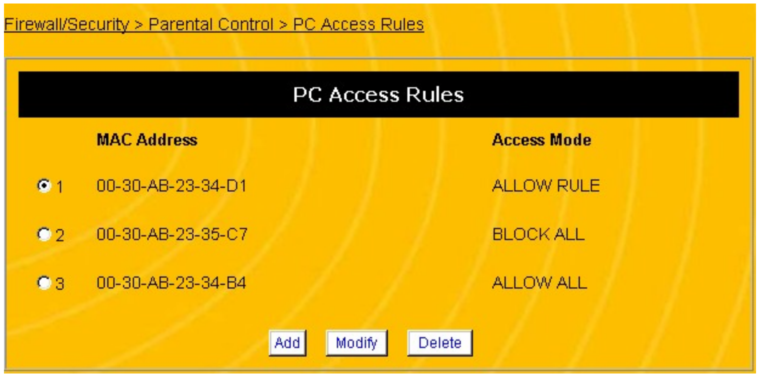
1. Select the level of Internet access you want to allow for the network: full Internet access, no Internet access, or access based on rules. If you click **Use Access Control Rules**, configure the rules in the lower half of the screen.
2. If you want to restrict access based on certain keywords, click **Restrict Access Using Keywords**. You will define keywords on the **Restrict Rules** screen (see page 32).
3. If you want to allow a temporary password override for the Internet restrictions, click **Allow Password Overrides**. You will define keywords on the **Set Override Password** screen (see page 33).
4. If you want to restrict access based on the time of day, click **Internet Access Curfew**. Enter the time range during

which you want to **Block** or **Allow** Internet access. (Times are in 24-hour format, so to block access from 10:00 pm to 6:00 am, select **Block** from **22:00** to **06:00**.)

5. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **Cancel**. We will reboot the router after all the changes are made.

## PC-LEVEL CONTROL

The router can also set access control based on each PC's MAC address. The MAC address is a unique hardware address assigned to each PC; MAC addresses are a six-part character code separated by dashes or colons. If you want to set access control for individual PCs by their MAC addresses, click **PC Access Rules**. This displays the **PC Access Rules** screen (see Figure 7).



Firewall/Security > Parental Control > PC Access Rules

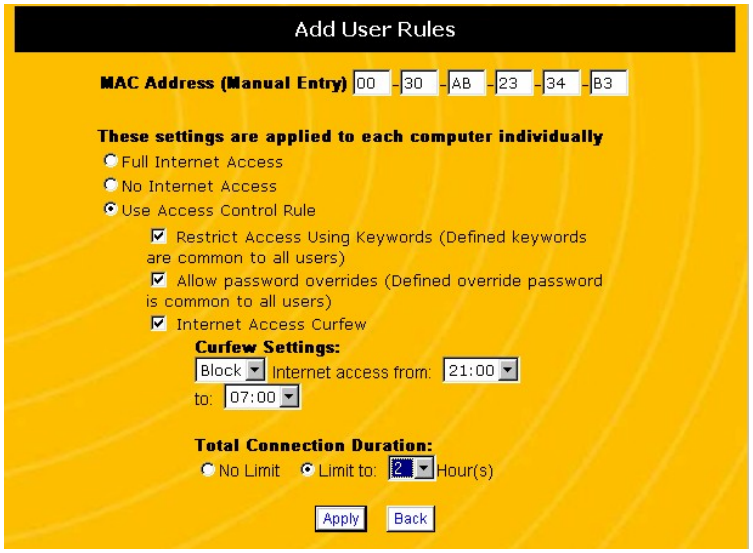
PC Access Rules

| | MAC Address | Access Mode |
|---|---|---|
| ● 1 | 00-30-AB-23-34-D1 | ALLOW RULE |
| ○ 2 | 00-30-AB-23-35-C7 | BLOCK ALL |
| ○ 3 | 00-30-AB-23-34-B4 | ALLOW ALL |

**Figure 7 PC Access Rules Screen**

The PC Access Rules screen displays the MAC address of each PC that has rules associated with it and whether the PC is allowed full Internet access (ALLOW ALL), no Internet access (BLOCK ALL), or Internet access based on a rule (ALLOW RULE). When you first open this screen, it will be blank except for the **Add**, **Modify**, and **Delete** buttons at the bottom.

1. To add access control rules to a new PC, click the **Add** button. This displays the **Add User Rules** screen (see Figure 8).



Add User Rules

MAC Address (Manual Entry) 00 - 30 - AB - 23 - 34 - B3

These settings are applied to each computer individually

○ Full Internet Access
○ No Internet Access
● Use Access Control Rule
☑ Restrict Access Using Keywords (Defined keywords are common to all users)
☑ Allow password overrides (Defined override password is common to all users)
☑ Internet Access Curfew

Curfew Settings:
Block Internet access from: 21:00 to: 07:00

Total Connection Duration:
○ No Limit ● Limit to: 2 Hour(s)

**Figure 8 Add User Rules Screen**

**NOTE: PCs have full access by default. If you do not add a PC to the User Rules list, that PC has full access.**

2. Enter the MAC Address of the PC you want to create rules for. Be sure to enter the six separate parts of the MAC address into the six separate boxes in the field. (If you do not know the MAC address of the PC, click on **DCHP Server**

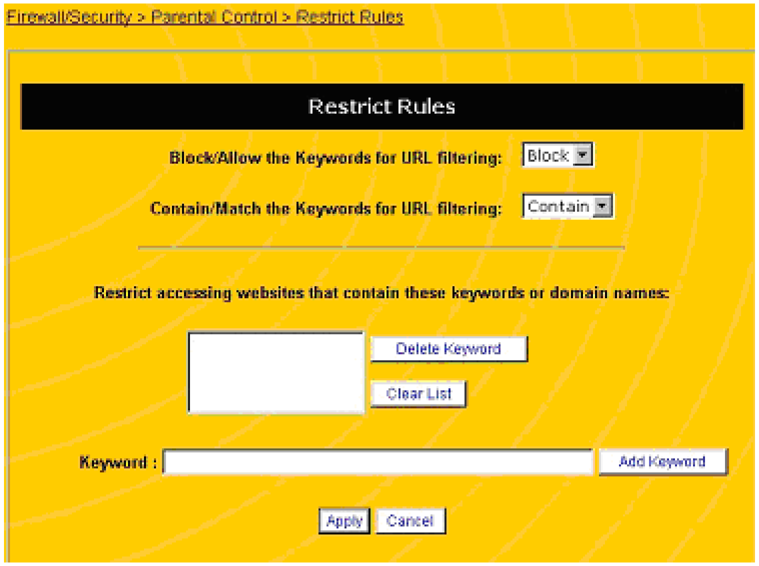
at the left of the screen (see X-REF). The bottom of this screen displays the MAC addresses of all computers connected to the router.)

3. Select the level of Internet access you want to allow for the network: full Internet access, no Internet access, or access based on rules. If you click **Use Access Control Rules**, configure the rules in the lower half of the screen.
4. If you want to restrict the PC's access based on certain keywords, click **Restrict Access Using Keywords**. You will define keywords on the **Restrict Rules** screen (see page 32).
5. If you want to allow a temporary password override for the Internet restrictions, click **Allow Password Overrides**. You will define keywords on the **Set Override Password** screen (see page 33). The override password applies to all users.
6. If you want to restrict this PC's access based on the time of day, click **Internet Access Curfew**. Enter the time range during which you want to **Block** or **Allow** Internet access. (Times are in 24-hour format, so to block access from 10:00 pm to 6:00 am, select **Block** from **22:00** to **06:00**.)
7. To restrict this PC to a certain amount of connection time, under Total Connection Duration Time, click Limit To and select the number of hours per day this PC is allowed to access the Internet.
8. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **Cancel**. We will reboot the router after all the changes are made.
9. Repeat the process with any other computers you wish to restrict access for.

10. To change the rules configuration for a PC, select the PC's MAC address on the PC Access Rules screen (see Figure 7 on page 29) and click the **Modify** button.
11. To delete all rules for a PC, select the PC's MAC address on the PC Access Rules screen (see Figure 7 on page 29) and click the **Delete** button.

## CONFIGURING RESTRICTION RULES

If you want to set access control for individual PCs by their unique MAC address, click **Restrict Rules**. This displays the **Restrict Rules** screen (see Figure 9).



Firewall/Security > Parental Control > Restrict Rules

Restrict Rules

Block/Allow the Keywords for URL filtering: Block

Contain/Match the Keywords for URL filtering: Contain

Restrict accessing websites that contain these keywords or domain names:

Keyword :

**Figure 9 Restrict Rules Screen**

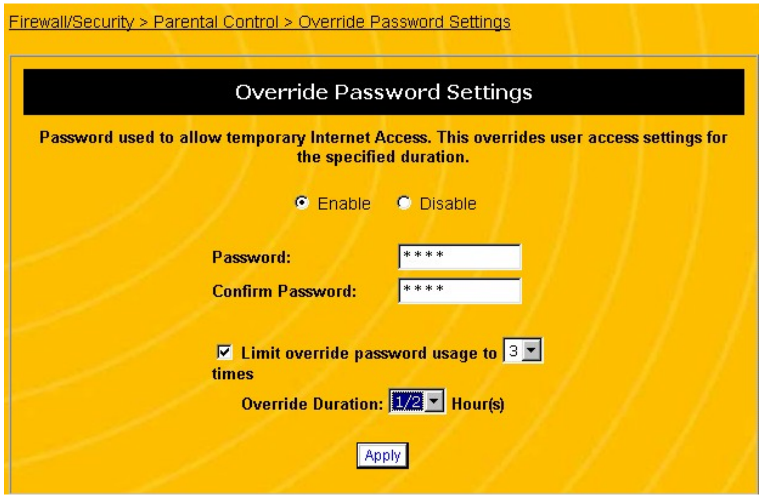
The Restrict Rules screen allows you to create a list of keywords for restricting Internet access. You can list keywords to block or to allow.

**NOTE: The same keyword list applies any PCs configured to use keyword-based restrictions.**

1. Under **Block/Allow the Keywords for URL Filtering**, select whether you want to create a list of keywords to **Block** or to **Allow**. If you select **Block**, PCs restricted by this rule will not be allowed to access sites that match keywords on the list. If you select **Allow**, PCs restricted by this rule will ONLY be allowed access to sites that match keywords on the list.
2. Under **Contain/Match the Keywords for URL Filtering**, select whether you want to restrict URLs that **Contain** the listed keywords or exactly **Match** the listed keywords.
3. Enter the keywords under the **Keyword** field at the bottom of the screen.
4. Click **Add Keyword** to add the keyword to the list.
5. If you want to delete a keyword, highlight the keyword on the list and click **Delete Keyword**. If you want to delete all the keywords from the list, click **Clear List**.
6. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **Cancel**. We will reboot the router after all the changes are made.

## CONFIGURING AN OVERRIDE PASSWORD

If you want to set a password to temporarily override Internet access restrictions, click **Set Override Password**. This displays the **Override Password Settings** screen (see Figure 10)



Firewall/Security > Parental Control > Override Password Settings

Override Password Settings

Password used to allow temporary Internet Access. This overrides user access settings for the specified duration.

● Enable ○ Disable

Password: ****

Confirm Password: ****

☑ Limit override password usage to 3 times

Override Duration: 1/2 Hour(s)

**Figure 10 Override Password Settings Screen**

1. To activate an override password, click **Enable**.
2. Enter the password under the **Password** field. Confirm the password by entering it again in the **Confirm Password** field.

**NOTE: For security reasons, the password will not be visible from this screen. Make a note of the password in the memo page of this manual (page 115) or some other safe location.**

3. If you want the password to expire after a certain number of uses, click **Limit Override Password Usage**. Then, enter the number of times the password will work before it expires.
4. In the **Override Duration** field, select the number of hours of Internet access the override password will grant. After this

amount of time has expired, the router will disconnect the PC.

5. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **Cancel**. We will reboot the router after all the changes are made.

## CONFIGURING BASIC ISP CONNECTIONS

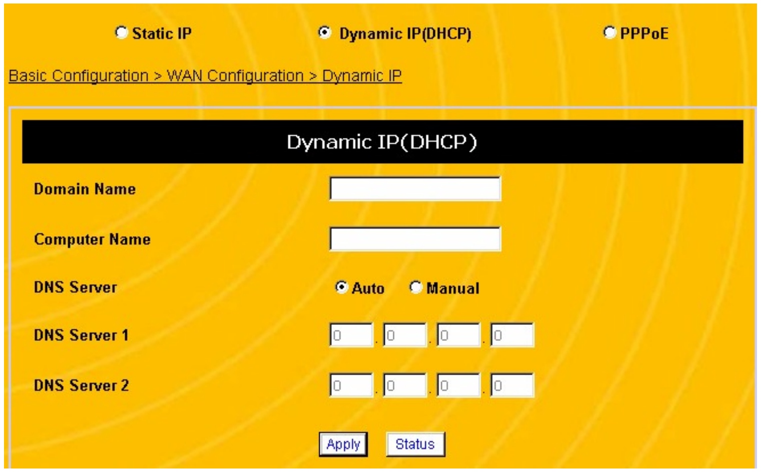
In many cases, you will be able to connect to your ISP without adjusting any of your router's communication settings. However, if your ISP assigns you a domain name or URL (e.g.,jonesfamily.net) or if your ISP tells you to communicate with a particular Domain Name System (*DNS*) server, you will need to enter this information into the router. (A DNS server translates the domain name or URL into the numeric designation—or *IP address*—of the computer that maintains that web site.)

To correctly configure the router to connect to the Internet, you may need the following information from your ISP:

- The domain name you were assigned by your ISP
- The name your computer was assigned by your ISP
- The IP addresses of the primary and secondary Domain Name System (*DNS*) servers used by your ISP. The IP address is a four-part number separated by periods. (You can also configure the router to automatically obtain the DNS server address from your ISP.)

Once you have all this information, you are ready to configure your router to communicate with your ISP:

1. In the menu on the left of the screen, click on **Basic Configuration** and then **WAN**. This displays the **WAN Configuration, Dynamic IP** screen (see Figure 5).



