



LevelOne

WBR-3407

11g Wireless ADSL Modem Router

User's Manual

Table of Contents

CHAPTER 1 INTRODUCTION	1
WBR-3407 Features	1
Package Contents	3
Physical Details	4
CHAPTER 2 INSTALLATION.....	6
Requirements.....	6
Procedure	6
CHAPTER 3 SETUP	8
Overview	8
Configuration Program	9
WAN Setup Wizard	10
Home Screen	12
Mode Screen.....	13
LAN Screen.....	14
Wireless Screen.....	16
Password Screen.....	21
CHAPTER 4 PC CONFIGURATION	22
Overview	22
Windows Clients.....	22
Macintosh Clients.....	34
Linux Clients.....	34
Other Unix Systems.....	34
Wireless Station Configuration.....	35
Using WPA-802.1x - Overview.....	36
802.1x Server Setup (Windows 2000 Server).....	37
802.1x Client Setup on Windows XP	47
CHAPTER 5 OPERATION AND STATUS	53
Operation	53
Status Screen.....	53
Connection Status - PPPoE & PPPoA	55
Connection Details - Dynamic IP Address	56
Connection Details - Fixed IP Address.....	57
CHAPTER 6 ADVANCED FEATURES	58
Overview	58
Internet.....	58
Dynamic DNS (Domain Name Server)	60
Firewall Rules	62
Firewall Services.....	67
Options	69
Schedule.....	70
Virtual Servers.....	71
CHAPTER 7 ADVANCED ADMINISTRATION	73
Overview	73
PC Database.....	74
Config File.....	78
Logging.....	79
E-mail	81

Diagnostics	83
Remote Admin	84
Routing	86
Upgrade Firmware	90
APPENDIX A TROUBLESHOOTING	91
Overview	91
General Problems	91
Internet Access	91
Wireless Access	92
APPENDIX B ABOUT WIRELESS LANS	93
Modes	93
BSS/ESS	93
Channels	94
WEP	94
Wireless LAN Configuration	94
APPENDIX C SPECIFICATIONS	95
Multi-Function WBR-3407	95
Wireless Interface	95
Regulatory Approvals	96

Chapter 1

Introduction

1

This Chapter provides an overview of the WBR-3407's features and capabilities.

Congratulations on the purchase of your new WBR-3407. The WBR-3407 is a multi-function device providing the following services:

- **ADSL Modem.**
- **Shared Broadband Internet Access** for all LAN users.
- **WBR3407** for 802.11b and 802.11g Wireless Stations.
- **4-Port Switching Hub** for 10BaseT or 100BaseT connections.

Wireless LAN

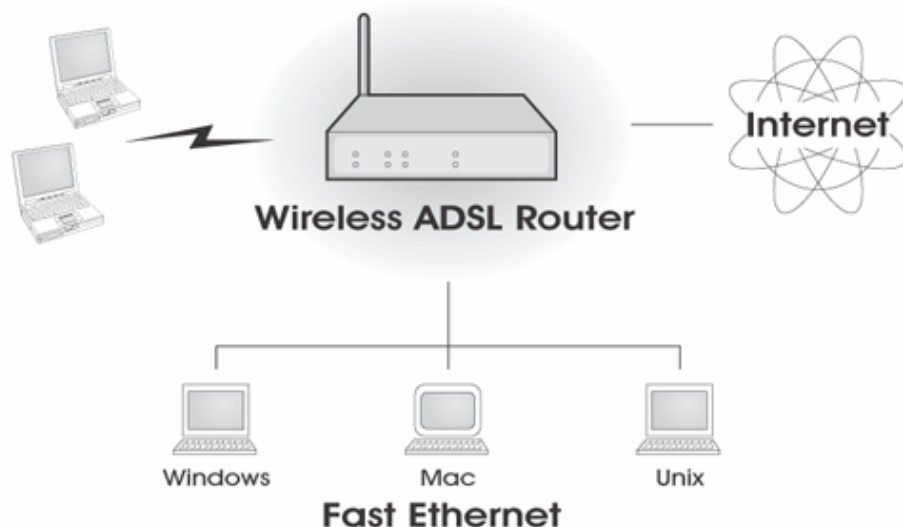


Figure 1: WBR-3407

WBR-3407 Features

The WBR-3407 incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the WBR-3407, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- **Built-in ADSL Modem.** The WBR-3407 has a built-in ADSL modem, supporting all common ADSL connections.
- **IPoA, PPPoE, PPPoA, Direct Connection Support.** The WBR-3407 supports all common connection methods.

- ***Auto-detection of Internet Connection Method.*** In most situations, the WBR-3407 can test your ADSL and Internet connection to determine the connection method used by your ISP.
- ***Fixed or Dynamic IP Address.*** On the Internet (WAN port) connection, the WBR-3407 supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- ***Application Level Gateways (ALGs).*** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users.
- ***Logs.*** Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.
- ***Firewall.*** As well as the built-in firewall to protect your LAN, you can define Firewall Rules to determine which incoming and outgoing traffic should be permitted.
- ***Dynamic DNS Support.*** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- ***VPN Pass through Support.*** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

Wireless Features

- ***Standards Compliant.*** The WBR-3407 complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- ***Supports both 802.11b and 802.11g Wireless Stations.*** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- ***Speeds to 54Mbps.*** All speeds up to the 802.11g maximum of 54Mbps are supported.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- ***WPA-PSK support.*** Support for the WPA-PSK is included. This version of WPA does not require a Radius Server on your LAN.
- ***WPA-802.1x support.*** Support for the WPA-PSK is included. This version of WPA requires a Radius Server on your LAN.
- ***Wireless MAC Access Control.*** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.

LAN Features

- ***4-Port Switching Hub.*** The WBR-3407 incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.

- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The WBR-3407 can act as a **DHCP Server** for devices on your local LAN and WLAN.

Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- **Configuration File Upload/Download.** Save (download) the configuration data from the WBR-3407 to your PC, and restore (upload) a previously-saved configuration file to the WBR-3407.
- **Remote Management.** The WBR-3407 can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- **Network Diagnostics.** You can use the WBR-3407 to perform a *Ping* or *DNS lookup*.

Security Features

- **Password - protected Configuration.** Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **Wireless LAN Security.** WEP (Wired Equivalent Privacy) is supported, as well as Wireless access control to prevent unknown wireless stations from accessing your LAN.
- **NAT Protection.** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the WBR-3407.
- **Firewall.** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Protection against DoS attacks.** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The WBR-3407 incorporates protection against DoS attacks.

Package Contents

The following items should be included:

- The WBR-3407 Unit
- 1 Cat-5 Ethernet (LAN) cable
- 1 RJ-11 (ADSL) cable
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front-mounted LEDs



Figure 2: Front Panel

- Power LED (Green)** **On** - Power on.
Off - No power.
- Status LED (Yellow)** **Off** - Normal operation.
Blinking - This LED blinks during start up, and during a Firmware Upgrade.
- LAN** For each port, there are 2 LEDs, to indicate the connection speed (10BaseT or 100BaseT) of each port.
- **100BT** - This will be ON if the LAN connection is using 100BaseT, and Blinking if data is being transferred via the corresponding LAN port.
 - **10BT** - This will be ON if the LAN connection is using 10BaseT, and Blinking if data is being transferred via the corresponding LAN port.
 - If neither LED is on, there is no active connection on the corresponding LAN port.
- WLAN LED** **On** – Wireless enabled.
Off - No Wireless connections currently exist.
Flashing - Data is being transmitted or received via the WBR3407. This includes "network traffic" as well as user data.
- WAN** **On** - ADSL connection is available.
Off - No ADSL connection.
Flashing - Data is being transmitted or received via the ADSL connection.

Rear Panel

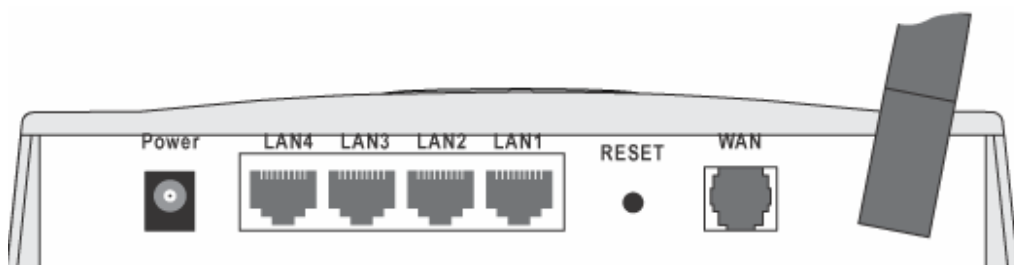


Figure 3: Rear Panel

Power port

Connect the supplied power adapter here.

**10/100BaseT
LAN connections**

Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.

Note:

Any LAN port on the WBR-3407 will automatically function as an "Uplink" port when required. Just connect any port to a normal port on the other hub, using a standard LAN cable.

**Reset Button
(Reset to Defaults)**

This button will reset the WBR-3407 to the factory default settings. To do this, press and hold the Reset Button for five (5) seconds, until the Status LED is lit, then release the Reset Button, and wait the WBR-3407 to restart using the factory default values.

**WAN port
(ADSL port)**

Connect this port to your ADSL line.

Chapter 2

Installation

2

This Chapter covers the physical installation of the WBR-3407.

Requirements

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and a DSL connection.
- To use the WBR3407, all Wireless devices must be compliant with the IEEE 802.11g or IEEE 802.11b specifications.

Procedure

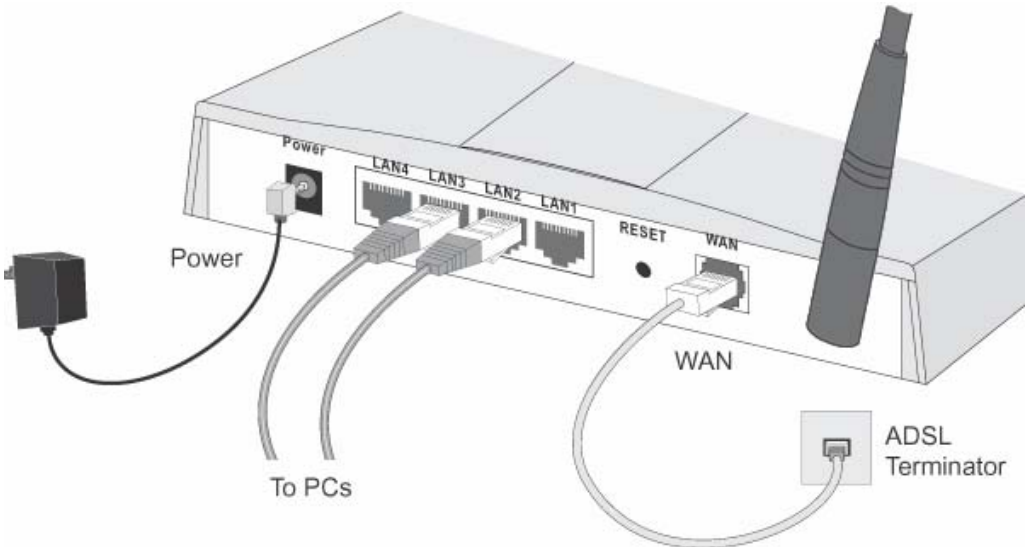


Figure 4: Installation Diagram

1. Choose an Installation Site

Select a suitable place on the network to install the WBR-3407.



For best Wireless reception and performance, the WBR-3407 should be positioned in a central location with minimum obstructions between the WBR-3407 and the PCs.

Also, if using multiple Access Points, adjacent Access Points should use different Channels.

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the Switching Hub ports on the WBR-3407. Both 10BaseT and 100BaseT connections can be used simultaneously.

If required, connect any port to a normal port on another Hub, using a standard LAN cable. Any LAN port on the WBR-3407 will automatically function as an "Uplink" port when required.

3. Connect ADSL Cable

Connect the supplied ADSL cable from to the WAN port on the WBR-3407 (the RJ11 connector) to the ADSL terminator provided by your phone company.

4. Power Up

Connect the supplied power adapter to the WBR-3407 and power up.

Use only the power adapter provided. Using a different one may cause hardware damage

5. Check the LEDs

- The *Power* LED should be ON.
- The *Status* LED should flash, then turn Off. If it stays on or blinking after 60 seconds, there is a hardware error.
- For each LAN (PC) connection, one of the LAN LEDs should be ON (provided the PC is also ON.)
- The *WLAN* LED should be ON
- The *WAN* LED should be ON if ADSL line is connected.

For more information, refer to *Front-mounted LEDs* in Chapter 1.

Chapter 3

Setup



This Chapter provides Setup details of the WBR-3407.

Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration
- Wireless setup
- Assigning a Password to protect the configuration data.

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the WBR-3407 you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4: PC Configuration
Check WBR-3407 operation and Status.	Chapter 5: Operation and Status
Use any of the following Advanced features: <ul style="list-style-type: none">• Internet• Dynamic DNS• Firewall Rules• Firewall Services• Schedule• Virtual Servers	Chapter 6: Advanced Features
Use any of the following Administration Configuration settings or features: <ul style="list-style-type: none">• PC Database• Config File• Logging• E-mail• Diagnostics• Remote Admin• Routing• Upgrade Firmware	Chapter 7 Advanced Administration

Configuration Program

The WBR-3407 contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript.**

The configuration program has been tested on the following browsers:

- Netscape V4.08 or later
- Netscape 7
- Internet Explorer V5.01 or later

Preparation

Before attempting to configure the WBR-3407, please ensure that:

- Your PC can establish a physical connection to the WBR-3407. The PC and the WBR-3407 must be directly connected (using the Hub ports on the WBR-3407) or on the same LAN segment.
- The WBR-3407 must be installed and powered ON.
- If the WBR-3407's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the WBR-3407 is allocated a new IP Address during configuration.

Using your Web Browser

To establish a connection from your PC to the WBR-3407:

1. After installing the WBR-3407 in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the WBR-3407, as in this example, which uses the WBR-3407's default IP Address:
`HTTP://192.168.0.1`
4. When prompted for the User name and Password, enter values as follows:
 - User name admin
 - Password password

If you can't connect

If the WBR-3407 does not respond, check the following:

- The WBR-3407 is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
 - Open the MS-DOS window or command prompt window.
 - Enter the command:

```
ping 192.168.0.1
```

If no response is received, either the connection is not working, or your PC's IP address is not compatible with the WBR-3407's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the WBR-3407's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the WBR-3407 are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

WAN Setup Wizard

The first time you connect to the WBR-3407, the WAN (Internet) Setup Wizard will run automatically. (The Setup Wizard will also run if the WBR-3407's default settings are restored.)

1. Step through the Wizard until finished.
 - You need the data supplied by your ISP. Most connection methods require some data input.
 - The common connection types are explained in the following table.
2. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
3. If the connection test fails:
 - Check all connections, and the front panel LEDs.
 - Check that you have entered all data correctly.

Common Connection Types

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) Some ISP's may require you to use a particular <i>Hostname</i> or <i>Domain</i> name, or MAC (physical) address.</p>
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you. Usually, the connection is "Always on".	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.</p>
PPPoE, PPPoA	You connect to the ISP only when required. The IP address is usually allocated automatically.	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) User name and password are always required.</p> <p>c) If using a Static (Fixed) IP address, you need the IP address and related information (Network Mask, Gateway IP address, and DNS address)</p>
IPoA (IP over ATM)	Normally, the connection is "Always on".	<p>a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically.</p> <p>b) IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.</p>

Home Screen

After finishing the Setup Wizard, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.



Figure 5: Home Screen

Main Menu

The main menu, on the left, contains links to the most-commonly used screen. To see the links to the other available screens, click "Advanced" or "Administration".

The main menu also contains two (2) buttons:

- **Log Out** - When finished, you should click this button to logout.
- **Restart** - Use this if you wish to restart the WBR-3407. Note that restarting the Router will break any existing connections to or through the Router.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your data will be ignored.



On each screen, clicking the "Help" button will display help for that screen.

Mode Screen

Use the *Mode* link on the main menu to reach the Mode screen. An example screen is shown below.

The screenshot shows a dark blue interface with the word "Mode" in large yellow letters at the top. Below it, the text "Device Mode" is followed by three configuration fields: "Device Name: WBR-3407A", "Device Mode: Modem (Modem only)", and "Language: English". At the bottom right, there are two buttons labeled "Save" and "Help".

Figure 6: LAN Screen

Data - Mode Screen

Device Mode	
Device Name	This field displays the current name of this device.
Device Mode	<p>Select the desired device mode for the router:</p> <ul style="list-style-type: none"> • Router - Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. • Modem - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. <p>Note:</p> <ul style="list-style-type: none"> • If the mode is changed, this device must restart when you save. • You will lose the connection until the restart is completed. • The menu will change when the mode is changed. Many features are only available in Router mode.
Language	Select the desired language for this user interface.

LAN Screen

Use the *LAN* link on the main menu to reach the LAN screen. An example screen is shown below.



Figure 7: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the WBR-3407, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the WBR-3407 is attached (the same value as the PCs on that LAN segment).
DHCP Server	<ul style="list-style-type: none"> • If Enabled, the WBR-3407 will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. • If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the WBR-3407 as the default Gateway. See the following section for further details. • The Start IP Address and Finish IP Address fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. <p>See the following section for further details on using DHCP.</p>

DHCP

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **Server** allocates a valid IP address to a DHCP **Client** (PC or device) upon request.

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- The WBR-3407 can act as a **DHCP server**.
- Windows 95/98/ME and other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the WBR-3407's DHCP Server

This is the default setting. The DHCP Server settings are on the **LAN** screen. On this screen, you can:

- Enable or Disable the WBR-3407's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.



You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the WBR-3407's, the following procedure is required.

1. Disable the DHCP Server feature in the WBR-3407. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the WBR-3407's IP Address as the *Default Gateway*.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP for all non-Server versions of Windows.

See *Chapter 4 - Client Configuration* for the procedure to check these settings.

Wireless Screen

The WBR-3407's settings must match the other Wireless stations.

Note that the WBR-3407 will automatically accept both 802.11b and 802.11g connections, and no configuration is required for this feature.

To change the WBR-3407's default settings for the WBR3407 feature, use the *Wireless* link on the main menu to reach the *Wireless* screen. An example screen is shown below.



Figure 8: Wireless Screen

Data - Wireless Screen

Identification	
Regulatory Domain	Select the correct domain for your location. It is your responsibility to ensure: <ul style="list-style-type: none"> • That the WBR-3407 is only used in domains for which is licensed. • That you select the correct domain, so that only the legal channels for that domain can be selected.
Station name	This is the same as the "Device Name" for the WBR-3407.
SSID (ESSID)	<ul style="list-style-type: none"> • If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). • To communicate, all Wireless stations should use the same SSID/ESSID.

Options	
Mode	<p>Select the desired mode:</p> <ul style="list-style-type: none"> • g & b - Both 802.11.g and 802.11b Wireless stations will be able to use the WBR-3407. • g only - Only 802.11g Wireless stations can use the WBR-3407. • b only - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the WBR-3407 if they are fully backward-compatible with the 802.11b standard.
Channel No.	<ul style="list-style-type: none"> • Select the Channel you wish to use on your Wireless LAN. • If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best. • If using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.
Broadcast SSID	<p>If enabled, the WBR-3407 will broadcast its SSID. This allows Wireless Stations will a "null" (blank) SSID to detect and use the correct SSID.</p> <p>Disable this feature if you do not want Wireless stations to be able to do this.</p>
Options	
Curent Setting	The curent setting is displayed. The default value is "Disabled" - no security.
Configure Button	Click this button to view the Wireless security sub-screen. See the following section for more details.
Access Point	
Enable Wireless Access Point	Enable this if you want to use WBR3407 function. If disabled, no Wireless stations can use the Access Point function, and all connections must be make via the wired LAN.
Allow access by ...	<p>Use this feature to determine which Wireless stations can use the Access Point. The options are:</p> <ul style="list-style-type: none"> • All Wireless Stations - All wireless stations can use the access point, provided they have the correct SSID and WEP settings. • Trusted Wireless stations only - Only wireless stations you designate as "Trusted" can use the access point, even if they have the correct SSID and WEP settings. This feature uses the MAC address to identify Wireless stations. The MAC address is a low-level network identifier which is unique to each PC or network device. To define the trusted wireless stations, use the "Set Stations" button.
Set Stations Button	Click this button to manage the trusted PC database.

Wireless Security

The Wireless Security sub-screen is accessed by the "Configure" button on the Wireless screen.

It provides 4 options for Wireless Security:

- **Disabled** - No security is used.
- **WEP** - Data is encrypted using the WEP standard.
- **WPA-PSK** - Data is encrypted using the WPA standard. Each Wireless station must have the same Pres-shared Key (PSK).
- **WPA-802.1x** - This system requires that a Radius Server be used for Authentication. Data is encrypted using WPA, but the keys are automatically generated, and do not need to be entered.