○ Static IP ● Dynamic IP(DHCP) ○ PPPoE

Basic Configuration > WAN Configuration > Dynamic IP

Dynamic IP(DHCP)

Domain Name

Computer Name

DNS Server ● Auto ○ Manual

DNS Server 1: 0 . 0 . 0 . 0

DNS Server 2: 0 . 0 . 0 . 0

**Figure 11 WAN Configuration, Dynamic IP Screen**

2. In the **Domain Name** field, enter the domain name you were assigned by your ISP.
3. In the **Computer Name** field, enter the name your computer was assigned by your ISP.
4. Under the **DNS Server** fields, select **Auto** to have the router automatically obtain the DNS server information from your ISP. Select **Manual** if you want to enter DNS server information by hand.
5. If you select **Manual** under **DNS Server**, enter the IP address of the primary and secondary (if available) DNS server used by your ISP. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

6. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, use the reboot command. See Rebooting the Router on page 77.**

# Advanced Router Configuration

For most users, the default settings of the router are exactly what they need; there is no reason for them go beyond the basic configuration we've already discussed. However, if one of the following conditions applies to your PC and network, you will need to delve into the more advanced configuration options of the router:

- Your ISP gives you a static IP address.
- Your ISP requires PPPoE support.
- Your ISP requires you to have a specific MAC or hardware address to connect to the network (MAC address spoofing).
- You want to make sure a particular PC (e.g., a mail server or a web host) always gets the same IP address.
- You need to run an Internet server or a web host from within the firewall (port mapping function).
- You want to use the Universal Plug and Play feature (UPnP).
- You have programs that must operate outside the firewall (DMZ function).
- You want to block an external PC from communicating with your network (MAC address blocking).
- You need to configure the router's DHCP settings or configure the router to operate within a LAN that has an existing DHCP server.
- You want to route or block data based on information in each individual data packet (packet filtering feature).

- You want to link your router to a dynamic DNS service.

## CONFIGURING FOR A STATIC IP ADDRESS

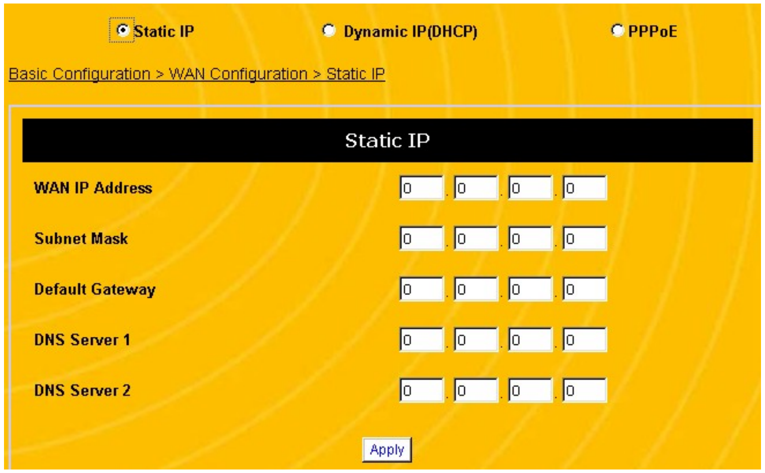
Follow the procedure below if your ISP provided you with a static IP address. If your ISP gave you a four-part number as “your address,” it is probably a static IP address. If your ISP did not give you an IP address at all, you do not have a static IP address. If you are not sure if you have a static IP address or what it might be, contact your ISP.

To complete this configuration process, you will need the following information from your ISP:

- Your static IP address (a four-part number separated by dots or periods)
- The subnet mask (also a four-part number separated by periods). The default value is 255.255.255.0
- The default gateway address. This is the IP address of your ISP’s router.
- The IP address of the Domain Name System (*DNS*) server(s) used by the ISP.

Once you have all this information, you are ready to configure your router to communicate with your ISP:

1. Open a browser window and login to the router.
2. Click **Basic Configuration**, then **WAN**. This displays the **WAN Configuration** screen.
3. At the top of the screen, click the radio button marked **Static IP**. This displays the **Static IP** screen (see Figure 12).



● Static IP ○ Dynamic IP(DHCP) ○ PPPoE

Basic Configuration > WAN Configuration > Static IP

Static IP

| | | | | |
|---|---|---|---|---|
| WAN IP Address | 0 | 0 | 0 | 0 |
| Subnet Mask | 0 | 0 | 0 | 0 |
| Default Gateway | 0 | 0 | 0 | 0 |
| DNS Server 1 | 0 | 0 | 0 | 0 |
| DNS Server 2 | 0 | 0 | 0 | 0 |

**Figure 12 WAN Configuration, Static IP Screen**

4. Under the **WAN IP Address** field, enter the IP address you received from your ISP. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.
5. Under the **Subnet Mask** field, enter the subnet mask you received from your ISP. Be sure to enter the four separate parts of the subnet mask into the four separate boxes in the field.
6. Under the **Default Gateway** fields, enter the IP address of your ISP’s preferred router. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.
7. Under the **DNS Server** fields, enter the IP address of the primary and secondary (if available) DNS server used by your ISP. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

8. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, use the reboot command. See Rebooting the Router on page 77.**

## CONFIGURING FOR PPPoE SUPPORT

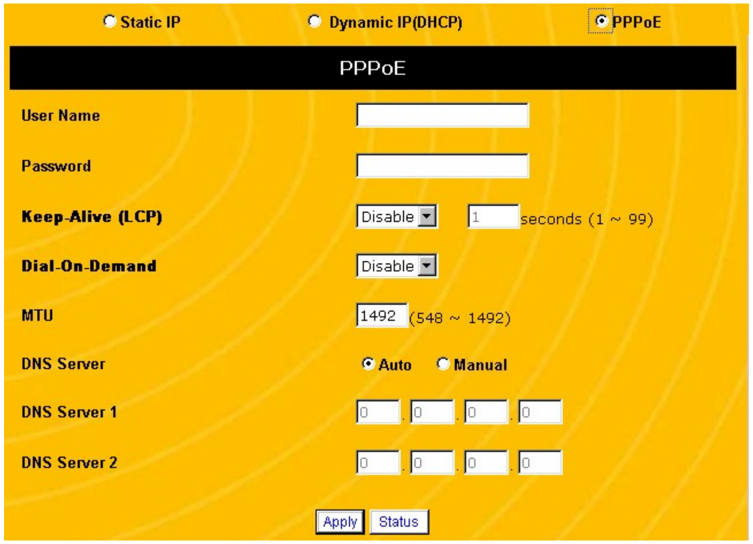
Follow the procedure below if your ISP requires PPPoE support. If you use a cable modem or DSL to connect to the Internet, you may need this feature enabled. To complete this configuration process, you will need the following information from your ISP:

- Your user name and password for your ISP account
- The Maximum Transmission Unit (*MTU*) supported by your ISP. The MTU is the largest number of bytes that can be transmitted as a single packet. (Any packets larger than this number will be broken into multiple packets before transmission.)
- The IP address of the Domain Name System (*DNS*) server used by the ISP. (You can also configure the router to automatically obtain the DNS server address from your ISP.)

Once you have all this information, you are ready to configure your router to communicate with your ISP:

1. Open a browser window and login to the router.
2. Click **Basic Configuration**, then **WAN**. This displays the **WAN Configuration** screen.

3. At the top of the screen, click the radio button marked **PPPoE**. This displays the **PPPoE** screen (see Figure 13).



○ Static IP ○ Dynamic IP(DHCP) ● PPPoE

PPPoE

| | |
|---|---|
| User Name | |
| Password | |
| Keep-Alive (LCP) | Disable 1 seconds (1 ~ 99) |
| Dial-On-Demand | Disable |
| MTU | 1492 (548 ~ 1492) |
| DNS Server | ● Auto ○ Manual |
| DNS Server 1 | 0 . 0 . 0 . 0 |
| DNS Server 2 | 0 . 0 . 0 . 0 |

**Figure 13 WAN Configuration, PPPoE Screen**

4. Under the **User Name** field, enter the name you use to login to the your ISP.
5. Under the **Password** field, enter the password you use to login to your ISP.
6. Many ISPs will disconnect a PC after a certain period of inactivity. The keep-alive function sends out a packet at a designated time interval to keep the ISP link active. If you want to turn on the keep-alive function, select **Enable** in the **Keep-Alive** field, then enter the number of seconds that should pass before the router sends out a packet. For example, if you enter 45 seconds, the router will transmit a

packet every 45 seconds to make sure the ISP does not disconnect the link.

7. Dial-on-demand is a feature that only activates the Internet connection when a program specifically calls for it. If you want to turn on the dial-on-demand function, select Enable in the **Dial-on-Demand** field.

8. In the **MTU** field, enter the maximum transmission unit allowed by your ISP. If your ISP has not specified an MTU size then 1492 is typically the default.

9. Under the **DNS Server** fields, select **Auto** to have the router automatically obtain the DNS server information from your ISP. Select **Manual** if you want to enter DNS server information by hand.

10. If you select **Manual** under **DNS Server**, enter the IP address of the primary and secondary (if available) DNS server used by your ISP. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

11. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, you must use the reboot command. See Rebooting the Router on page 77.**

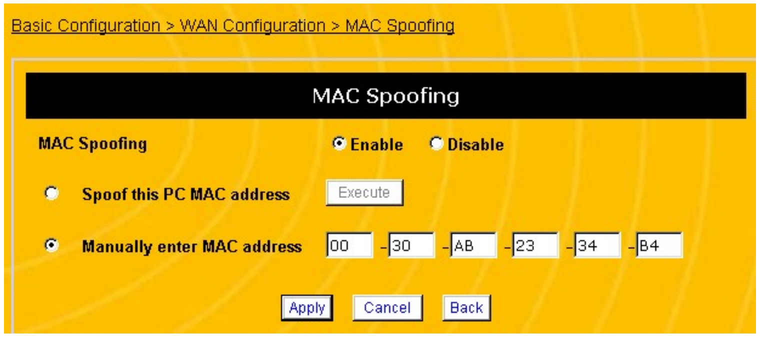
## ENABLING MAC ADDRESS SPOOFING

Some ISPs require you to have a single MAC address to connect to the Internet. (The MAC address is a unique hardware address assigned to each PC; MAC addresses are a six-part character code separated by dashes or colons.) With MAC address spoofing, you can configure the router to transmit data using the MAC address that the ISP expects.

Follow the steps below to enable MAC address spoofing:

1. Open a browser window and login to the router.

2. In the menu at the left side of the screen, click **Basic Configuration**, then **WAN**, then **MAC Address Spoofing**. This displays the **MAC Spoofing** screen (see Figure 14).



Basic Configuration > WAN Configuration > MAC Spoofing

MAC Spoofing

MAC Spoofing ● Enable ○ Disable

○ Spoof this PC MAC address Execute

● Manually enter MAC address 00 - 30 - AB - 23 - 34 - B4

**Figure 14 MAC Spoofing Screen**

3. Click **Enable** to turn on the MAC spoofing feature.

4. To have the router use the MAC address of the PC you are currently using, click **Spoof this PC MAC Address** and then click **Execute**. The router will automatically obtain the MAC address from the computer you are using and enter it into the MAC address field.

5. To manually enter a specific MAC address, click **Manually enter MAC Address**, then enter the MAC address. Be sure to enter the six separate parts of the MAC address into the six separate boxes in the field.

6. Click **Apply**. If the router displays a dialogue box that says “*Values are saved. Do you really want to reboot the system now?*” click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, you must use the reboot command. See Rebooting the Router on page 77.**

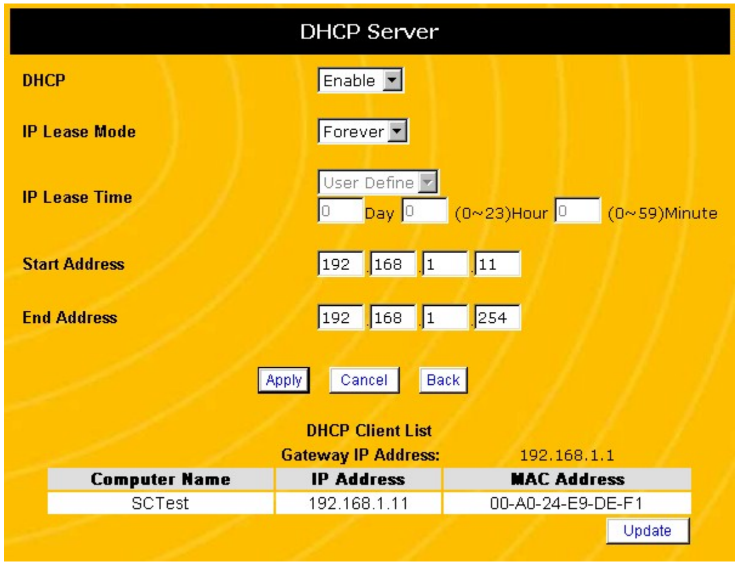
## CONFIGURING A FIXED IP ADDRESS FOR A PC

Most of the time, you want to let the router automatically assign IP addresses to computers that connect to it using Dynamic Host control Protocol or *DHCP*. In some cases—for instance, a mail server, a web host, or a computer that operates as the DMZ—you need to make sure that a PC always receives the same IP address.

### RESERVING FIXED IP ADDRESSES

If the PC supports DHCP, follow the steps below to configure the router to always give the same IP address to that PC:

1. Open a browser window and login to the router.
2. Click **Basic Configuration**, then **DHCP Server**. This displays the **DHCP Server** screen (see Figure 15).



DHCP Server

DHCP: Enable

IP Lease Mode: Forever

IP Lease Time: User Define
0 Day 0 (0~23)Hour 0 (0~59)Minute

Start Address: 192 . 168 . 1 . 11

End Address: 192 . 168 . 1 . 254

Apply Cancel Back

DHCP Client List

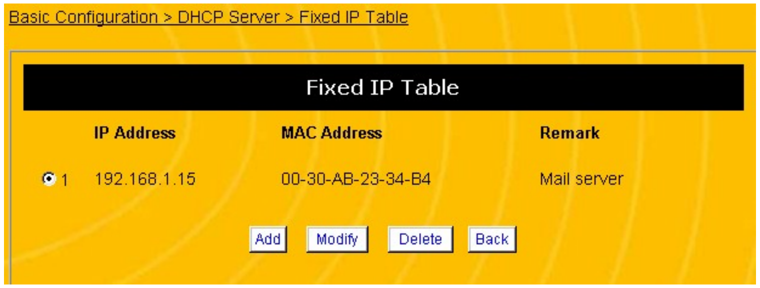
Gateway IP Address: 192.168.1.1

| Computer Name | IP Address | MAC Address |
|---|---|---|
| SCTest | 192.168.1.11 | 00-A0-24-E9-DE-F1 |

Update

**Figure 15 DHCP Server Screen**

3. In the DHCP client list at the bottom of the screen, identify the computer you want to assign the fixed IP address to. Copy down the PC’s IP address and MAC address. If you have not yet connected the PC, identify an unused IP address to reserve for the fixed IP address computer.
4. In the menu on the left frame, click **Fixed IP Table**. This displays the **Fixed IP Table** screen. (See Figure 16.)