Wireless Security - WEP

If WEP is selected, the screen will look like the following:

Figure 9: WEP Screen

Data - WEP Screen

Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
Key Size	Select the option to match other Wireless Stations: <ul style="list-style-type: none"> • 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only.

	You must enter a Key Value for the Default Key .
Key Value	Enter the key value or values you wish to use. The Default Key is required, the other keys are optional. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

Wireless Security - WPA-PSK

If WPA-PSK is selected, the screen will look like the following:

Figure 10: WPA-PSK Screen

Data - WPA-PSK Screen

PSK	Also called the "Network Key". Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.
Key Lifetime	Enter the required time period.
Encryption	Select the desired option. Other Wireless Stations must use the same method.

Wireless Security - WPA-802.1x

If WPA-802.1x is selected, the screen will look like the following.

Note that to use 802.1x:

- You need a Radius Server.
- The Radius Server must have "Client" login for the WBR-3407, using its IP address and the the "Shared Key" set on this screen.
- Each client (user) must obtain a Certificate to authenticate against the Radius Server. See Chapter 4 - PC Configuration for details.

The screenshot shows a configuration window titled "Wireless Security". The "Security System" is set to "WPA-802.1x". The "Radius Server" field is empty, with the label "(Name or IP address)" next to it. The "Radius Port" field contains the value "1812". The "Shared Key" field is empty. There are four buttons at the bottom: "Save", "Cancel", "Help", and "Close".

Figure 11: WPA-802.1x Screen

Data - WPA-802.1x Screen

Radius Server Address	Enter the name or IP address of the Radius Server on your network.
Radius Port	Enter the port number used for connections to the Radius Server.
Shared Key	This is used for the <i>Client Login</i> on the Radius Server. Enter the key value to match the Radius Server.

Note: The Encryption method used is TKIP.

Password Screen

The password screen allows you to assign a password to the WBR-3407.



Figure 12: Password Screen

Old Password	Enter the existing password in this field.
New password	Enter the new password here.
Verify password	Re-enter the new password here.

You will be prompted for the password when you connect, as shown below.

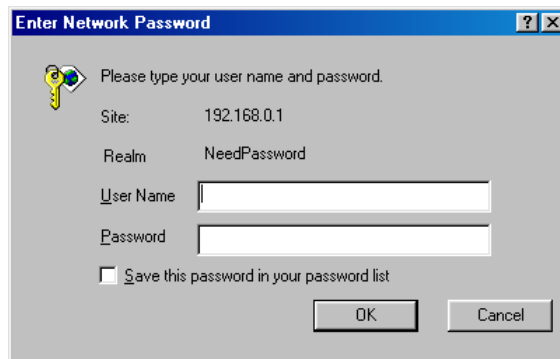


Figure 13: Password Dialog

- The "User Name" is always `admin`
- Enter the password for the WBR-3407, as set on the *Password* screen above.

Chapter 4

PC Configuration



This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

Windows Clients

This section describes how to configure Windows clients for Internet access via the WBR-3407.

The first step is to check the PC's TCP/IP settings.

The WBR-3407 uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

If using the default WBR-3407 settings, and the default Windows TCP/IP settings, no changes need to be made.

- By default, the WBR-3407 will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

- The *Gateway* must be set to the IP address of the WBR-3407
- The *DNS* should be set to the address provided by your ISP.



Note!

If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 8 - Advanced Setup* for details.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

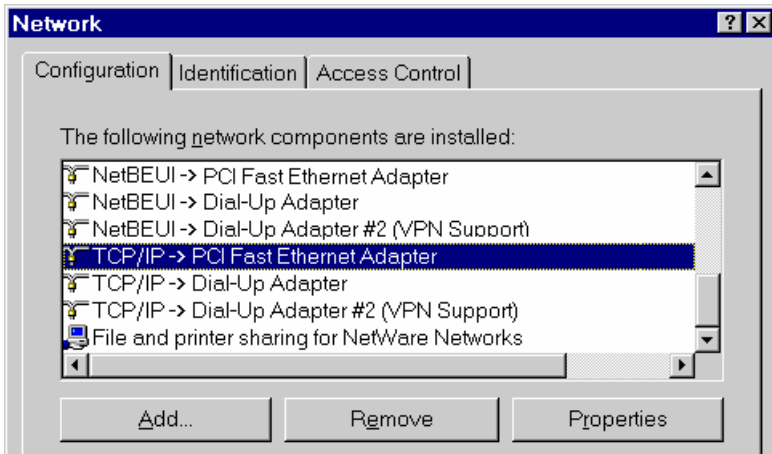


Figure 14: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

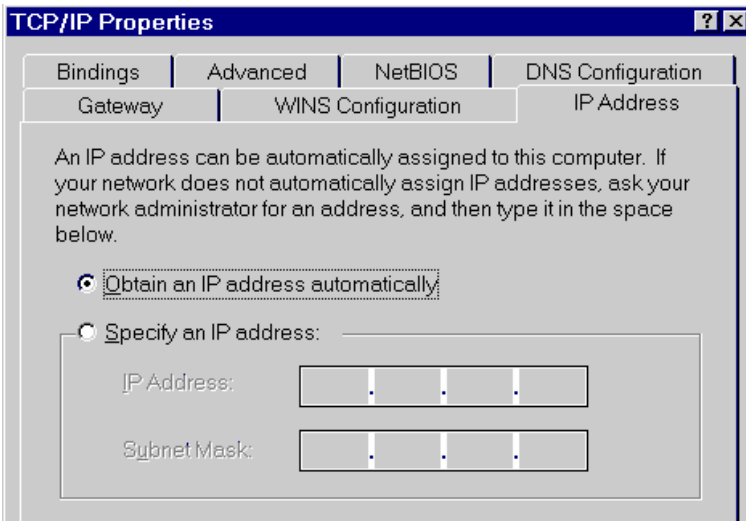


Figure 15: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the WBR-3407 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the WBR-3407.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

- On the *Gateway* tab, enter the WBR-3407's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to the WBR-3407.

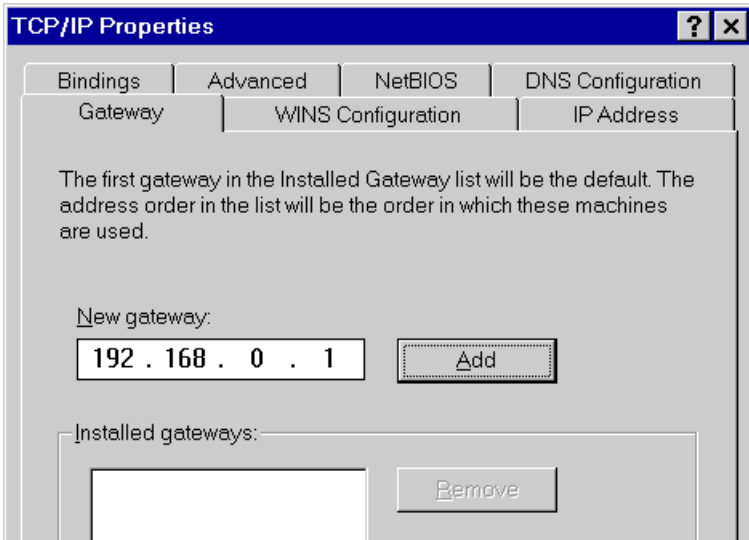


Figure 16: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

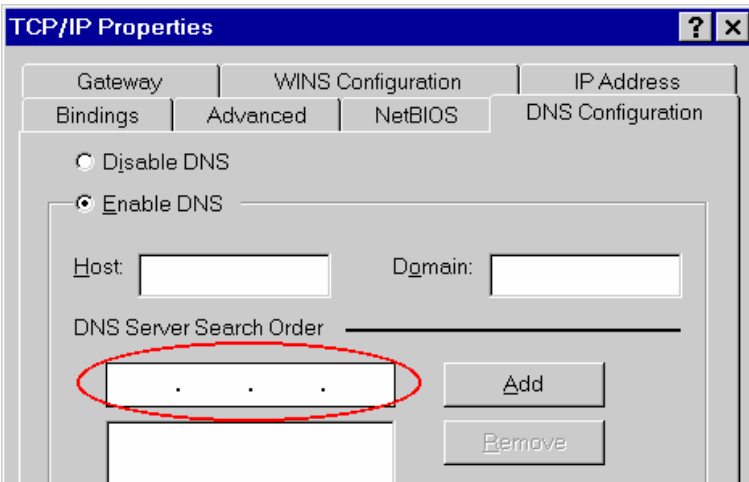


Figure 17: DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.