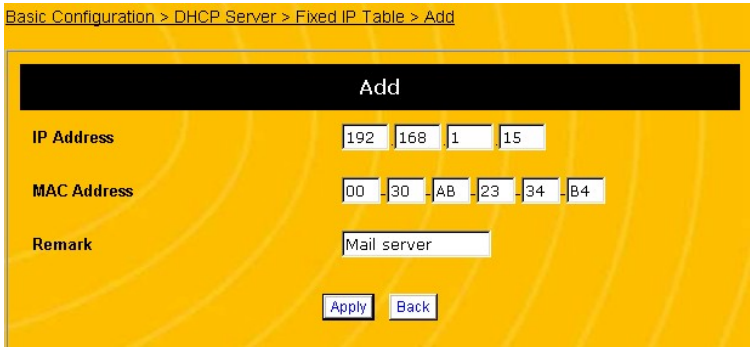


Fixed IP Table

| | IP Address | MAC Address | Remark |
|---|---|---|---|
| ● 1 | 192.168.1.15 | 00-30-AB-23-34-B4 | Mail server |

**Figure 16 DHCP, Fixed IP Table Screen**

5. Click the **Add** button at the bottom of the screen. This displays the **Add Fixed IP** screen. (See Figure 17.)



Add

IP Address: 192 . 168 . 1 . 15

MAC Address: 00 - 30 - AB - 23 - 34 - B4

Remark: Mail server

**Figure 17 DHCP, Add Fixed IP Screen**

6. Enter the **IP Address** you want to reserve for the PC. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.
7. Enter the **MAC Address** of the PC.
8. Enter any **Remarks** or comments, and click **Apply**. The router will return you to the **Fixed IP Table** screen.

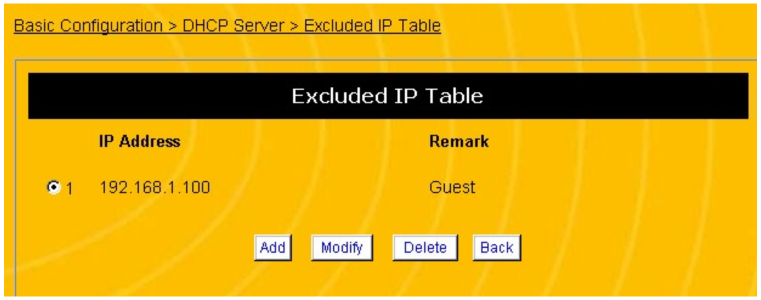
9. Repeat the process with any other computers you wish to reserve IP addresses for.
10. To change the IP address for a PC, select the PC's MAC address on the **Fixed IP Table** screen and click the **Modify** button. Make any changes and click **Apply**. The router will return you to the **Fixed IP Table** screen.
11. To delete the IP address for a PC, select the PC's MAC address on the **Fixed IP Table** screen and click the **Delete** button.

## EXCLUDING FIXED IP ADDRESSES

If the PC does not support DHCP, you will need to manually configure the IP address on that PC and then make sure that the DHCP server never assigns that IP address. If you add the address in the DHCP server's "exclude" table, we can make sure the router never assigns that IP address.

Follow the steps below to configure the router to exclude the IP address assigned to the PC:

1. At the PC, manually configure the IP address. Record the IP address.
2. Open a browser window and login to the router.
3. Click **Basic Configuration**, then **DHCP Server**, then **Excluded IP Table**. This displays the **Excluded IP Table** screen (see Figure 18).



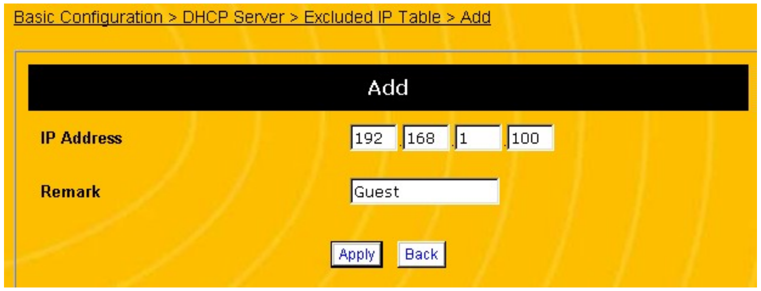
Basic Configuration > DHCP Server > Excluded IP Table

Excluded IP Table

| | IP Address | Remark |
|---|---|---|
| ● 1 | 192.168.1.100 | Guest |

**Figure 18 DHCP, Excluded IP Table Screen**

4. Click the **Add** button at the bottom of the screen. This displays the **Add Excluded IP** screen. (See Figure 19.)



Basic Configuration > DHCP Server > Excluded IP Table > Add

Add

| | |
|---|---|
| **IP Address** | 192 . 168 . 1 . 100 |
| **Remark** | Guest |

**Figure 19 DHCP, Add Excluded IP Screen**

5. Enter the **IP Address** that the DHCP server should not assign (i.e., the address you manually configured on the PC). Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

6. Enter any **Remarks** or comments, and click **Apply.** The router will return you to the **Excluded IP Table** screen.

7. Repeat the process with any other IP addresses you wish to add to the DHCP server's "exclude" list.

8. To change the IP address, select the address on the **Excluded IP Table** screen and click the **Modify** button. Make any changes and click **Apply**. The router will return you to the **Excluded IP Table** screen.

9. To delete the IP address for a PC, select the PC's MAC address on the **Excluded IP Table** screen and click the **Delete** button.

## CONFIGURING A PC AS A HOST (PORT MAPPING)

The Internet uses *ports* to specify different types of service requests. For instance, an email message contains a code for port 110 (POP3 mail services) while a web page request contains a code for port 80 (HTTP services). This allows the router to send the requests to the correct host: any marked as port 110 is routed to the mail server, and any data marked as port 80 is routed to the web server.

If you want to set up one or more PCs as a host, you must tell the router what services should be sent to that host. This configuration is called *port mapping*. TCP/IP, the Internet protocol standard, has over four thousand ports defined for different services. Of these, about one thousand are considered "well-known" ports; these are the ports used most often. Table 2 lists just a few of the most commonly needed well-known ports. (Complete lists of all well-known ports are readily available online; simply do a web site search for "well-known ports".)

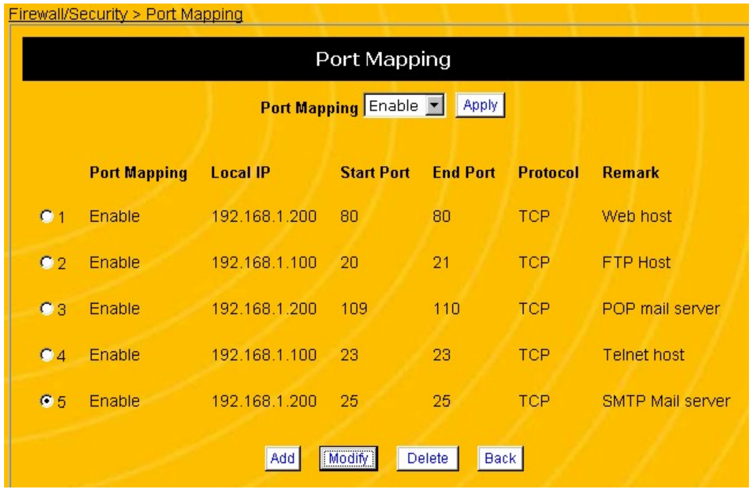
**Table 2  Commonly Used Well-Known Ports (TCP)**

| Number | Description |
|---|---|
| 18 | Message Send Protocol (MSP) |
| 20 | FTP – Data |
| 21 | FTP – Control |
| 22 | SSH Remote Login Protocol |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 49 | Login Host Protocol (Login) |
| 53 | Domain Name System (DNS) |
| 69 | Trivial File Transfer Protocol (TFTP) |
| 70 | Gopher Services |
| 80 | HTTP |
| 109 | POP2 |
| 110 | POP3 |
| 119 | Newsgroup (NNTP) |
| 194 | Internet Relay Chat (IRC) |
| 458 | Apple QuickTime |
| 1080 | Socks |

Once you have determined which PCs need to support which services, follow the steps below to configure the router to map the required ports to the host PC:

1. Assign a fixed IP address to the PC you want to set up as a service host (see *Configuring a Fixed IP Address for a PC* on page 45).  Record this IP address.

2. Open a browser window and login to the router.
3. Click **Firewall/Security**, then **Port Mapping**. This displays the **Port Mapping** screen (see Figure 20), which shows the status of existing port mappings.  When you first open this screen, it will be blank except for the **Enable** field and the buttons at the bottom of the screen.



Firewall/Security > Port Mapping

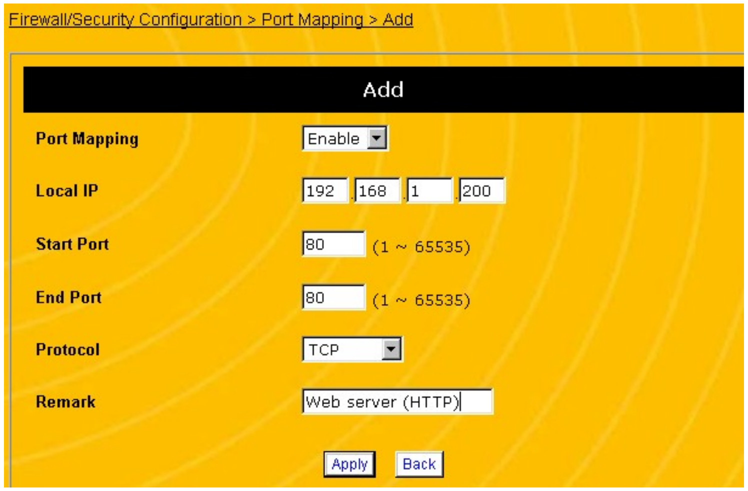
Port Mapping

Port Mapping: Enable ▼ Apply

| | Port Mapping | Local IP | Start Port | End Port | Protocol | Remark |
|---|---|---|---|---|---|---|
| ○ 1 | Enable | 192.168.1.200 | 80 | 80 | TCP | Web host |
| ○ 2 | Enable | 192.168.1.100 | 20 | 21 | TCP | FTP Host |
| ○ 3 | Enable | 192.168.1.200 | 109 | 110 | TCP | POP mail server |
| ○ 4 | Enable | 192.168.1.100 | 23 | 23 | TCP | Telnet host |
| ● 5 | Enable | 192.168.1.200 | 25 | 25 | TCP | SMTP Mail server |

**Figure 20  Port Mapping Screen**

4. In the **Port Mapping** field, select **Enable**.  This will enable all port mappings.
5. To add new port mapping, click the **Add** button.  This displays the **Port Mapping Add** screen (see Figure 21).



Firewall/Security Configuration > Port Mapping > Add

Add

Port Mapping: Enable

Local IP: 192 168 1 200

Start Port: 80 (1 ~ 65535)

End Port: 80 (1 ~ 65535)

Protocol: TCP

Remark: Web server (HTTP)

**Figure 21 Port Mapping, Add Screen**

6. In the **Port Mapping** field, select **Enable**. This will enable **this port only**.
7. In the **Local IP** field, enter the fixed IP address reserved for the host computer. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.
8. In the **Start Port** field, enter the first port of the range you want to map to this computer. (See Table 2 for a few of the most commonly needed well-known ports.)
9. In the **End Port** field, enter the last port of the range you want to map to this computer. To assign a single port to this computer, enter the same port number in the **Start** and **End** fields.

**NOTE: Port ranges are consecutive. If you need to assign non-consecutive ports to a PC, simply enter the PC twice with the different port ranges (see Figure 20 on page 52).**

10. In the **Protocol** field, select **TCP**, **UDP**, or **TCP/UDP** according to the needs of your network. TCP port mappings are different from UDP port mappings, but most of the common well-known ports are the same across both protocols. The ports listed in Table 2 are TCP protocol port mappings.
11. Enter any **Remark** or comment to help you remember what this port mapping function is.
12. Click **Apply**. This will take you back to the **Port Mapping** screen (see Figure 20 on page 52).
13. To change the port mapping for a PC, select the PC's IP address on the **Port Mapping** screen (see Figure 20 on page 52) and click the **Modify** button.
14. To delete all mapping for a PC, select the PC's IP address on the **Port Mapping** screen (see Figure 20 on page 52) and click the **Delete** button.
15. When you are finished with the port mapping, return to the **Port Mapping** screen (see Figure 20 on page 52) and click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

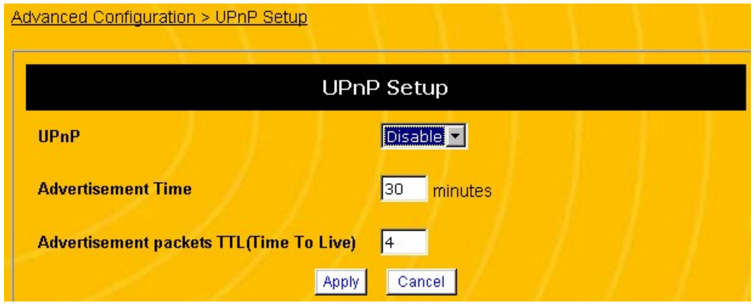
**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, use the reboot command. See Rebooting the Router on page 77.**

## CONFIGURING UNIVERSAL PLUG AND PLAY (UPnP)

Universal Plug and Play or *UPnP* is a networking architecture that provides compatibility among computers, networking equipment, software and peripherals. With UPnP, connected devices communicate their features to the network at a times interval so other devices can access those features.

Follow the steps below to configure UPnP support:

1. Open a browser window and login to the router.
2. Click **Advanced Configuration**, then **UPnP**. This displays the **UPnP Setup** screen (see Figure 22).



UPnP: Disable

Advertisement Time: 30 minutes

Advertisement packets TTL(Time To Live): 4

**Figure 22 UPnP Setup Screen**

3. In the **UPnP** field, select **Enable**.
4. In the **Advertisement Time** field, enter how often you want the router to transmit its UPnP feature message.
5. In the **Advertisement Packets TTL (Time to Live)** field, enter how many connections or devices the packet can travel through (or hop) before it expires.

6. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, use the reboot command. See Rebooting the Router on page 77.**

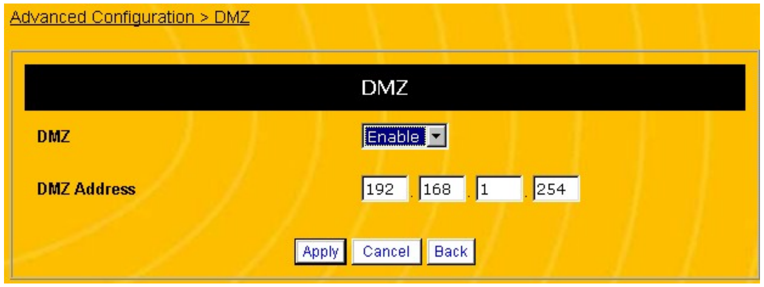
## CONFIGURING A DMZ

The router allows you to configure a single PC on the LAN to be forwarded all traffic received on the Firewalls WAN interface. If you want a PC to receive all Internet traffic unfiltered from the Internet then they should be configured as the DMZ. Follow the steps below if you need to configure a PC to operate as a DMZ.