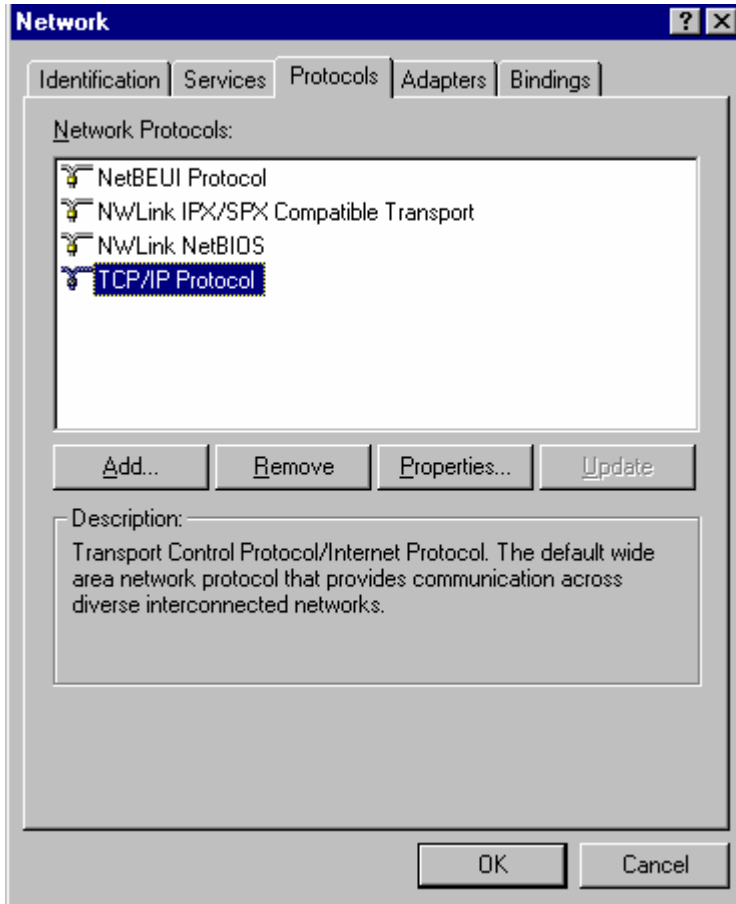


Figure 18: Windows NT4.0 - TCP/IP

2. Click the *Properties* button to see a screen like the one below.

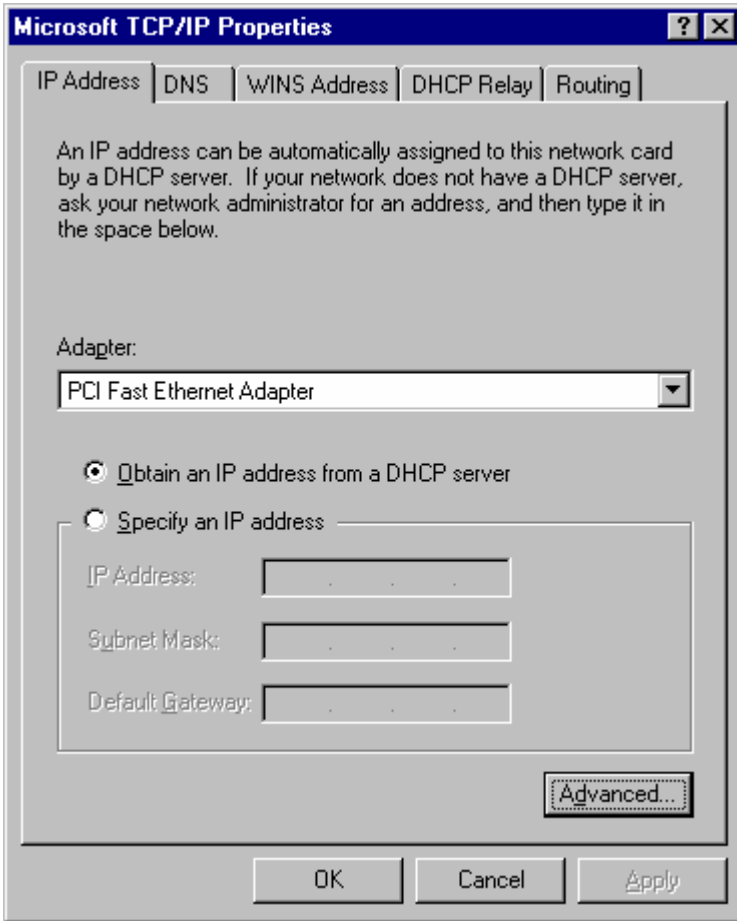


Figure 19: Windows NT4.0 - IP Address

3. Select the network card for your LAN.
4. Select the appropriate radio button - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*, as explained below.

Obtain an IP address from a DHCP Server

This is the default Windows setting. **Using this is recommended.** By default, the WBR-3407 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the WBR-3407.

Specify an IP Address

If your PC is already configured, check with your network administrator before making the following changes.

1. The *Default Gateway* must be set to the IP address of the WBR-3407. To set this:
 - Click the *Advanced* button on the screen above.
 - On the following screen, click the *Add* button in the *Gateways* panel, and enter the WBR-3407's IP address, as shown in Figure 20 below.
 - If necessary, use the *Up* button to make the WBR-3407 the first entry in the *Gateways* list.

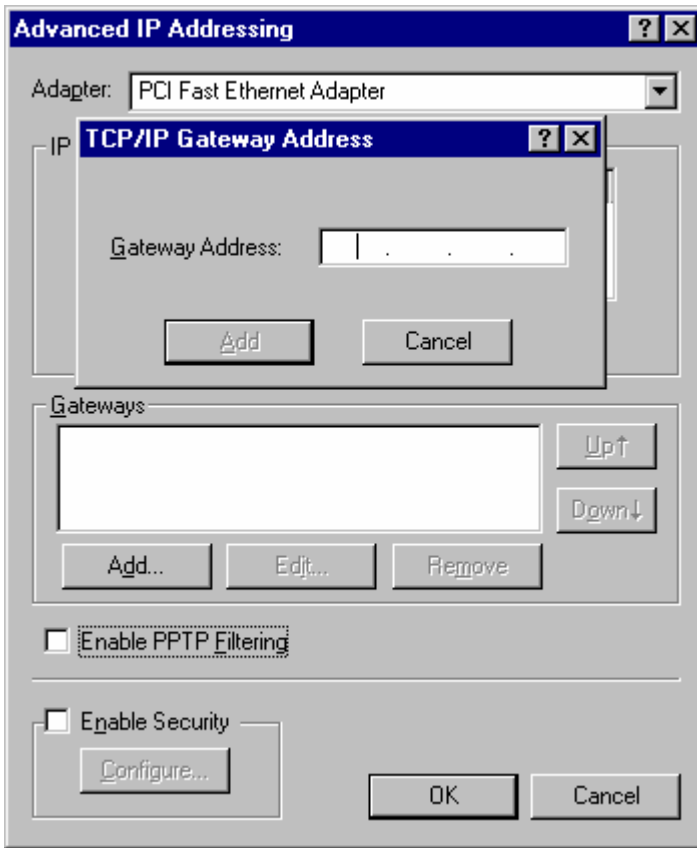


Figure 20 - Windows NT4.0 - Add Gateway

2. The DNS should be set to the address provided by your ISP, as follows:
 - Click the DNS tab.
 - On the DNS screen, shown below, click the *Add* button (under *DNS Service Search Order*), and enter the DNS provided by your ISP.

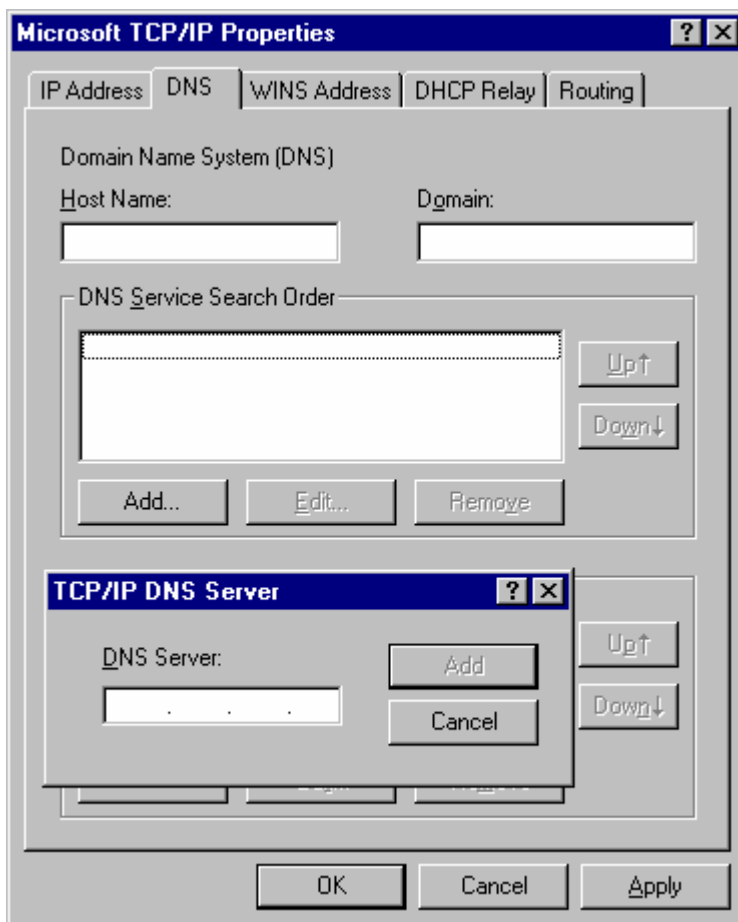


Figure 21: Windows NT4.0 - DNS

Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

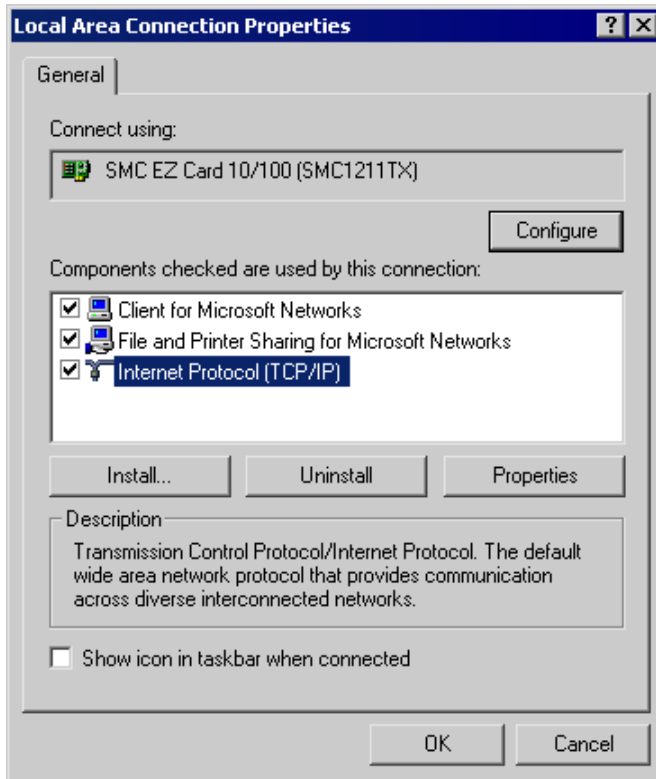


Figure 22: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

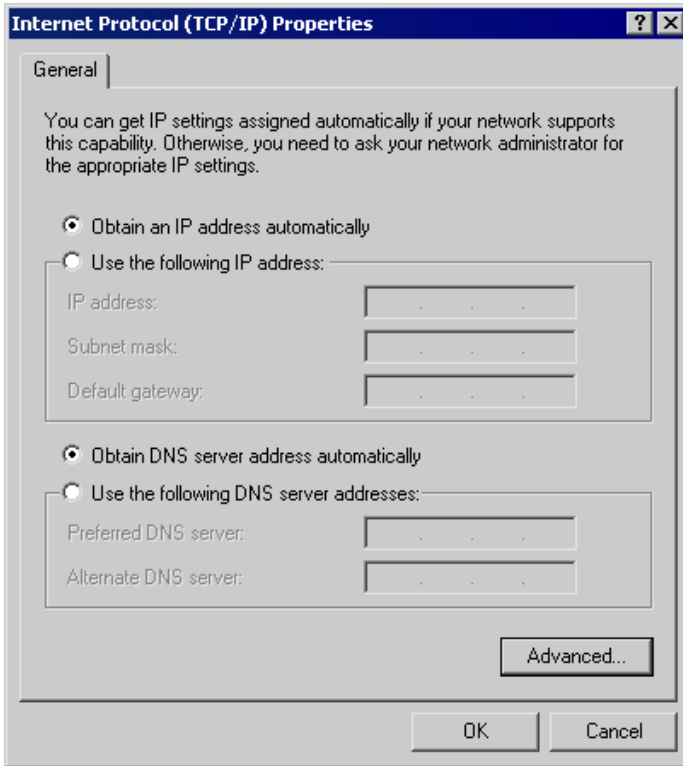


Figure 23: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct, as described below.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the WBR-3407 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the WBR-3407.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the WBR-3407's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the WBR-3407.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