**NOTE: Any PC that is configured to operate as the DMZ is not protected from malicious access by the router.**

**NOTE: Though a DMZ is set up to receive all traffic unfiltered by the firewall, traffic is still subject to translation by NAT. This means that Applications that are damaged by NAT (i.e. SIP) will still be affected.**

1. Assign a fixed IP address to the PC you want to set up in the DMZ (see *Configuring a Fixed IP Address for a PC* on page 45). Record this IP address.
2. Open a browser window and login to the router.
3. Click **Advanced Configuration**, then **DMZ**. This displays the **DMZ** screen (see Figure 23).



Advanced Configuration > DMZ

DMZ

DMZ: Enable

DMZ Address: 192 . 168 . 1 . 254

**Figure 23 DMZ Screen**

4. In the **DMZ** field, select **Enable**.
5. In the **DMZ Address** field, enter the fixed IP address reserved for the DMZ computer. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.
6. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, use the reboot command. See Rebooting the Router on page 77.**

## CHANGING THE DHCP CONFIGURATION

To connect to a network or to the Internet, computers need to have an IP address that identifies them to other computers on the network. Dynamic Host Control Protocol or DHCP allows computers to automatically obtain an IP address when they login so the system administrator doesn't have to manually assign an IP address for each computer.

The WNR2004 router can act as a DHCP server, so it can provide IP addresses to computers on your network. By default, the DHCP server function is enabled. In most cases, the default settings will serve your network just fine. However, you will have to change the DHCP settings if the following conditions apply:

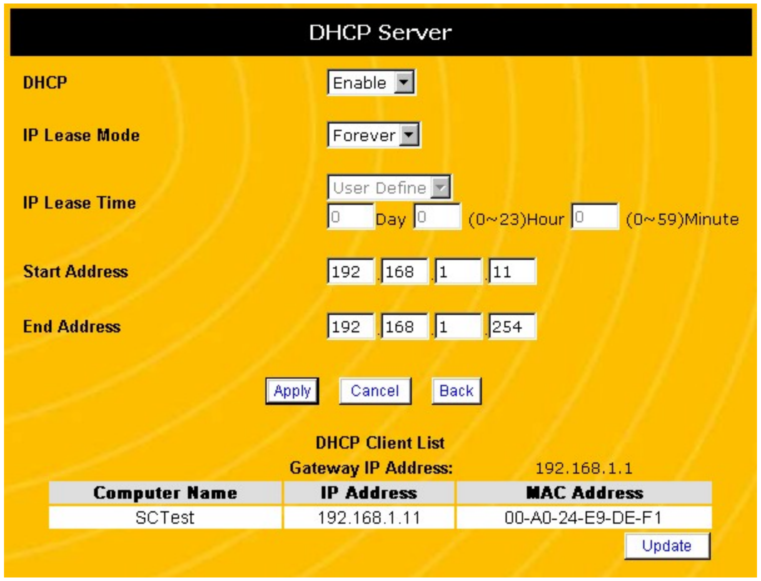
- If you want more control over which IP addresses the router assigns and how long those addresses are valid.
- If you are adding the router to a network that already has a DHCP server.

**NOTE: Incorrect DHCP settings can cause PCs to lose connection with the router. If your PCs connect to the router and the Internet or if you're note sure whether you need to change your DHCP settings, you probably don't need to change them.**

### CHANGING THE DHCP SERVER SETTINGS

Follow the procedure below to change what IP addresses are available to the DHCP server and how long the addresses are valid:

1. Open a browser window and login to the router.
2. Click **Basic Configuration**, then **DHCP Server**. This displays the **DHCP Server** screen (see Figure 24).



DHCP Server

DHCP: Enable

IP Lease Mode: Forever

IP Lease Time: User Define
0 Day 0 (0~23)Hour 0 (0~59)Minute

Start Address: 192 .168 .1 .11

End Address: 192 .168 .1 .254

DHCP Client List

Gateway IP Address: 192.168.1.1

| Computer Name | IP Address | MAC Address |
|---|---|---|
| SCTest | 192.168.1.11 | 00-A0-24-E9-DE-F1 |

**Figure 24 DHCP Server Screen**

3. Verify that the **DHCP** field is set to **Enable**.
4. Under the **IP Lease Mode** field, select **Forever** if you want IP addresses to always be valid. If you want addresses to be valid for only a short period of time, select **Expire.**
5. If you select **Expire** in the **IP Lease Mode** field, enter the length of time you want the IP addresses to remain valid. You can select a preset value from the list, or you can enter a number of days, hours, and minutes.
6. Under the **Start Address** field, enter the first IP address you want the router to be able to assign. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

7. Under the **End Address** field, enter the last IP address you want the router to be able to assign. The router will assign any IP address that falls into this range.

**NOTE: The Start and End Addresses should be in the same subnet as the LAN IP address. If the LAN IP Address were 192.168.1.1 and the subnet mask were 255.255.255.0 then the first three parts of the Start and End IP addresses would need to be 192.168.1.**

8. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, you must use the reboot command. See Rebooting the Router on page 77.**

### DISABLING THE DHCP SERVER

Follow the procedure below to disable the router's DHCP server function:

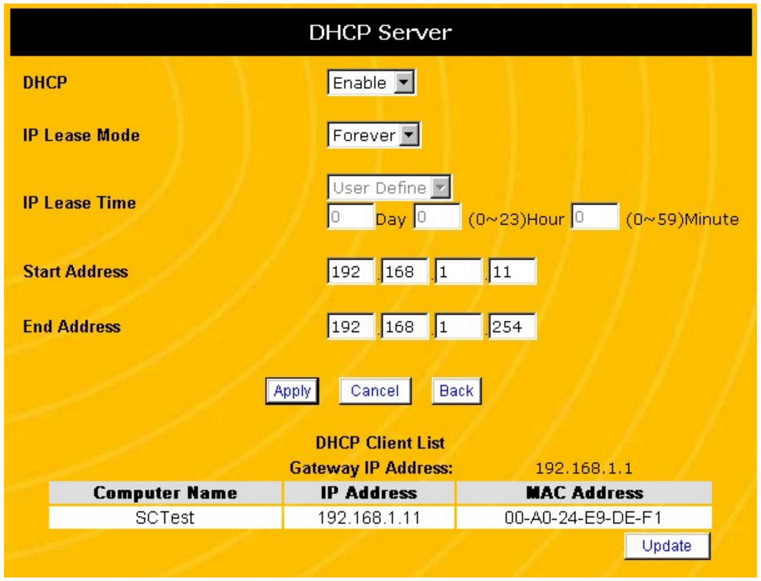
**NOTE: Do not disable the DHCP server unless there is another DHCP server on this network or you are prepared to give a static IP address to each computer accessing it.**

1. Open a browser window and login to the router.
2. At the **System Information** screen (see Figure 2 on page 24), record the MAC address of the router. The router's MAC address is listed under the LAN status information.

3. At the PC that serves as your network's DHCP server, reserve a fixed IP address for the router. Record this IP address along with the network subnet mask.

4. Open a browser window and login to the router.

5. Click **Basic Configuration**, then **DHCP Server**. This displays the **DHCP Server** screen (see Figure 24).



DHCP Server

DHCP: Enable

IP Lease Mode: Forever

IP Lease Time: User Define
0 Day 0 (0~23)Hour 0 (0~59)Minute

Start Address: 192 . 168 . 1 . 11

End Address: 192 . 168 . 1 . 254

DHCP Client List

Gateway IP Address: 192.168.1.1

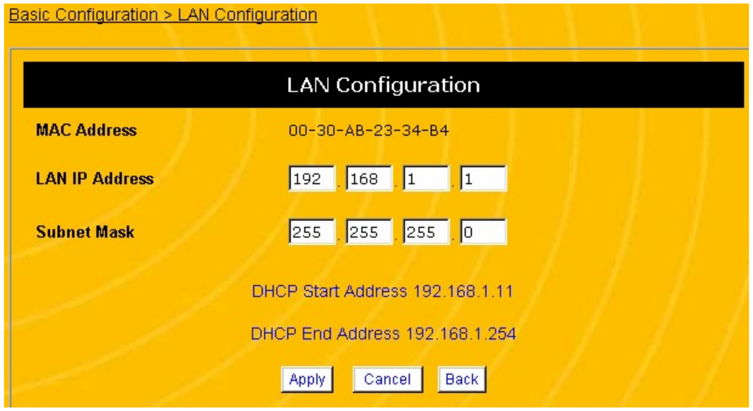
| Computer Name | IP Address | MAC Address |
|---|---|---|
| SCTest | 192.168.1.11 | 00-A0-24-E9-DE-F1 |

**Figure 25 DHCP Server Screen**

6. Set the **DHCP** field to **Disable**.

7. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **Cancel**. We will reboot the router after all the changes are made.

8. Click **Basic Configuration**, then **LAN**. This displays the **LAN Configuration** screen (see Figure 24).



Basic Configuration > LAN Configuration

LAN Configuration

MAC Address: 00-30-AB-23-34-B4

LAN IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

DHCP Start Address 192.168.1.11

DHCP End Address 192.168.1.254

**Figure 26 LAN Configuration Screen**

9. Under the **LAN IP Address** field, enter the IP address you reserved for the router. Enter the four separate parts of the IP address into the four separate boxes in the field.

10. Under the **Subnet Mask** field, enter the subnet mask the router should use. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

11. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it, use the reboot command. See Rebooting the Router on page 77.**

**NOTE: If you cannot communicate with the router after it reboots, verify that the first three parts of your PC's IP address match the router's IP address and that**

**both the PC and the router are using the same subnet mask.**

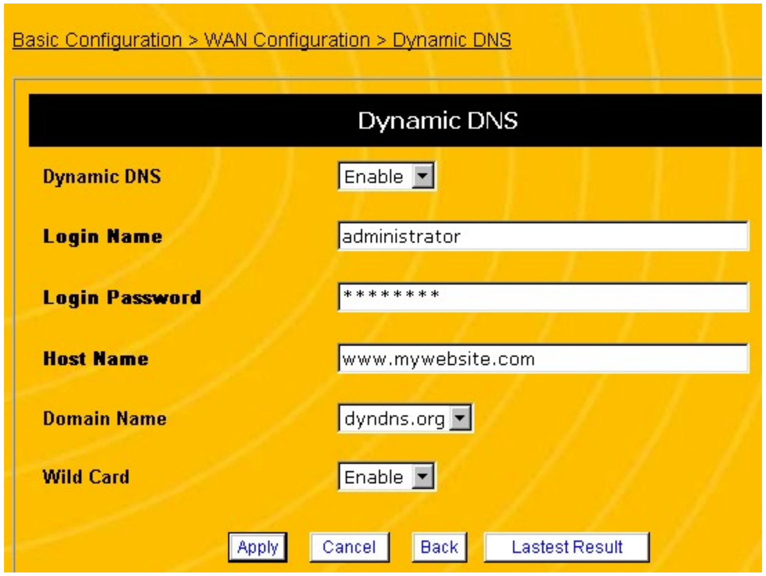
## ENABLING DYNAMIC DNS

A Domain Name System (DNS) server maintains a list of Internet addresses and URLs (web addresses) and the IP address of the computer that maintains the website. Usually, the IP address for the host computer must be static. A *dynamic DNS* service provides an alias for host computer that have dynamic IP addresses.

You should enable the dynamic DNS feature if you have a dynamic IP address from you ISP and you want to maintain an Internet host on your network. Follow the steps below to enable dynamic DNS:

**NOTE: Before enabling the dynamic DNS feature, you must have an account with a dynamic DNS service provider.**

1. Open a browser window and login to the router.
2. In the menu at the left side of the screen, click **Basic Configuration**, then **WAN**, then **Dynamic DNS**. This displays the **Dynamic DNS** screen (see Figure 27)



Basic Configuration > WAN Configuration > Dynamic DNS

Dynamic DNS

| | |
|---|---|
| Dynamic DNS | Enable |
| Login Name | administrator |
| Login Password | ******** |
| Host Name | www.mywebsite.com |
| Domain Name | dyndns.org |
| Wild Card | Enable |

**Figure 27 Dynamic DNS Screen**

3. In the **Dynamic DNS** Field, select **Enable**.
4. Enter the **Login Name** and **Login Password** for your dynamic DNS account.
5. Enter the host name of the domain. This is the URL that users will enter to connect to your website.
6. Select the **Domain Name** of you dynamic DNS provider.
7. Under the **Wild Card** field, select **Enable** to allow wild card lookups of your host name.
8. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, you must use the reboot command. See Rebooting the Router on page 77.**

## EDITING THE ROUTING TABLE

To provide Internet access, the router must be able to contact all the PCs on your network. If all the PCs on your network are directly attached to the router, the router always knows where they are. However, if a PC is attached to the router through an intermediary device (such as another router or another PC), the router cannot find it. These intermediate devices are called a *gateway*, because they serve a gate between the router and the remote PC.

The *routing table* tells the router which gateway devices these remote PCs or networks are connected to. Maintaining the routing table lets the router know which gateway device to send a data packet to reach a remote PC. You may have to edit the routing table if the following conditions apply:

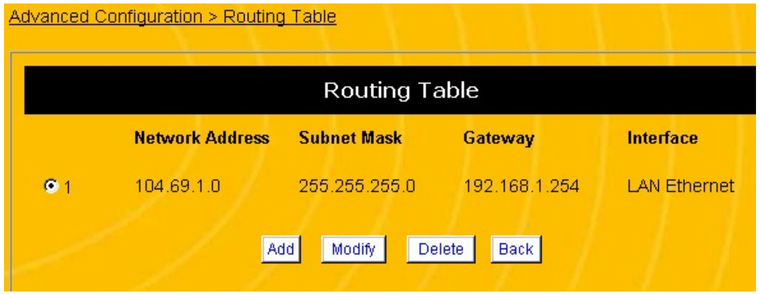
- You have more than one router on your network
- You want to divide your network into smaller “virtual networks” or *subnetworks*

To edit the routing table, you will need the following information:

- The IP address for each remote PC, remote network or subnetwork.
- The subnet mask for each remote PC, remote network or subnetwork.
- The IP address of the gateway device. The gateway is a router or computer connecting one network to another.

Follow the steps below to edit the routing table:

1. Open a browser window and login to the router.
2. Click **Advanced Configuration**, then **Routing Table**. This displays the **Routing Table** screen (see Figure 28).



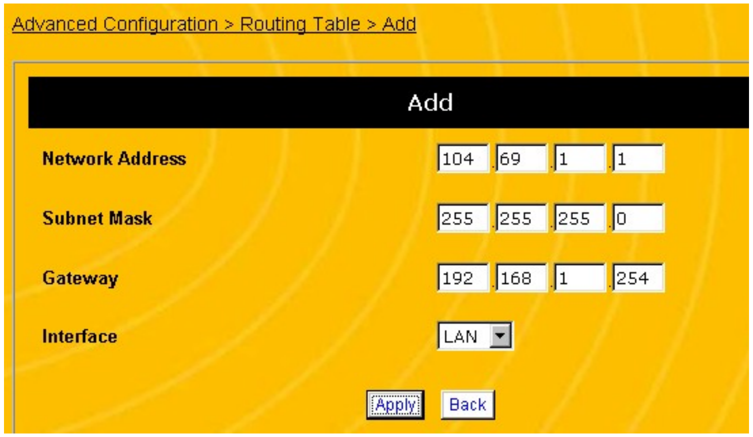
Advanced Configuration > Routing Table

Routing Table

| | Network Address | Subnet Mask | Gateway | Interface |
|---|---|---|---|---|
| ● 1 | 104.69.1.0 | 255.255.255.0 | 192.168.1.254 | LAN Ethernet |

**Figure 28 Routing Table Screen**

3. When you first view this screen, the table will be blank. Click the **Add** button to add a routing entry to the table. This displays the **Routing Table, Add** screen (see Figure 29).



Advanced Configuration > Routing Table > Add

Add

| | |
|---|---|
| Network Address | 104 . 69 . 1 . 1 |
| Subnet Mask | 255 . 255 . 255 . 0 |
| Gateway | 192 . 168 . 1 . 254 |
| Interface | LAN |

**Figure 29 Routing Table, Add Screen**

4. Under the **Network Address** field, enter the IP address of the remote PC or network you want to configure a route for. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

5. Under the **Subnet Mask** field, enter a subnet mask for the remote PC you entered above. If you are providing the route for a specific PC then the subnet mask of the PC should be 255.255.255.255. Otherwise a subnet mask indicating the size of the network should be used. Be sure to enter the four separate parts of the subnet mask into the four separate boxes in the field.

6. Under the **Gateway** field, enter the IP address of the intermediary device that stands between this router and the remote PC. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

7. Under the **Interface** field, select whether the *gateway* is attached to the router's **WAN** port or one of the **LAN** ports. If the WNR2004 is connected to the Internet then it should not need a route to the WAN so LAN should almost always be set. If the Router is being used to create a subnetwork then the WAN may be more commonly used.

8. Click **Apply**. This will take you back to the **Routing Table** screen.

9. To change the routing for a PC, select the PC's IP address on the **Routing Table** screen (see Figure 28 on page 66) and click the **Modify** button.

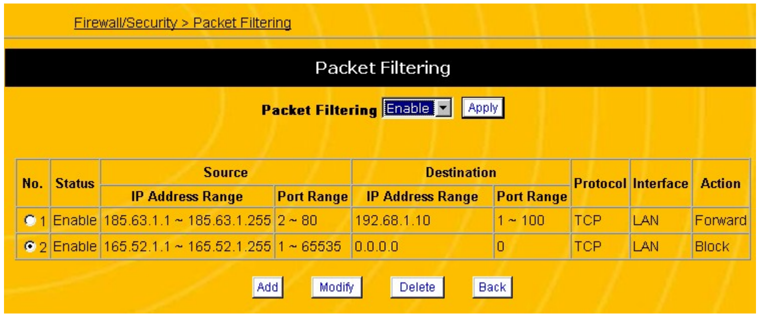
10. To delete the routing table entry for a PC, select the PC's IP address on the **Routing Table** screen (see Figure 28 on page 66) and click the **Delete** button.

## CONFIGURING PACKET FILTERING

Packet filtering allows you to route or block data based on information in each individual data packet. For example, if you want to allow only email from a particular server and block all other traffic, you can configure the router to allow only those packets that come in on the mail protocol ports (see Table 2 on page 51 for a few of the most commonly needed well-known ports). Follow the steps below to configure packet filtering:

1. Open a browser window and login to the router.

2. In the menu at the left side of the screen, click **Firewall Security** and then **Packet Filtering**. This displays the **Packet Filtering** screen (see Figure 30).



Firewall/Security > Packet Filtering

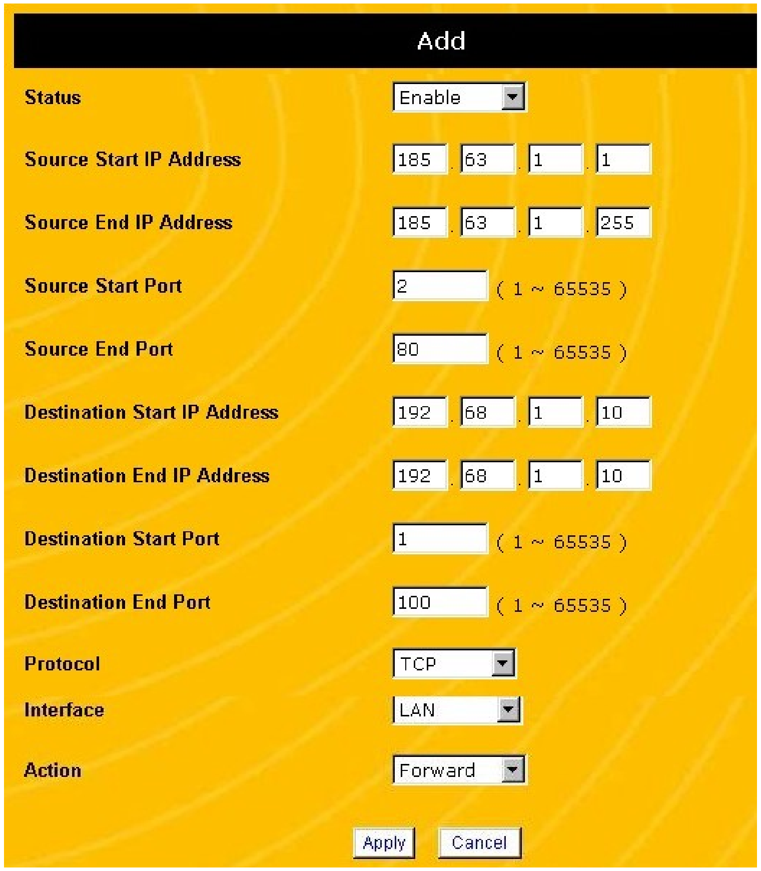
Packet Filtering

Packet Filtering Enable ▼ Apply

| No. | Status | Source | | Destination | | Protocol | Interface | Action |
|---|---|---|---|---|---|---|---|---|
| | | IP Address Range | Port Range | IP Address Range | Port Range | | | |
| ○ 1 | Enable | 185.63.1.1 ~ 185.63.1.255 | 2 ~ 80 | 192.68.1.10 | 1 ~ 100 | TCP | LAN | Forward |
| ● 2 | Enable | 165.52.1.1 ~ 165.52.1.255 | 1 ~ 65535 | 0.0.0.0 | 0 | TCP | LAN | Block |

**Figure 30 Packet Filtering Screen**

3. When you first view this screen, the table will be blank. Click the **Add** button to add a packet filtering entry to the table. This displays the **Packet Filtering, Add** screen (see Figure 31).



Add

| | |
|---|---|
| Status | Enable ▼ |
| Source Start IP Address | 185 . 63 . 1 . 1 |
| Source End IP Address | 185 . 63 . 1 . 255 |
| Source Start Port | 2 ( 1 ~ 65535 ) |
| Source End Port | 80 ( 1 ~ 65535 ) |
| Destination Start IP Address | 192 . 68 . 1 . 10 |
| Destination End IP Address | 192 . 68 . 1 . 10 |
| Destination Start Port | 1 ( 1 ~ 65535 ) |
| Destination End Port | 100 ( 1 ~ 65535 ) |
| Protocol | TCP ▼ |
| Interface | LAN ▼ |
| Action | Forward ▼ |

**Figure 31 Packet Filtering, Add Screen**

4. Under the **Status** field, click **Enable**.
5. In the **Source Start IP Address** field, enter the first IP address of the range of addresses you want to filter packets

*from*. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

6. In the **Source End IP Address** field, enter the last IP address of the range of you want to filter packets *from*. If you want to filter from a single IP address, enter the same IP address as the **Start IP Address**. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

**NOTE: IP addresses entered in these fields are consecutive. If you need to filter packets from non-consecutive IP addresses, enter the IP addresses as two or more different ranges.**

7. In the **Source Start Port** field, enter the first port of the range you want to filter packets *from*. (See Table 2 on page 51 for a few of the most commonly needed well-known ports.)
8. In the **Source End Port** field, enter the last port of the range you want to filter packets *from*. To filter packets from a single port, enter the same port number in the **Start** and **End** fields.

**NOTE: Port ranges are consecutive. If you need to filter packets from non-consecutive ports, enter the ports addresses as two or more different ranges.**

9. If you want to forward packets, in the **Destination Start IP Address** field, enter the first IP address of the range of addresses you want to send packets *to*. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.
10. In the **Destination End IP Address** field, enter the last IP address of the range of you want to send packets *to*. If you want to send packets to a single IP address, enter the same

IP address as the **Start IP Address**. Be sure to enter the four separate parts of the IP address into the four separate boxes in the field.

**NOTE: IP addresses entered in these fields are consecutive. If you need to send packets to non-consecutive IP addresses, enter the IP addresses as two or more different ranges.**

11. In the **Destination Start Port** field, enter the first port of the range you want to send packets to. (See Table 2 on page 51 for a few of the most commonly needed well-known ports.)
12. In the **Destination End Port** field, enter the last port of the range you want to send packets to. To send packets to a single port, enter the same port number in the **Start** and **End** fields.

**NOTE: Port ranges are consecutive. If you need to send packets to non-consecutive ports, enter the ports addresses as two or more different ranges.**

13. In the **Protocol** field, select **TCP**, **UDP**, **TCP/UDP**, or **ICMP** according to the needs of your network.
14. Under the **Interface** field, select whether the *destination IP address* is attached to the router's **WAN** port or one of the **LAN** ports.
15. Under the **Action** field, select **Forward** to send the packets to a destination IP address or select **Block** to restrict the data packets from entering your network.

**NOTE: If you select *Forward*, you must enter a destination IP address.**

16. Click **Apply**. This will take you back to the **Packet Filtering** screen (see Figure 30 on page 69).

17. To change the packet filtering settings, select the IP address range on the **Packet Filtering** screen (see Figure 30 on page 69) and click the **Modify** button.

18. To delete the packet filtering settings, select the IP address range on the **Packet Filtering** screen (see Figure 30 on page 69) and click the **Delete** button.

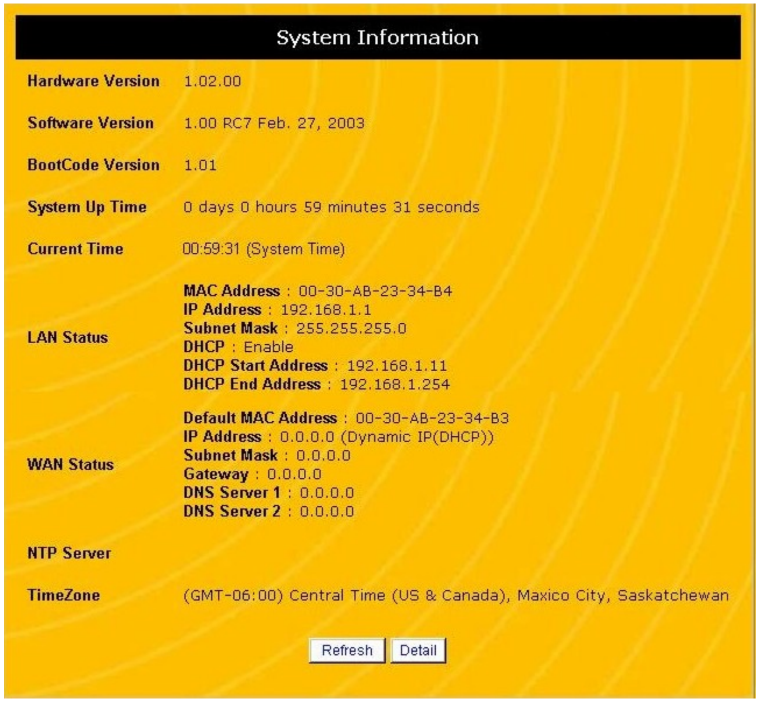
19. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, you must use the reboot command. See Rebooting the Router on page 77.**

# Router Maintenance Features

## SYSTEM INFORMATION SCREEN

The System Information screen provides a quick snapshot of the router's status and configuration. Whenever you login to the router, the System Information screen displays first.



System Information

| | |
|---|---|
| **Hardware Version** | 1.02.00 |
| **Software Version** | 1.00 RC7 Feb. 27, 2003 |
| **BootCode Version** | 1.01 |
| **System Up Time** | 0 days 0 hours 59 minutes 31 seconds |
| **Current Time** | 00:59:31 (System Time) |
| **LAN Status** | **MAC Address** : 00-30-AB-23-34-B4<br>**IP Address** : 192.168.1.1<br>**Subnet Mask** : 255.255.255.0<br>**DHCP** : Enable<br>**DHCP Start Address** : 192.168.1.11<br>**DHCP End Address** : 192.168.1.254 |
| **WAN Status** | **Default MAC Address** : 00-30-AB-23-34-B3<br>**IP Address** : 0.0.0.0 (Dynamic IP(DHCP))<br>**Subnet Mask** : 0.0.0.0<br>**Gateway** : 0.0.0.0<br>**DNS Server 1** : 0.0.0.0<br>**DNS Server 2** : 0.0.0.0 |
| **NTP Server** | |
| **TimeZone** | (GMT-06:00) Central Time (US & Canada), Maxico City, Saskatchewan |

**Figure 32 System Information Screen**

The System Information screen shows the following information:

## HARDWARE, SOFTWARE, AND BOOTCODE VERSION

This information defines the version of your router. Record this information in case you have to contact customer support.

## SYSTEM UP TIME

This field displays how long the router has been operating since it was last rebooted.

## CURRENT TIME (SYSTEM TIME)

If Network Time Protocol or *NTP* is disabled, this field resets to zero when the router is rebooted. If NTP is enabled, this field displays the current time.