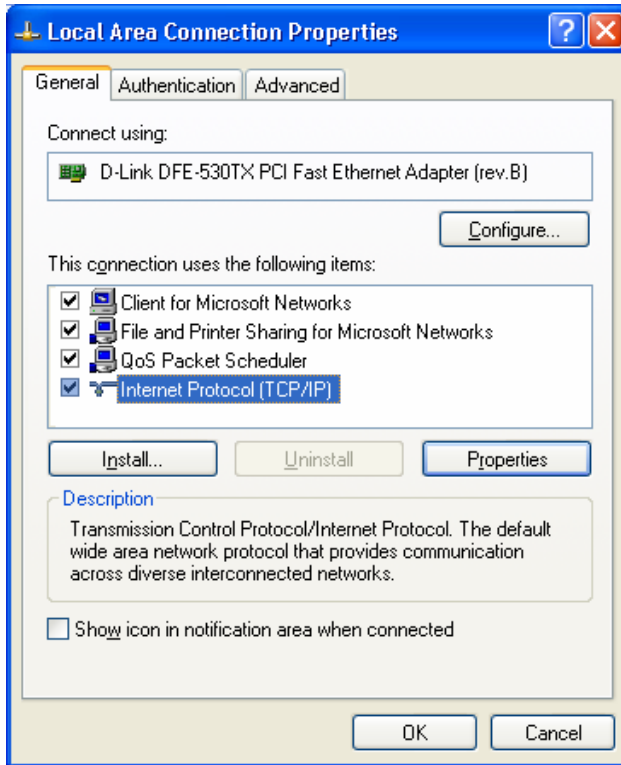


Figure 24: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

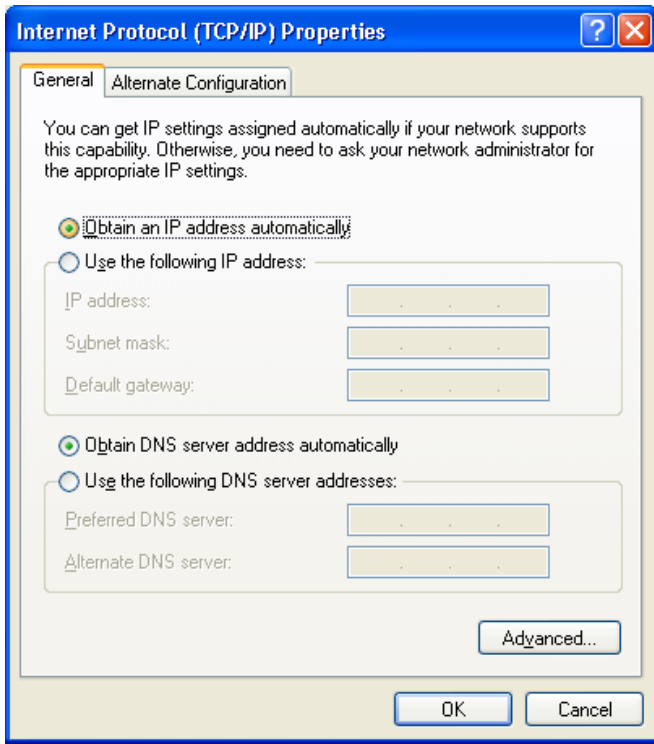


Figure 25: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the WBR-3407 will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the WBR-3407.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the WBR-3407's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the WBR-3407.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Internet Access

To configure your PCs to use the WBR-3407 for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 9x/ME/2000

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?".
7. Click *Finish* to close the Internet Connection Wizard.
Setup is now completed.

For Windows XP

1. Select *Start Menu - Control Panel - Network and Internet Connections*.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.
7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard.
Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the WBR-3407, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "WBR-3407".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "WBR-3407" location.

Macintosh Clients

From your Macintosh, you can access the Internet via the WBR-3407. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the WBR-3407's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the WBR-3407, it is only necessary to set the WBR-3407 as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the WBR-3407.
- Ensure your DNS (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
 - Use the "Deactivate" and "Activate" buttons, if available.
 - OR, restart your system.

Other Unix Systems

To access the Internet via the WBR-3407:

- Ensure the "Gateway" field for your network card is set to the IP Address of the WBR-3407.
- Ensure your DNS (Name Server) settings are correct.

Wireless Station Configuration

This section applies to all Wireless stations wishing to use the WBR-3407's Access Point, regardless of the operating system which is used on the client.

To use the WBR3407 in the WBR-3407, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to <i>Infrastructure</i> (rather than Ad-hoc) Access points only operate in <i>Infrastructure</i> mode.
SSID (ESSID)	This must match the value used on the WBR-3407. The default value is wireless . Note! The SSID is case sensitive.
Wireless Security	By default, Wireless security on the WBR-3407 is disabled . <ul style="list-style-type: none"> • If WEP or WPA-PSK is enabled on the WBR-3407, each station must use the same settings as the WBR-3407. • If WPA-802.1x is enabled, each station must obtain a certificate for authentication. See the following section for details.

Using WPA-802.1x - Overview

802.1x mode provides greater security and centralized management, but it is more complex to configure.

Wireless Station Configuration

For each of the following items, each Wireless Station must have the same settings as the WBR3407.

802.1x Authentication	Each client must obtain a Certificate which is used for authentication for the Radius Server.
802.1x Encryption	Typically, EAP-TLS is used. This is a dynamic key system, so keys do NOT have to be entered on each Wireless station.

Radius Server Configuration

If using **WPA-802.1x** mode, the Radius Server on your network must be configured as follow:

- It must provide and accept **Certificates** for user authentication.
- There must be a **Client Login** for the WBR3407 itself.
 - The WBR3407 will use its Default Name as its Client Login name.
 - The *Shared Key*, set on the *Security* Screen of the Access Point, must match the *Shared Secret* value on the Radius Server.
- **Encryption** settings must be correct.

802.1x Server Setup (Windows 2000 Server)

This section describes using *Microsoft Internet Authentication Server* as the Radius Server, since it is the most common Radius Server available that supports the EAP-TLS authentication method.

The following services on the Windows 2000 Domain Controller (PDC) are also required:

- dhcpd
- dns
- rras
- webservr (IIS)
- Radius Server (Internet Authentication Service)
- Certificate Authority

Windows 2000 Domain Controller Setup

1. Run *dcpromo.exe* from the command prompt.
2. Follow all of the default prompts, ensure that DNS is installed and enabled during installation.

Services Installation

1. Select the Control Panel - Add/Remove Programs.
2. Click *Add/Remove Windows Components* from the left side.
3. Ensure that the following components are activated (selected):
 - *Certificate Services*. After enabling this, you will see a warning that the computer cannot be renamed and joined after installing certificate services. Select *Yes* to select certificate services and continue
 - *World Wide Web Server*. Select *World Wide Web Server* on the *Internet Information Services (IIS)* component.
 - From the *Networking Services* category, select *Dynamic Host Configuration Protocol (DHCP)*, and *Internet Authentication Service* (DNS should already be selected and installed).

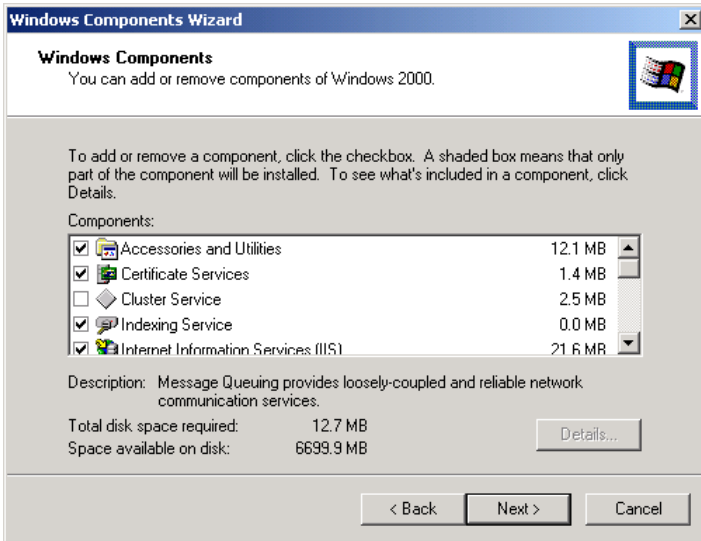


Figure 26: Components Screen

4. Click *Next*.
5. Select the *Enterprise root CA*, and click *Next*.

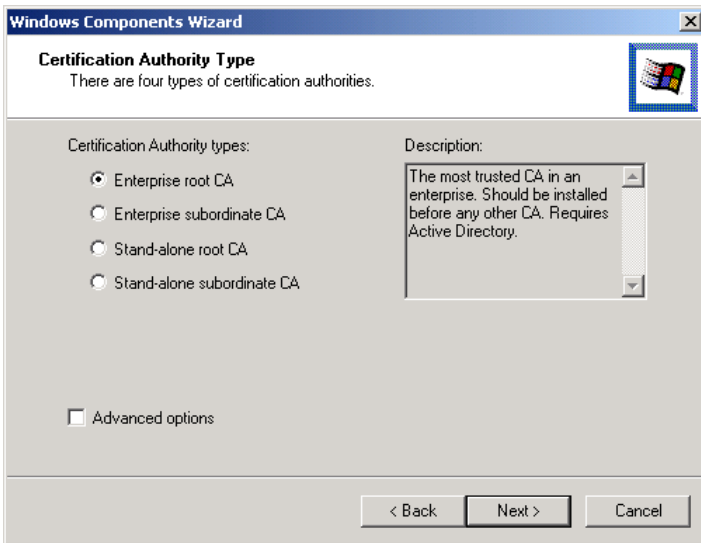


Figure 27: Certification Screen

6. Enter the information for the Certificate Authority, and click *Next*.

Windows Components Wizard

CA Identifying Information
Enter information to identify this CA

CA name:

Organization:

Organizational unit:

City:

State or province: Country/region:

E-mail:

CA description:

Valid for: Years Expires:

< Back Next > Cancel

Figure 28: CA Screen

7. Click *Next* if you don't want to change the CA's configuration data.
8. Installation will warn you that Internet Information Services are running, and must be stopped before continuing. Click *Ok*, then *Finish*.