## LAN STATUS

**MAC Address** This field displays the MAC address the router uses to communicate with PCs attached locally.

**IP Address** This field displays the IP address the router uses to communicate with PCs attached locally. The default IP address is 192.168.1.1.

**Subnet Mask** This field displays the subnet mask address the router uses to communicate with PCs attached locally. The default subnet mask is 255.255.255.0.

**DHCP** This field shows whether the router’s DHCP server is enabled or disabled.

**DHCP Start Address** This field displays the first IP address (the start of the range) available to the the DHCP server.

**DHCP End Address** This field displays the last IP address (the endt of the range) available to the the DHCP server.

## WAN STATUS

**Default MAC Address** This field displays the MAC address the router uses to communicate with the ISP.

**IP Address** This field displays the IP address the router uses to communicate with the ISP. It also indicates whether the router is obtaining an IP address automatically from the ISP.

**Subnet Mask** This field displays the subnet mask the router uses to communicate with the ISP.

**Gateway** This field displays the IP address of the ISPs gateway.

**DNS Server 1** This field displays the IP address of the primary Domain Name System server the rotuer uses to lookup URLs.

**DNS Server 2** This field displays the IP address of the secondary Domain Name System server the rotuer uses to lookup URLs.

## NTP SERVER

If the Network Time Protocol (*NTP*) is enabled, this field will display the domain name or URL of the NTP server the router is using to update its system clock.

## TIME ZONE

This field displays the selected time zone the router is using to maintain its system clock.

## REFRESH

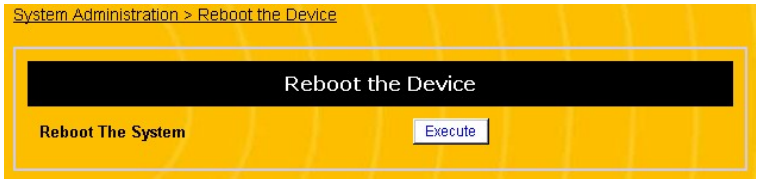
Click the **Refresh** button to update the **System Information** screen.

## REBOOTING THE ROUTER

Whenever you have changed the router's configuration, you must reboot the router before the changes take effect. If the router does not prompt you to reboot it at the end of the last configuration step, you must use the reboot command.

### SOFTWARE REBOOT

1. From the menu at the left of the screen, click on **System Administration**, then **Reboot the Device**. This displays the **Reboot the Device** screen (Figure 33).



System Administration > Reboot the Device

Reboot the Device

Reboot The System

**Figure 33 Reboot the Device Screen**

2. Click **Execute**. When the router displays a dialogue box that says "*Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

### HARDWARE REBOOT

If you cannot access the configuration screens, you will need to reboot the router through the hardware. There are two different methods to reboot the router from the hardware:

**Method 1:** Power the router off and back on again.

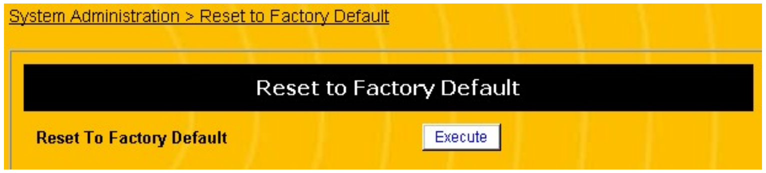
**Method 2:** Use a pencil or pin to press the reset button at the rear of the router. Release the button immediately.

## RESETTING THE ROUTER TO FACTORY DEFAULTS

Use this feature whenever you want to clear any changes you have made to the router and reset the configuration back to it's factory defaults. If a configuration causes problems with the router, resetting it to the factory defaults may be the only way to correct the problem. Also, if you are selling the router, you should reset it to factory defaults to protect your internal network information.

### RESTORING FACTORY DEFAULTS WITH THE SOFTWARE

1. From the menu at the left of the screen, click on **System Administration**, then **Reset to Factory Defaults**. This displays the **Reset to Factory Defaults** screen (Figure 34).



System Administration > Reset to Factory Default

Reset to Factory Default

Reset To Factory Default

**Figure 34 Reset to Factory Defaults Screen**

2. Click **Execute**. When the router displays a dialogue box that says "*Do you really want to reset to factory default?*" click **OK**. This will reboot the router and reload the original configuration settings, erasing any and all changes.
3. After you reset the router to its factory default configuration, you must login to the router using the factory default IP address and password. (See Logging In on page 22.)

### RESTORING FACTORY DEFAULTS WITH THE HARDWARE

If you cannot access the configuration screens, you will need to reset the factory defaults through the hardware. Use a pencil or pin to press the reset button at the rear of the router. Hold the reset button in for 10 seconds, then release it.

After you reset the router to its factory default configuration, you must login to the router using the factory default IP address and password. (See Logging In on page 22.)

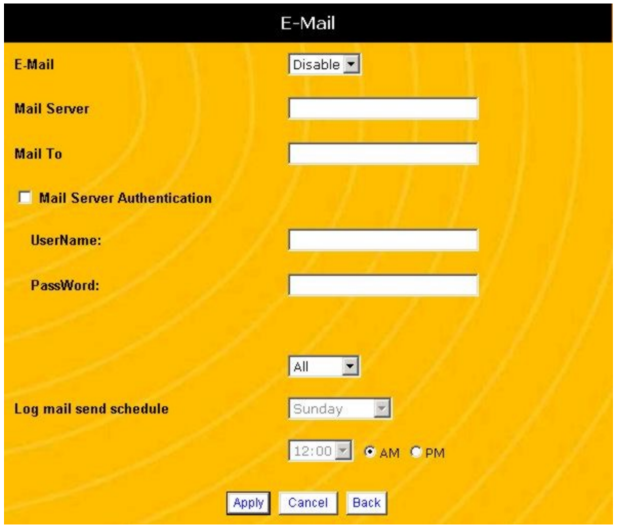
## SYSTEM LOGS

The system logs track access to the router, communication with the ISP, and errors. The system log is most useful for troubleshooting the router.

### AUTOMATICALLY EMAILING SYSTEM LOGS

You can configure the router to email a copy of its system log to a computer automatically.

1. Open a browser window and login to the router.
2. In the menu at the left side of the screen, click **System Administration**, then **Log/Report**, then **Email**. This opens the **Email Logs** screen (see Figure 35).



E-Mail

E-Mail: Disable

Mail Server:

Mail To:

☐ Mail Server Authentication

UserName:

PassWord:

All

Log mail send schedule: Sunday

12:00 ● AM ○ PM

**Figure 35 Email Logs Screen**

3. In the **Email** field, select **Enable**.
4. In the **Mail Server** field, enter the name of the mail server the router should send the log to. The mail server name will usually have the following format:

```
mail.uniden.com
```

5. In the **Mail To** field, enter name of the user or email account the router should send the log to.
6. If this account requires authentication to receive external email, click **Mail Server Authentication**, then enter the **User Name** and **Password**.
7. If you select the **Daily** log, select what time the router should send the log each day.

8. If you select the **Weekly** log, select what day each week and what time on that day the router should send the log.

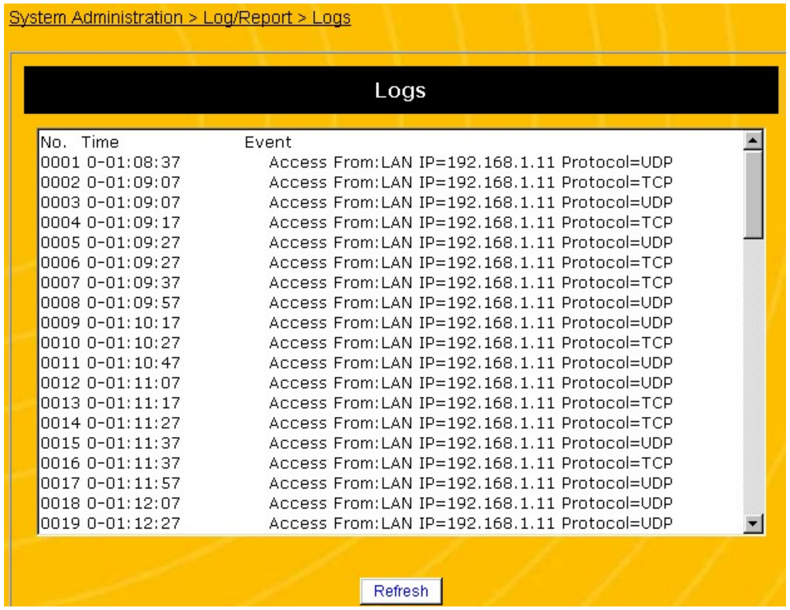
9. Click **Apply**. If the router displays a dialogue box that says "*Values are saved. Do you really want to reboot the system now?*" click **OK**. This will reboot the router and apply all configuration changes.

**NOTE: If the router does not prompt you to reboot it at the end of the last configuration step, you must use the reboot command. See Rebooting the Router on page 77.**

## READING SYSTEM LOGS

1. Open a browser window and login to the router.

2. In the menu at the left side of the screen, click **System Administration**, then **Log/Report**, then **Logs**. This opens the **Logs** screen (see Figure 36).



```
No.  Time           Event
0001 0-01:08:37       Access From:LAN IP=192.168.1.11 Protocol=UDP
0002 0-01:09:07       Access From:LAN IP=192.168.1.11 Protocol=TCP
0003 0-01:09:07       Access From:LAN IP=192.168.1.11 Protocol=UDP
0004 0-01:09:17       Access From:LAN IP=192.168.1.11 Protocol=TCP
0005 0-01:09:27       Access From:LAN IP=192.168.1.11 Protocol=UDP
0006 0-01:09:27       Access From:LAN IP=192.168.1.11 Protocol=TCP
0007 0-01:09:37       Access From:LAN IP=192.168.1.11 Protocol=TCP
0008 0-01:09:57       Access From:LAN IP=192.168.1.11 Protocol=UDP
0009 0-01:10:17       Access From:LAN IP=192.168.1.11 Protocol=UDP
0010 0-01:10:27       Access From:LAN IP=192.168.1.11 Protocol=TCP
0011 0-01:10:47       Access From:LAN IP=192.168.1.11 Protocol=UDP
0012 0-01:11:07       Access From:LAN IP=192.168.1.11 Protocol=UDP
0013 0-01:11:17       Access From:LAN IP=192.168.1.11 Protocol=TCP
0014 0-01:11:27       Access From:LAN IP=192.168.1.11 Protocol=TCP
0015 0-01:11:37       Access From:LAN IP=192.168.1.11 Protocol=UDP
0016 0-01:11:37       Access From:LAN IP=192.168.1.11 Protocol=TCP
0017 0-01:11:57       Access From:LAN IP=192.168.1.11 Protocol=UDP
0018 0-01:12:07       Access From:LAN IP=192.168.1.11 Protocol=UDP
0019 0-01:12:27       Access From:LAN IP=192.168.1.11 Protocol=UDP
```

**Figure 36 Logs Screen**

This screen displays the following information:

**No.** This field displays a sequentially assigned number for each log event.

**Time** This field displays time at which the event was logged. This time is based on the Current Time/System Time field on the **System Information** screen.

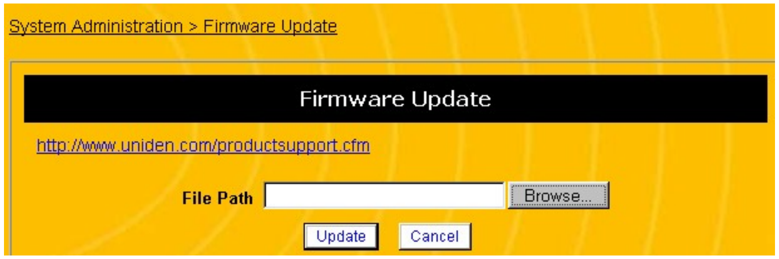
**Event** This field displays a description of the event. Some examples of events are a PC accessing the router, the router receiving an error from the ISP or any PC, an unauthroized IP or MAC address trying to access the router, a PC logging into the router, a PC logging into the network, etc.

## UPDATING THE FIRMWARE

Follow the steps below to upgrade the firmware on your router.

**NOTE: Updating the firmware may erase some or all of your configuration changes. Be sure to record any configuration changes you have made before updating the router's firmware.**

1. Open a browser window and login to the router.
2. In the menu at the left side of the screen, click **System Administration**, then **Firmware Update**. This opens the **Firmware Update** screen (see Figure 37).



System Administration > Firmware Update

Firmware Update

http://www.uniden.com/productsupport.cfm

**Figure 37 Firmware Update Screen**

3. Click the website hyperlink at the top of the screen to go to the Uniden product support page.
4. Search for the correct router firmware update by clicking on the hypertext on the **Firmware Update** screen and searching for your model number (WNR2004)
5. Download the firmware update file to you PC.
6. At the **Firmware Update** screen, click the **Browse** button and find the firmware update file on your PC.
7. Click the **Update** button to update the firmware.

# Wireless Configuration

The **WNR2004 802.11b Access Point/Router** is configured to work with other 802.11b wireless products directly out of the box. There is no need for you to configure your Access Point, unless you want to enable increased security (WEP), or other configuration options (see Figure 38).

If you want to change the default configurations, you will need to access the browser-based utility of the WNR2004 AP and select the **Wireless Configuration** from the menu on the left hand side.

**Note: If you are having trouble communicating with your Access Point, please see "Trouble Shooting" on page 90.**

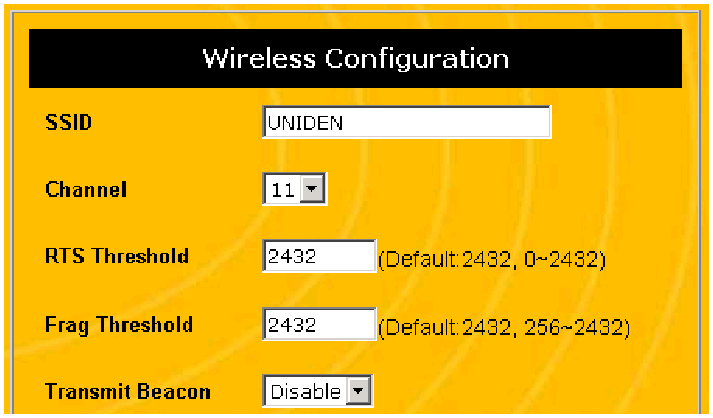
Set each of the parameters on this page as desired, and click Apply. The parameters are described in more detail below

## SSID

The Service Set Identifier (SSID) is a 32-character, case-sensitive field that identifies your **WNR2004 Wireless AP/Router** and wireless network to wireless clients that support the IEEE 802.11b wireless standard. You should use a unique SSID to control access to your private network, and to prevent conflicts with other wireless networks that may be nearby. The **WNR2004 Wireless AP/Router** is configured with a default SSID of **UNIDEN** (see Figure 38).