DHCP server configuration

1. Click on the Start - Programs - Administrative Tools - DHCP
2. Right-click on the server entry as shown, and select *New Scope*.

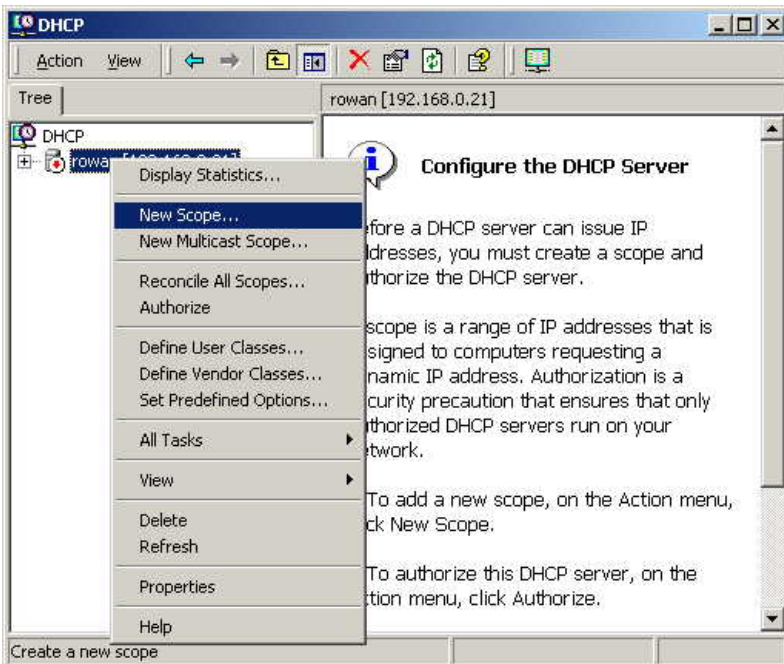


Figure 29: DHCP Screen

3. Click *Next* when the New Scope Wizard Begins.
4. Enter the name and description for the scope, click *Next*.
5. Define the IP address range. Change the subnet mask if necessary. Click *Next*.

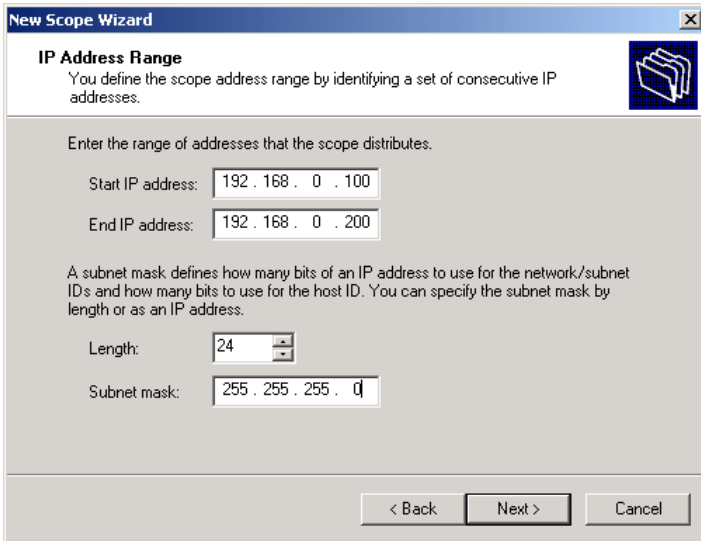


Figure 30:IP Address Screen

6. Add exclusions in the address fields if required. If no exclusions are required, leave it blank. Click *Next*.
7. Change the *Lease Duration* time if preferred. Click *Next*.
8. Select *Yes, I want to configure these options now*, and click *Next*.
9. Enter the router address for the current subnet. The router address may be left blank if there is no router. Click *Next*.
10. For the Parent domain, enter the domain you specified for the domain controller setup, and enter the server's address for the IP address. Click *Next*.

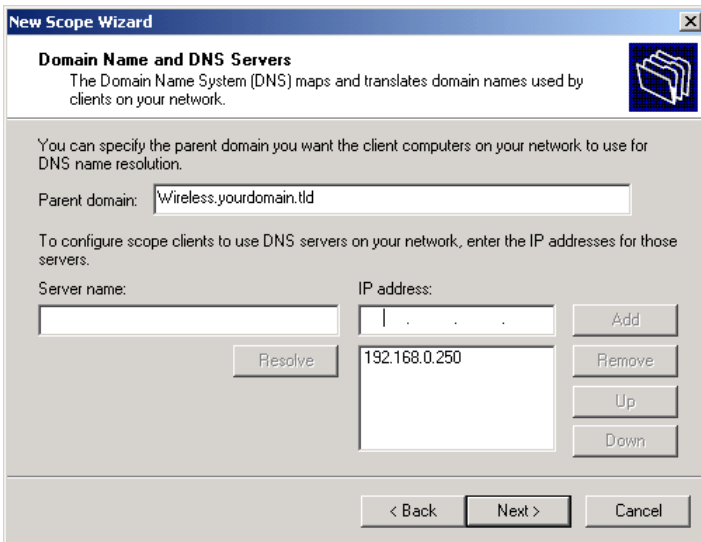


Figure 31: DNS Screen

11. If you don't want a WINS server, just click *Next*.
12. Select *Yes, I want to activate this scope now*. Click *Next*, then *Finish*.
13. Right-click on the server, and select *Authorize*. It may take a few minutes to complete.

Certificate Authority Setup

1. Select Start - Programs - Administrative Tools - Certification Authority.
2. Right-click *Policy Settings*, and select *New - Certificate to Issue*.

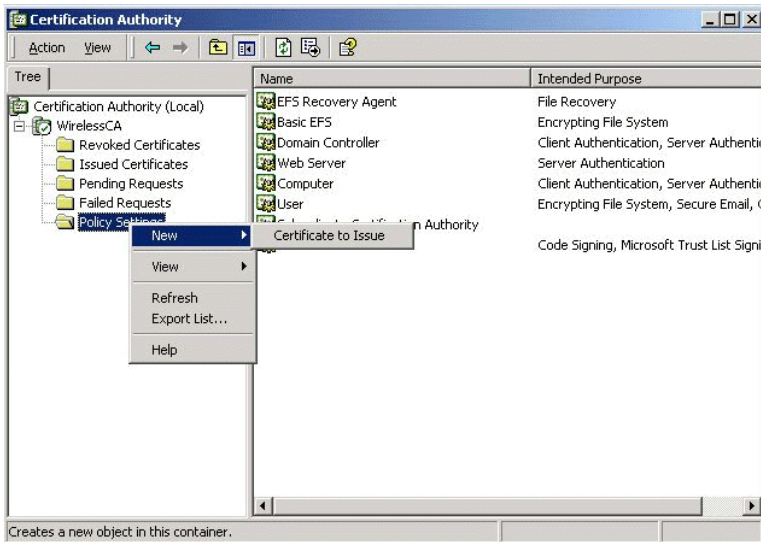


Figure 32: Certificate Authority Screen

3. Select *Authenticated Session* and *Smartcard Logon* (select more than one by holding down the Ctrl key). Click *OK*.



Figure 33: Template Screen

4. Select Start - Programs - Administrative Tools - Active Directory Users and Computers.
5. Right-click on your active directory domain, and select *Properties*.

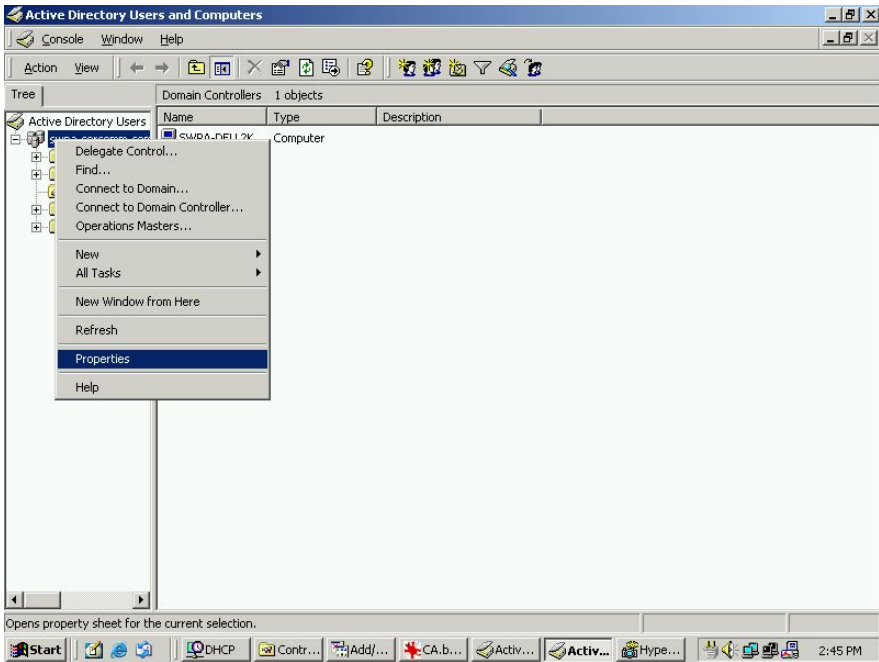


Figure 34: Active Directory Screen

6. Select the *Group Policy* tab, choose *Default Domain Policy* then click *Edit*.

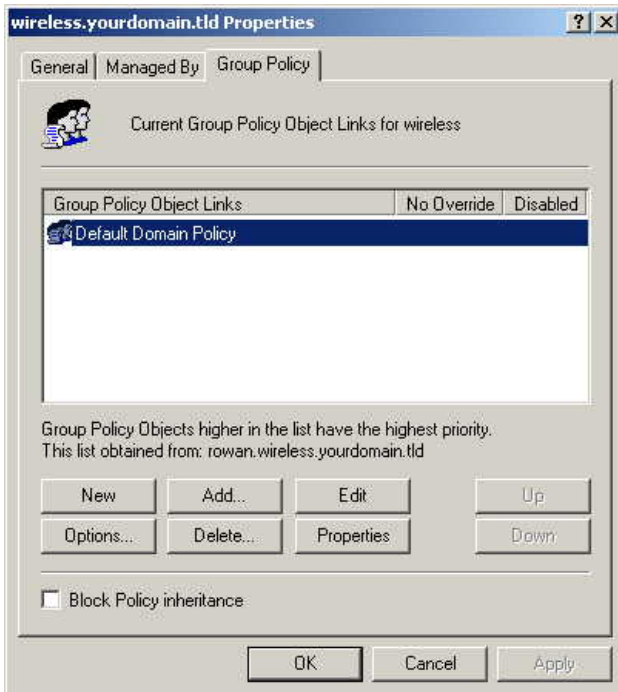


Figure 35: Group Policy Tab

7. Select *Computer Configuration - Windows Settings - Security Settings - Public Key Policies*, right-click *Automatic Certificate Request Settings - New - Automatic Certificate Request*.

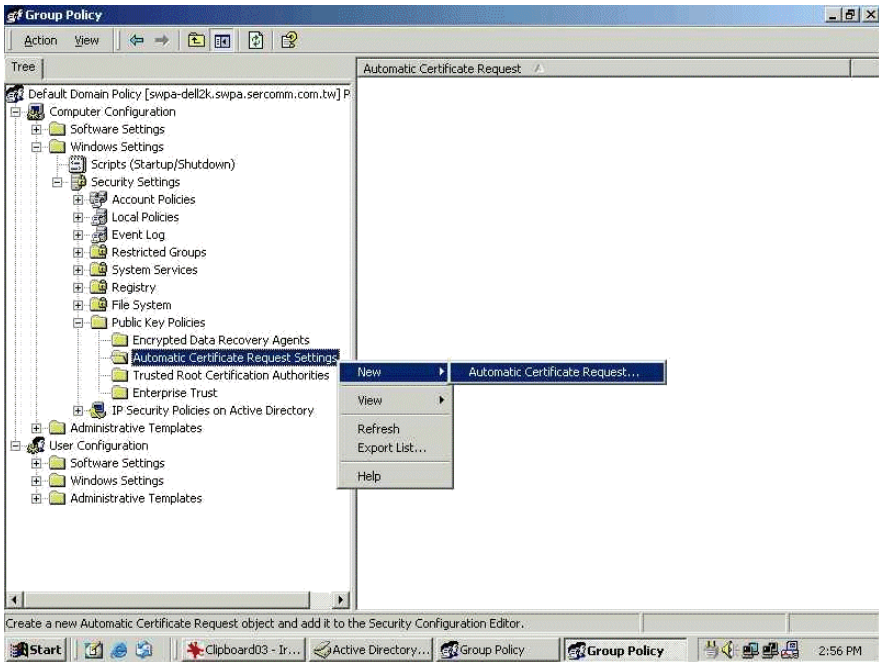


Figure 36: Group Policy Screen

8. When the Certificate Request Wizard appears, click *Next*.
9. Select *Computer*, then click *Next*.



Figure 37: Certificate Template Screen

10. Ensure that your certificate authority is checked, then click *Next*.
11. Review the policy change information and click *Finish*.
12. Click *Start - Run*, type `cmd` and press enter.
Enter `secdit /refreshpolicy machine_policy`
This command may take a few minutes to take effect.

Internet Authentication Service (Radius) Setup

1. Select Start - Programs - Administrative Tools - Internet Authentication Service
2. Right-click on *Clients*, and select *New Client*.

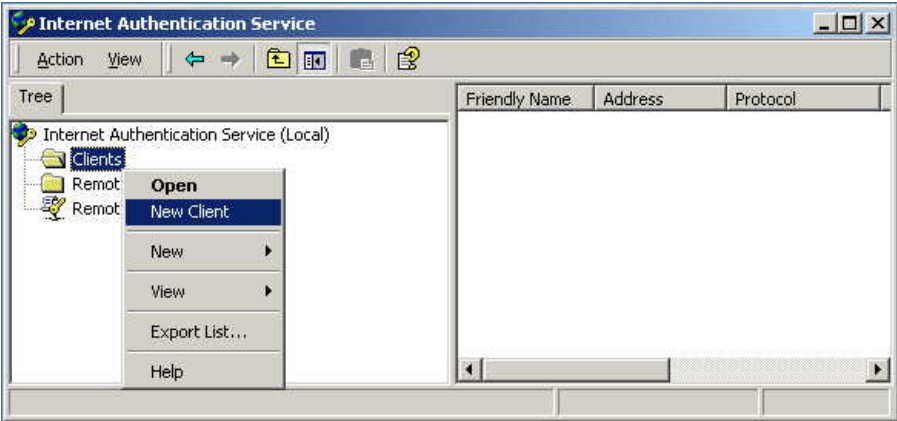


Figure 38: Service Screen

3. Enter a name for the access point, click *Next*.
4. Enter the address of the WBR3407, and set the shared secret, as entered on the WBR3407.
5. Click *Finish*.
6. Right-click on *Remote Access Policies*, select *New Remote Access Policy*.
7. Assuming you are using EAP-TLS, name the policy `eap-tls`, and click *Next*.
8. Click *Add...*
If you don't want to set any restrictions and a condition is required, select *Day-And-Time-Restrictions*, and click *Add...*

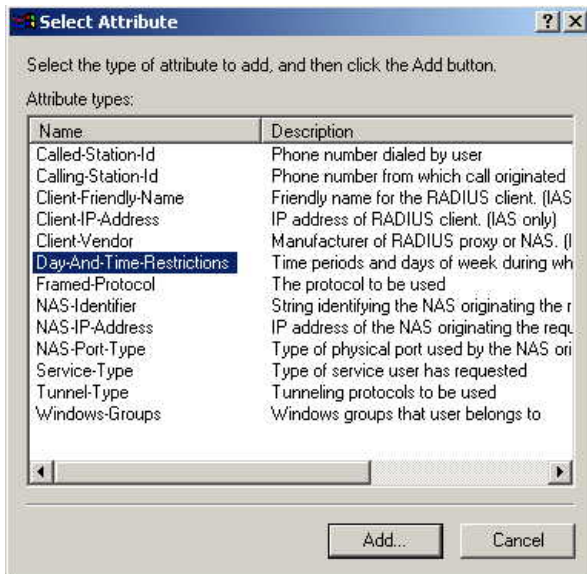


Figure 39: Attribute Screen

9. Click *Permitted*, then *OK*. Select *Next*.
10. Select *Grant remote access permission*. Click *Next*.

11. Click *Edit Profile...* and select the *Authentication* tab. Enable *Extensible Authentication Protocol*, and select *Smart Card or other Certificate*. Deselect other authentication methods listed. Click *OK*.

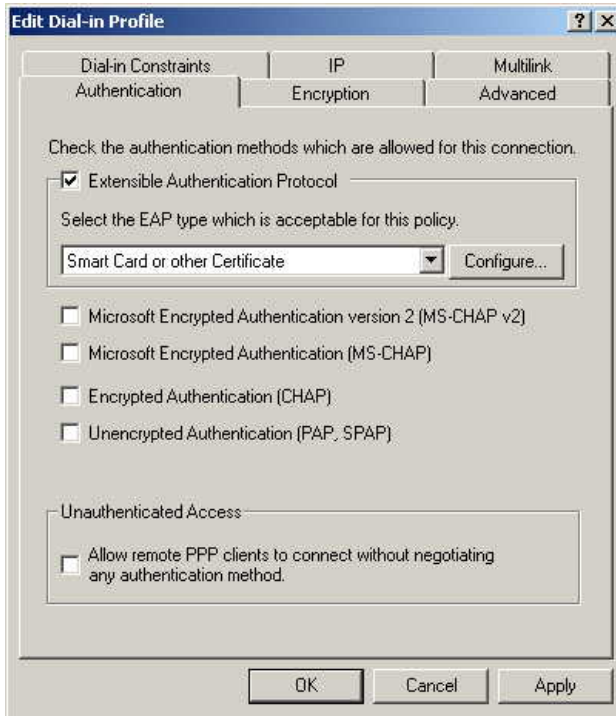


Figure 40: Authentication Screen

12. Select *No* if you don't want to view the help for EAP. Click *Finish*.

Remote Access Login for Users

1. Select Start - Programs - Administrative Tools- Active Directory Users and Computers.
2. Double click on the user who you want to enable.
3. Select the *Dial-in* tab, and enable *Allow access*. Click *OK*.

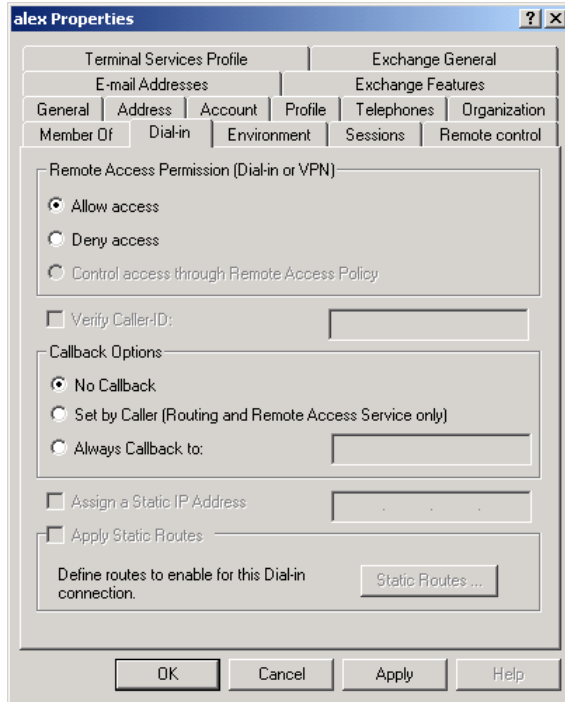


Figure 41: Dial-in Screen

802.1x Client Setup on Windows XP

Windows XP ships with a complete 802.1x client implementation. If using Windows 2000, you can install SP3 (Service Pack 3) to gain the same functionality.

If you don't have either of these systems, you must use the 802.1x client software provided with your wireless adapter. Refer to your vendor's documentation for setup instructions.

The following instructions assume that:

- You are using Windows XP
- You are connecting to a Windows 2000 server for authentication.
- You already have a login (User name and password) on the Windows 2000 server.

Client Certificate Setup

1. Connect to a network which doesn't require port authentication.
2. Start your Web Browser. In the *Address* box, enter the IP address of the Windows 2000 Server, followed by */certsrv*
e.g `http://192.168.0.2/certsrv`
3. You will be prompted for a user name and password. Enter the *User name* and *Password* assigned to you by your network administrator, and click *OK*.