**Note: All clients on the same wireless LAN must have the same SSID. If you change the SSID on the WNR2004 Wireless AP/Router, you must change the SSID for each computer and/or device you are**

**wanting to connect using the 802.11b wireless network.**



Wireless Configuration

SSID: UNIDEN

Channel: 11

RTS Threshold: 2432 (Default:2432, 0~2432)

Frag Threshold: 2432 (Default:2432, 256~2432)

Transmit Beacon: Disable

Figure 38 Wireless Configuration Screen

## CHANNEL

Channels are the spectrum range where your wireless signals are transmitted. The default is channel 1. However, to maximize performance for your wireless network, another channel may give you better performance. Select the channel you wish to use (channel 1 through 11) from the pull-down menu.

**Note: For better performance, avoid using channels occupied by other AP's in the area.**

## RTS THRESHOLD

RTS (Request to Send) Threshold is the packet size by which the router will judge whether to activate the RTS mechanism. When RTS is activated control packets are used by the access point to regulate the traffic giving the various connected clients Clear To Send (CTS) messages before data can be transmitted from a client. RTS is used to avoid collisions.

The default value is 2432, which is quite large so that RTS is not activating in most cases. When RTS is activated, overall performance decreases due to the associated overhead incorporated into the packets. In most network environments, RTS is not necessary.

## FRAG THRESHOLD

Fragmentation Threshold is the size at which packets are divided into smaller packets to be transmitted on an 802.11 wireless LAN. This fragmentation is done to improve performance when transmitting large files over the wireless network. The fragmentation threshold is determined on a station-by-station basis.

## TRANSMIT BEACON

For security you can choose to disable the broadcasting beacon signal identifying your access point.

## WEP ENCRYPTION

To make your network more secure, you may choose to use Wired Equivalent Privacy (WEP). WEP is an encryption scheme used to protect your wireless data communications. WEP uses a combination of 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. The **WNR2004 Wireless AP/Router** supports both 64-bit WEP and 128-bit WEP. To connect all computers with a Wireless LAN using WEP, each AP and client in the network must use an identical 64-bit or 128-bit WEP key. In simple terms, a 128-bit key will give you a more secure network than a 64-bit key.

**Note: Some products refer to 64-bit encryption as 40-bit encryption. Both are names for the same encryption technology.**

**802.11b clients inserted into your laptop or desktop computer must have the same WEP settings as the AP in order for them to communicate with each other.**

## WEP KEY CONFIGURATION

WEP keys can automatically be created by using a Pass Phrase or generated Manually.

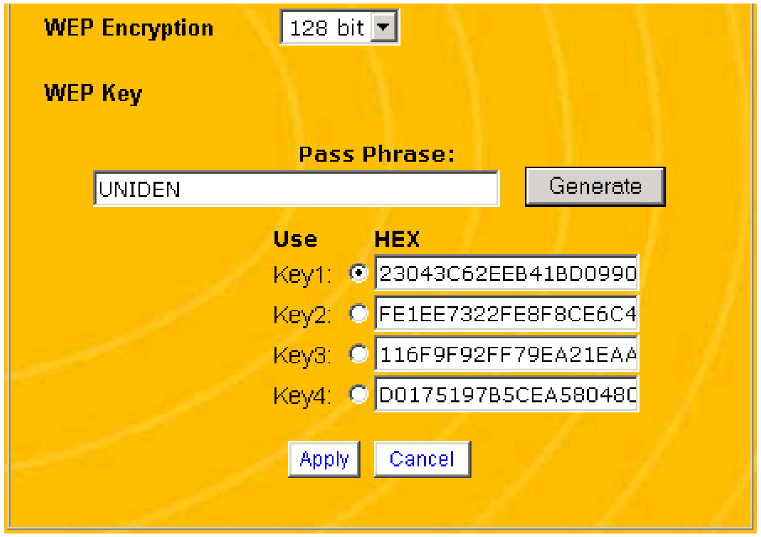
### PASS PHRASE METHOD

When you enter a pass phrase, the **WNR2004 AP/Router** generates four WEP keys for you. You can generate those same WEP keys on any wireless client whose configuration utility supports pass phrases. To setup WEP using a pass phrase, perform the following steps.

1. Select either **64-bit** or **128-bit WEP** encryption from the pull-down menu.
2. Type a pass phrase of up to 31 alphanumeric characters into the **Pass Phrase** field and click Generate to create the hex key(s).
3. Select the active WEP key set (1, 2, 3, or 4) for 64-bit encryption. WEP 128-bit encryption creates only one key. Verify that you are using the same active key for all clients on your wireless network. (If a client does not support pass phrases, you may manually enter the desired key on that client.)

4. Click Apply. Remember that changes do not take effect until after you **Reboot** your **WNR2004 Wireless AP/Router**. See Rebooting the Router on page 77.

A sample WEP configuration using a pass phrase is shown in the following figure.



WEP Encryption: 128 bit

WEP Key

Pass Phrase: UNIDEN

| Use | | HEX |
|---|---|---|
| Key1: | ● | 23043C62EEB41BD0990 |
| Key2: | ○ | FE1EE7322FE8F8CE6C4 |
| Key3: | ○ | 116F9F92FF79EA21EAA |
| Key4: | ○ | D0175197B5CEA58048C |

**Figure 39 WEP Configuration Screen**

MANUAL KEY ENTRY

To manually enter the WEP keys, perform the following steps:

1. Select either **64-bit** or **128-bit** WEP encryption from the pull-down menu.

2. When **WEP 64-bit** is selected, type 5 alpha characters in the range of “A-Z” (e.g. MyKey) in the WEP Key 1 entry field. Alternatively, you may enter 10 digit hexadecimal values in the range of “A-F” and “0-9”.

   You can also enter WEP keys in the Key 2, Key 3 and Key 4 if you wish. Select the active WEP key set (1, 2, 3, or 4) for 64-bit encryption.

   128- bit WEP encryption consists of 26 hexadecimal characters and 13 alpha characters. Verify that you are using the same active key for all clients on your wireless network.

3. Click **Apply**. Remember that changes do not take effect until after you **Reboot** your **WNR2004 Wireless AP/Router.** See Rebooting the Router on page 77.

# Trouble Shooting

This section provides a brief troubleshooting guide for common problems. If this guide does not solve your problem, see our support website at www.uniden.com/productsupport.cfm or contact customer support at 1 (800) 775-9060

## POWER LED DOES NOT TURN ON

1. Make sure the power adapter is properly connected to your router.
2. Check that you are using the 7.5V DC power adapter supplied with the router.
3. Test the outlet the router is connected to, or move the power connection to another outlet.

If all connections are fine but the router still does not power on, contact technical support.

## TEST LED STAYS ON

When you reboot the router, the Test LED comes on while the router undergoes its power-on-self test. The LED should go out when the router completes its self-test. If the Test LED does not go out, cycle the power on the router. If the Test LED still does not go out, contact technical support.

## TEST LED DOES NOT COME ON

When you reboot the router, the Test LED comes on while the router undergoes its power-on-self test. The LED should go out when the router completes its self-test. If the Test LED does not come on during a reboot, cycle the power on the router. If the Test LED still does not come on, contact technical support.

## A SINGLE PC CANNOT CONNECT TO THE ROUTER OR THE INTERNET

Follow these steps if a single PC on the network cannot connect to the router or to the Internet:

1. Check the Ethernet connection between your computer and the router. Verify that the PC is connected to one of the four LAN ports on the router.
2. Verify that the IP address of the PC is in the correct network range. Open a DOS command window and type **ipconfig**; this will make the PC display its IP address.
3. If the PC displays an incorrect IP address or does not display an IP address, you'll need to re-configure the PC's IP address (see Step 2: PC Configuration on page 16).
4. Check the router's **Basic Configuration, DHCP Server** screen to verify that the settings are correct. If DHCP is disabled, try enabling it.
5. Check the router's **Firewall/Security, Parental Control** screen to see if that PC has been restricted
6. Check the router to verify that the Link light for the port connected to the PC is turned on.
7. Check the PC's network interface card to verify that the Link light is turned on.
8. Attempt to login to the router from the problem PC.
9. If you cannot login to the router, attempt to PING the PC. Open a DOS command window and type the following command (assuming the router IP address is 192.168.1.1):

```
ping 192.168.1.1
```

10. If you do not receive any replies from the PING command, the PC is not communicating with the router. Contact customer support.

## NO PCS CAN CONNECT TO THE INTERNET

NOTE: **If you have previously connected to the Internet and suddenly cannot, it is most likely a problem with your ISP. Contact your ISP's technical support.**

Follow these steps if you have not yet successfully connected to the Internet:

1. Verify that PCs connected through the router can communicate with each other. If they can't, follow the troubleshooting steps in A Single PC Cannot Connect to The Router or the Internet on page 91
2. Verify that the cable or DSL modem is connected to the WAN port on the router.
3. Check the router to verify that the Link light for the WAN port is turned on. If it is not, try plugging a PC into the WAN port; if the Link light comes on, the port is functioning properly. Plug your cable/DSL modem back into the port.
4. Check the cable/DSL modem to verify that its Link light is turned on. If the Link light on the cable/DSL modem is not turned on, consult the owner's manual for the cable/DSL modem.
5. Check the router's **Firewall/Security, Parental Control** screen to see if any PCs have been restricted
6. Verify that the router is properly configured to interact with your ISP. See Step 3: Basic Router Configuration on page

21 and Advanced Router Configuration on page 38 for details on configuring the router to connect to your ISP.

7. If the configuration seems correct, contact your ISP to verify the settings needed to connect to their network.
8. If the configuration settings you have match those of your ISP, there may be an incorrect configuration setting on some other screen. Reset your router to factory defaults, and start the configuration again.
9. If you are using PPPoE or Dynamic IP to connect to your ISP, you can check the status of the connection from the **Basic Configuration, WAN, PPPoE** or the **Basic Configuration, WAN, Dynamic IP (DHCP)** screen. Click the **Status** button at the bottom of these screens to check the status of the connection.
10. If you still cannot connect to you ISP, contact customer support for your ISP.

## Specifications

| | |
|---|---|
| Model No | WNR2004 |
| Standards | IEEE 802.3i, IEEE 802.3U, IEEE 802.3x, IEEE 802.11b |
| Network and Routing Protocols | Static and Dynamic Routing with TCP/IP, DHCP, PPPoE, DNS, NAT, TFTP, HTTP, IPSec, L2TP, PPTP |
| WAN Port | 1 RJ-45 connector |
| LAN Ports | 4 RJ-45 UTP connectors |
| Wireless Network Speeds | Auto-fallback 11, 5.5, 2 and 1 Mbps |
| Wireless Encryption | WEP 64-bit<br>WEP 128-bit |
| Wireless Range | Up to 150 m (500 ft.) indoors and 500 m (1650 ft.) outdoors |
| LED Indicators | 1 Power<br>1 Test<br>1 WAN (Link/Activity/Speed)<br>4 LAN (Link/Activity/Speed)<br>1 Wireless (Link/Activity) |
| Power | External 7.5V DC |
| Operating Temperature | $32^o$ - $104^o$ F ($0^o$ – $40^o$ C) |
| Storage Temperature | $-4^o$ – $158^o$ F ($-20^o$ – $70^o$ C) |

# Legal Notice

**Statement of Conditions**

Uniden reserves the right to make changes to the products described in this document without notice.

Uniden does not assume any liability due to the user or application of the product(s) or circuit layout(s) described herein.

## IC NOTICE:

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

## FCC INFORMATION

FEDERAL COMMUNICATIONS COMMISSION (FCC) COMPLIANCE NOTICE: RADIO FREQUENCY NOTICE

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

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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

will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: (1) Reorient or relocate the receiving antenna, (2) Increase the separation between the equipment and 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.

FEDERAL COMMUNICATIONS COMMISSION (FCC) RADIATION EXPOSURE STATEMENT

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

THE FCC WANTS YOU TO KNOW

Changes or modifications to this product not expressly approved by Uniden, or operation of this product in any way other than as detailed by the owner's manual, could void your authority to operate this product and will void any warranty.

# Precautions!

Before you read anything else, please observe the following:

**Warning!**

> **Uniden America Corporation DOES NOT represent this unit to be waterproof. To reduce the risk of fire, electrical shock, or damage to the unit, DO NOT expose this unit to rain or moisture.**

## IMPORTANT SAFETY INSTRUCTION

When using your product, these basic safety precautions should always be followed to reduce the risk of fire, electrical shock, and injury to persons:

1. Read and understand all instructions.
2. Follow all warnings and instructions marked on the product.
3. Do not use this product near water; for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
4. Do not place this product on an unstable cart, stand, or table. The product may fall, causing serious damage to the unit.
5. Slots and openings in the cabinet and the back or bottom are provided for ventilation. To protect the product from overheating, these openings must not be blocked or covered. This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
6. If this product includes a cable, do not allow anything to rest on it and do not locate this product where the cable will be damaged by persons walking on it.

7. Do not overload wall outlets and extension cords, as this can result in the risk of fire or electrical shock.
8. Never push objects of any kind into this product through cabinet slots, as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.
9. To reduce the risk of electric shock, do not disassemble this product. Take it to qualified service personnel when service or repair work is required. Opening or removing covers may expose you to dangerous voltages or other risks. Incorrect reassembly can cause electric shock when the appliance is subsequently used.
10. Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:

    A. If liquid has been spilled into the product.

    B. If the product has been exposed to rain or water.

    C. If the product does not operate normally when following the operating instructions. (Adjust only those controls that are covered by the operating instructions. Improper adjustment of other controls may result in damage and will often require extensive repair work by a qualified technician.)

    D. If the product has been dropped or the cabinet has been damaged.

    E. If the product exhibits a distinct change in performance.

IMPORTANT ELECTRICAL CONSIDERATIONS

Unplug all electrical appliances when you know an electrical storm is approaching. Lightning can pass through your household wiring and damage any device connected to it. This product is no exception.

**Warning!**

**Please do not attempt to unplug any appliance during an electrical storm.**

## One Year Limited Warranty

**Important: Evidence of original purchase is required for warranty service.**

WARRANTOR: UNIDEN AMERICA CORPORATION (“UNIDEN”)

ELEMENTS OF WARRANTY: Uniden warrants, for one year, to the original retail owner, this Uniden Product to be free from defects in materials and craftsmanship with only the limitations or exclusions set out below.

WARRANTY DURATION: This warranty to the original user shall terminate and be of no further effect twelve (12) months after the date of original retail sale. The warranty is invalid if the Product is (A) damaged or not maintained as reasonable or necessary, (B) modified, altered, or used as part of any conversion kits, subassemblies, or any configurations not sold by Uniden, (C) improperly installed, (D) serviced or repaired by someone other than an authorized Uniden service center for a defect or malfunction covered by this warranty, (E) used in any conjunction with equipment or parts or as part of any system not manufactured by Uniden, or (F) installed or programmed by anyone other than as detailed by the owner’s manual for this product.

STATEMENT OF REMEDY: In the event that the product does not conform to this warranty at any time while this warranty is in effect, warrantor will either, at its option, repair or replace the defective unit and return it to you without charge for parts, service, or any other cost (except shipping and handling) incurred by warrantor or its representatives in connection with the performance of this warranty. Warrantor, at its option, may replace the unit with a new or refurbished unit. THE LIMITED WARRANTY SET FORTH ABOVE IS THE SOLE AND ENTIRE

WARRANTY PERTAINING TO THE PRODUCT AND IS IN LIEU OF AND EXCLUDES ALL OTHER WARRANTIES OF ANY NATURE WHATSOEVER, WHETHER EXPRESS, IMPLIED OR ARISING BY OPERATION OF LAW, INCLUDING, BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS WARRANTY DOES NOT COVER OR PROVIDE FOR THE REIMBURSEMENT OR PAYMENT OF INCIDENTAL OR CONSEQUENTIAL DAMAGES. Some states do not allow this exclusion or limitation of incidental or consequential damages so the above limitation or exclusion may not apply to you.

LEGAL REMEDIES: This warranty gives you specific legal rights, and you may also have other rights which vary from state to state. This warranty is void outside the United States of America.

PROCEDURE FOR OBTAINING PERFORMANCE OF WARRANTY: If, after following the instructions in the owner's manual you are certain that the Product is defective, pack the Product carefully (preferably in its original packaging). The Product should include all parts and accessories originally packaged with the Product. Include evidence of original purchase and a note describing the defect that has caused you to return it. The Product should be shipped freight prepaid, by traceable means, to warrantor at:

Uniden America Corporation
Parts and Service Division
4700 Amon Carter Blvd
Fort Worth, TX 76155
(800) 775-9060

## Glossary

**Ad.Hoc -** Ad.Hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for an access point.

**Adapter -** A printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card (NIC) is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

**Backbone -** The part of a network that connects most of the systems and networks together and handles the most data.

**Bandwidth -** The transmission capacity of a given facility, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps).

**Bit -** A binary digit. The value 0 or 1 used in the binary numbering system. Also, the smallest form of data.

**Boot -** To cause the computer to start executing instructions. Personal computers contain built-in instructions in ROM chip that are automatically executed on startup. These instructions search for the operating system, load it, and pass control to it.

**Bridge** - A device that interconnects different networks together.

**Broadband -** A data-transmission scheme in which multiple signals share the bandwidth of a single medium. This allows the transmission of voice, data, and video signals over that medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

**Browser** - An application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

**Cable Modem** – A device that connects a computer to the cable television network, which in turn connects to the Internet. Once connected, cable modem users have a continuous connection to the Internet. Cable modems feature asymmetric transfer rates: around 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

**Data Packet** - One frame in a packet-switched message. Most data communication is based on dividing the transmitted message into packets.
For example, an Ethernet packet can be from 64 to 1518 bytes in length.

**Default Gateway** - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

**DHCP** (Dynamic Host Configuration Protocol) - A protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

**DNS** - The Domain Name System (DNS) is the way that Internet domain names are located and translated into an Internet Protocol (IP) address. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

**Domain** - A sub network comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

**Download** - To receive a file transmitted over a network. In a communications session, download means receive, and upload means transmit.

**Driver** - A software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific adapter, and is installed during the setup of the adapter.

**DSSS** (Direct-Sequence Spread-Spectrum) - DSSS generates a redundant bit pattern for each bit transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

**Dynamic DNS** (Domain Name System) – A system for keeping a domain name linked to a changing IP address. A dynamic DNS Service Provider maintains a database of the updated IP addresses linked to a domain name.

**Dynamic IP Address** - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

**Dynamic Routing** - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

**Ethernet** - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

**Fast Ethernet** - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

**Firewall** – A firewall is a set of related programs, located at a network gateway server, which protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access. A firewall, working closely with a router, examines

**Firmware** - Programming that is inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

**Flash Memory** - Flash memory is an electronic storage device capable of recording several megabytes of data files.

**Fragmentation** - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

**Hardware** - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the “box” and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

**Hub** - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

**IEEE** (Institute of Electrical and Electronics Engineers) - The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and has several large societies in special areas, such as the IEEE Computer Society.

**IEEE 802.11** - Industry standard that enables wireless LAN hardware from different manufacturers to communicate.

**Infrastructure Mode** - A mode of operation of the 802.11b wireless protocol that allows all computers on a wired and wireless network to share a peripheral, such as a printer or high speed Internet Access.

**IP Address** - In the most widely installed level of the Internet Protocol (IP) today, and IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

**IPCONFIG** – A utility that provides for querying, defining and managing IP addresses within a network. This utility is commonly used under Windows NT and 2000, for configuring networks with a static IP address.

**IPSec** (Internet Protocol Security) - A developing standard for security at the network or packet-processing layer of network communication. A big advantage of IPSec is that security arrangements can be handled without requiring changes to individual user computers.

**IRQ** (Interrupt Request) – A hardware interrupt on a PC. There are 16 IRQ lines used to signal the CPU that a peripheral event has started or terminated. Except for PCI devices, two devices cannot use the same line.

**ISP** (Internet Service Provider) - A company that provides individuals and companies access to the Internet and other related services such as website building and virtual hosting.

**LAN** (Local Area Network) – A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

**Latency** - The time delay between when the first bit of a packet is received and the last bit is forwarded.

**Link Quality** - The quality of data being received.

**MAC Address** (Media Access Control Address) - A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

**Mbps** (Megabits per Second) – One million bits per second; a unit of measurement of the speed of data transmission.

**NAT** (Network Address Translation) – The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

**Network** - A system that transmits any combination of voice, video, and/or data between users.

**NIC** (Network Interface Card) – A board installed in a computer system, usually a PC, to provide network communication capabilities to and from that computer system. Also called an adapter.

**NTP** (Network Time Protocol) **-** is a protocol used to synchronize computer clock times in a network of computers.

**Packet Filtering -** Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).

**PCI** (Peripheral Component Interconnect) – A peripheral bus commonly used in PCs, Macintoshes and workstations. It was designed primarily by Intel and first appeared on PCs in late 1993. PCI provides a high-speed data path between the CPU and peripheral devices (video, disk, network, etc.). There are typically three of four PCI slots on the motherboard. In a Pentium PC, there is generally a mix of PCI and ISA slots or PCI and EISA slots. Early on, the PCI bus was known as a “local bus.” PCI allows IRQs to be shared, which helps to solve the problem of limited IRQs available on a PC. For example, if there were only one IRQ left over after ISA devices were given their required IRQs, all PCI devices could share it. In a PCI-only machine, there cannot be insufficient IRQs, as all can be shared.

**PCMCIA -** The PCMCIA (Personal Computer Memory Card International Association) is an industry group organized in 1989 to promote standards for a credit card-size memory or I/O device that would fit into a personal computer, usually a notebook or laptop computer.

**Peer-to-Peer Networking** – Allows users to share local resources between PCs without needing an access point or router.

**Ping** (Packet Internet Groper) – An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

**Plug-and-Play** – The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

**Port** – A pathway into and out of the computer of a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems, and printers.

**PPPoE** (Point to Point Protocol over Ethernet) – A method used mostly by DSL providers for connecting personal computers to a broadband modem for Internet access. It is similar to how a dial-up connection works but at higher

**PPTP** (Point-to-Point Tunneling Protocol) – A protocol (set of communication rules) that allows corporations to extend their own corporate network through private “tunnels” over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

**Print Server** - A hardware device that enables a printer to be located anywhere in the network.

**RIP** (Routing Information Protocol) – A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers and is known to waste bandwidth. AppleTalk, DECnet, TCP/IP, NetWare, and VINES all use incompatible versions of RIP.

**RJ-11** (Registered Jack-11) – A telephone connector that holds up to six wires. The RJ-11 is the common connector used to plug a telephone into a wall.

**RJ-45** - A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

**Router** - Protocol-dependent device that connects sub networks together. Routers are useful in breaking down a very large network into smaller sub networks; they introduce longer delays and typically have much lower throughput rates than bridges.

**Routing Table** – Is a user defined list of steps stating how to process various incoming traffic.

**Server** - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

**Signal Strength** – The amount of electromagnetic energy is present. A receiver (such as the one in your access point determines the strength of the signal for each wireless channel.

**Software** – Instructions for the computer. A series of instructions that performs a particular task is called a “program.” The two major categories of software are “system software” and “application software.” System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user. A common misconception is that software is data. It is not, software tells the hardware how to process the data.

**SOHO** (Small Office/Home Office) – Market segment of professionals who work at home or in small offices.

**Static IP Address** - A permanent IP address that is assigned to a node in a TCP/IP network.

**SPI** (Stateful Packet Inspection) – Maintains a log of sessions and requests for each application and determines if the conditions between the client and the application are “normal”. If a request appears unrelated to the current application session, the request is denied.

**Static Routing** - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

**Subnet Mask** - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to form part of the host ID address field into a field for subnets.

**Switch** – 1. A data switch connects computing devices to host computers, allowing a large number of devices to share a limited number of ports.
2. A device for making, breaking, or changing the connections in an electrical circuit.

**TCP** (Transmission Control Protocol) – A method (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP keeps track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

**TCP/IP** (Transmission Control Protocol/Internet Protocol) - The basic communication language or protocol of the Internet. It can also be used as a communication protocol in a private network (either an intranet or an extranet). When you are set up with access to the Internet, your computer is uses the TCP/IP protocol.

**TFTP** (Trivial File Transfer Protocol) – A version of the TCP/IP FTP protocol that has no directory or password capability.

**Throughput** - The amount of data moved successfully from one place to another in a given time period.

**Topology** - A network's topology is a logical characterization of how the devices on the network are connected and the distances between them. The most common network devices include hubs, switches, routers, and gateways.

Most large networks contain several levels of interconnection, the most important of which include edge connections, backbone connections, and wide-area connections.

**UDP** (User Datagram Protocol) – A communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP.

**Upgrade** – To replace existing software of firmware with a newer version.

**Upload** – To send a file transmitted over a network. In a communications session, upload means transmit, and download means receive.

**URL** (Uniform Resource Locator) – The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

**VLAN** (Virtual LAN) – A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

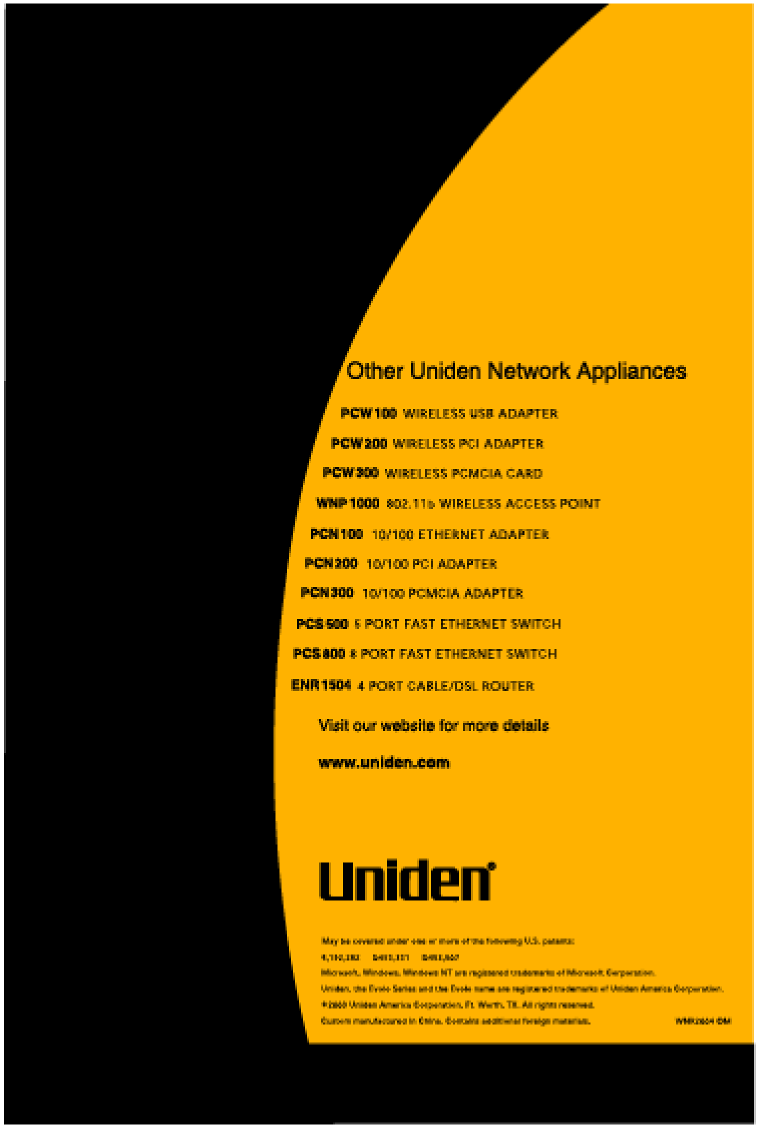
**WAN** (Wide-Area Network) - A communications network that covers a wide geographic area, such as a state or country.

**WEP** (Wired Equivalent Privacy) – A data privacy mechanism based on 64-bit and 128-bit shared key algorithms, as described in the IEEE802.11 standard.

**WINIPCFG** - Configuration utility based on the Win32 API for querying, defining, and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

**Workgroup** - Two or more individuals that share files and databases.

## MEMO



Other Uniden Network Appliances

| | |
|---|---|
| PCW 100 | WIRELESS USB ADAPTER |
| PCW 200 | WIRELESS PCI ADAPTER |
| PCW 300 | WIRELESS PCMCIA CARD |
| WNP 1000 | 802.11b WIRELESS ACCESS POINT |
| PCN 100 | 10/100 ETHERNET ADAPTER |
| PCN 200 | 10/100 PCI ADAPTER |
| PCN 300 | 10/100 PCMCIA ADAPTER |
| PCS 500 | 5 PORT FAST ETHERNET SWITCH |
| PCS 800 | 8 PORT FAST ETHERNET SWITCH |
| ENR 1504 | 4 PORT CABLE/DSL ROUTER |

Visit our website for more details

www.uniden.com

Uniden®

WNR2004 OM