Figure 42: Connect Screen

4. On the first screen (below), select *Request a certificate*, click *Next*.

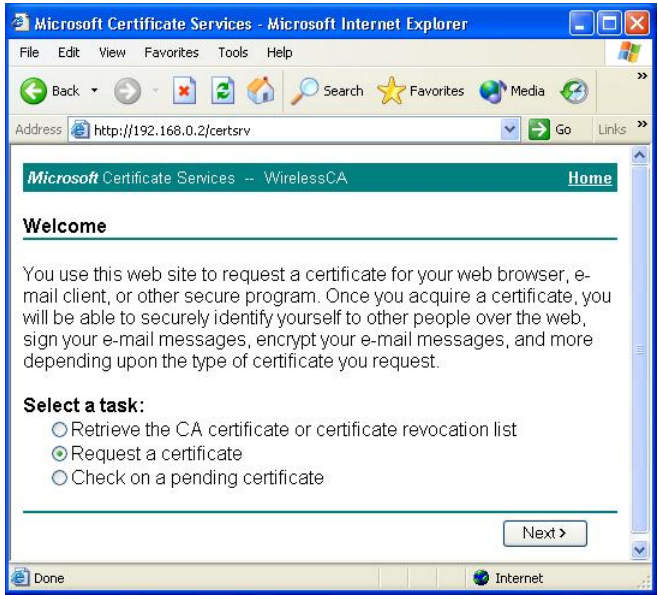


Figure 43: Wireless CA Screen

5. Select *User certificate request* and select *User Certificate*, then click *Next*.

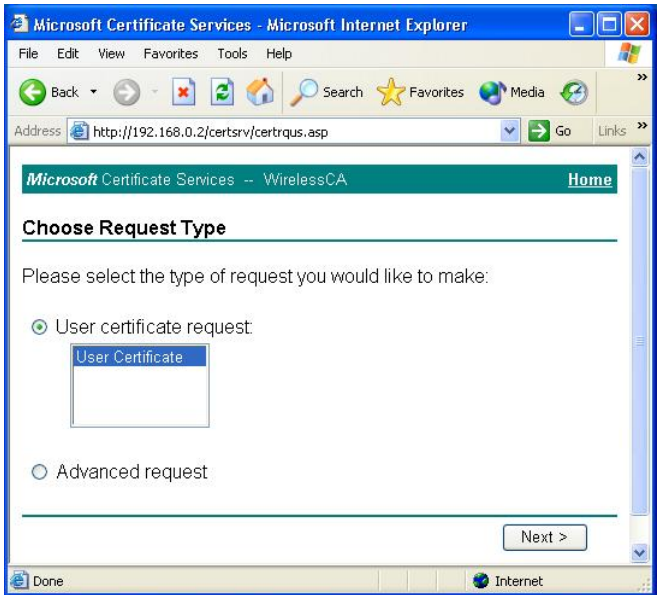


Figure 44: Request Type Screen

6. Click *Submit*.

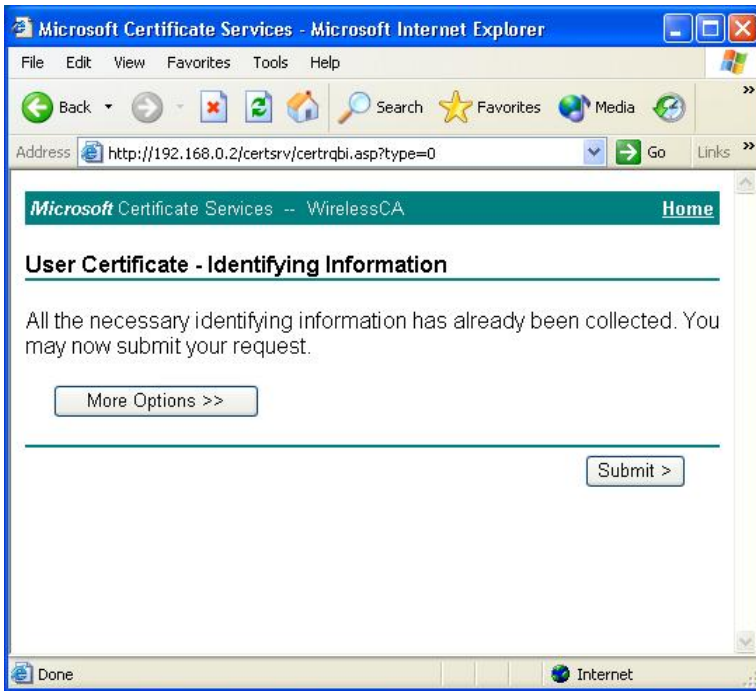


Figure 45: Identifying Information Screen

7. A message will be displayed, then the certificate will be returned to you. Click *Install this certificate*.

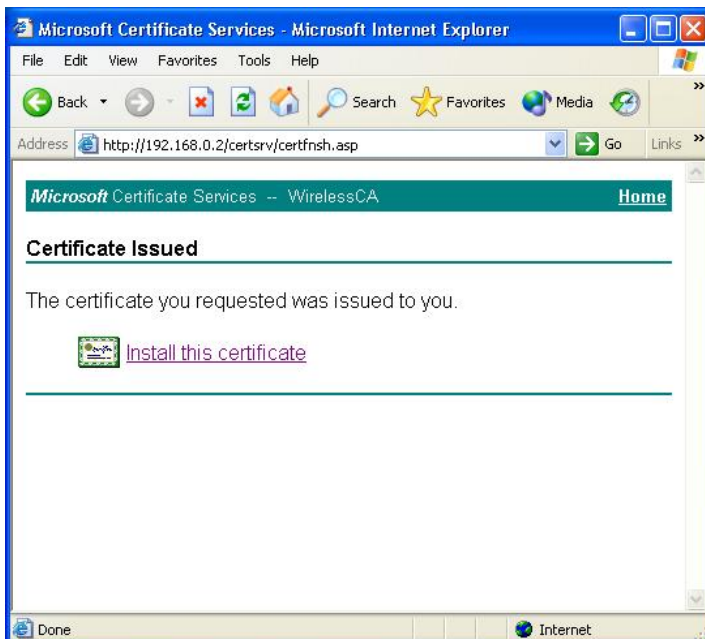


Figure 46: Certificate Issued Screen

8. . You will receive a confirmation message. Click *Yes*.

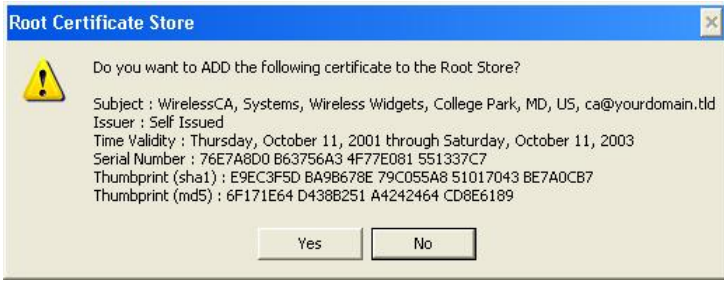


Figure 47: Root Certificate Screen

9. Certificate setup is now complete.

802.1x Authentication Setup

1. Open the properties for the wireless connection, by selecting *Start - Control Panel - Network Connections*.
2. Right Click on the *Wireless Network Connection*, and select *Properties*.
3. Select the *Authentication* Tab, and ensure that *Enable network access control using IEEE 802.1X* is selected, and *Smart Card or other Certificate* is selected from the EAP type.

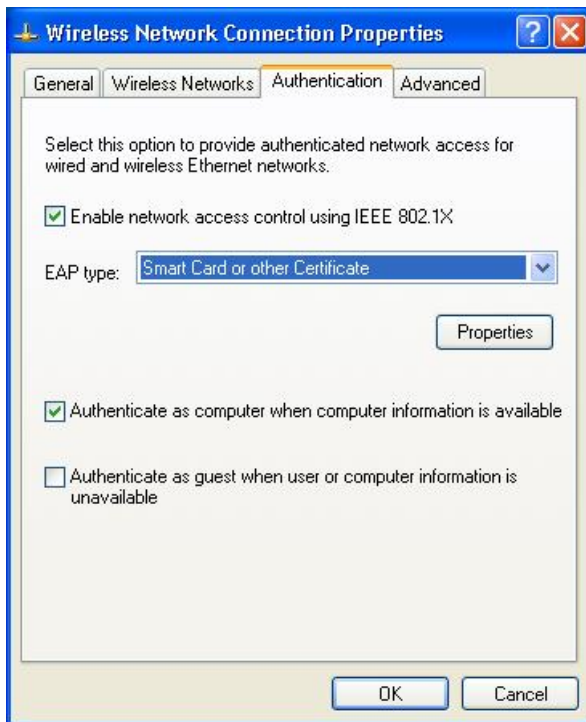


Figure 48: Authentication Tab

Encryption Settings

The Encryption settings must match the APs (Access Points) on the Wireless network you wish to join.

- Windows XP will detect any available Wireless networks, and allow you to configure each network independently.

- Your network administrator can advise you of the correct settings for each network. 802.1x networks typically use EAP-TLS. This is a dynamic key system, so there is no need to enter key values.

Enabling Encryption

To enable encryption for a wireless network, follow this procedure:

- Click on the *Wireless Networks* tab.

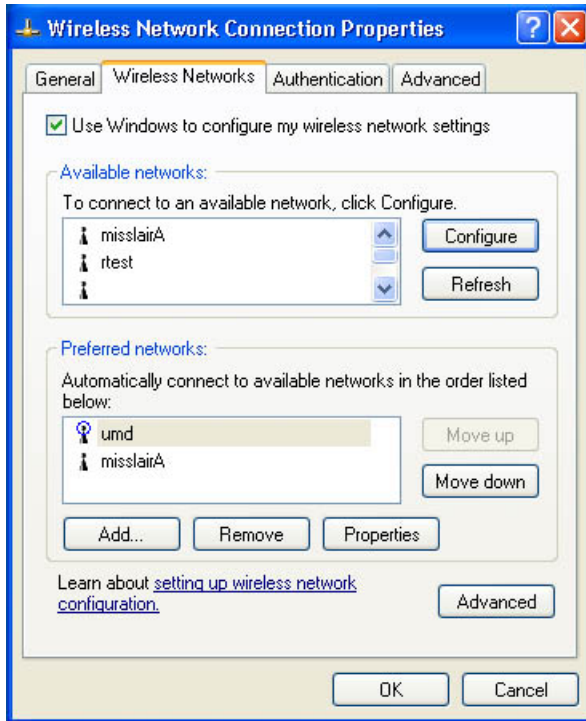


Figure 49: Wireless Networks Screen

- Select the wireless network from the *Available Networks* list, and click *Configure*.
- Select and enter the correct values, as advised by your Network Administrator. For example, to use EAP-TLS, you would enable *Data encryption*, and click the checkbox for the setting *The key is provided for me automatically*, as shown below.

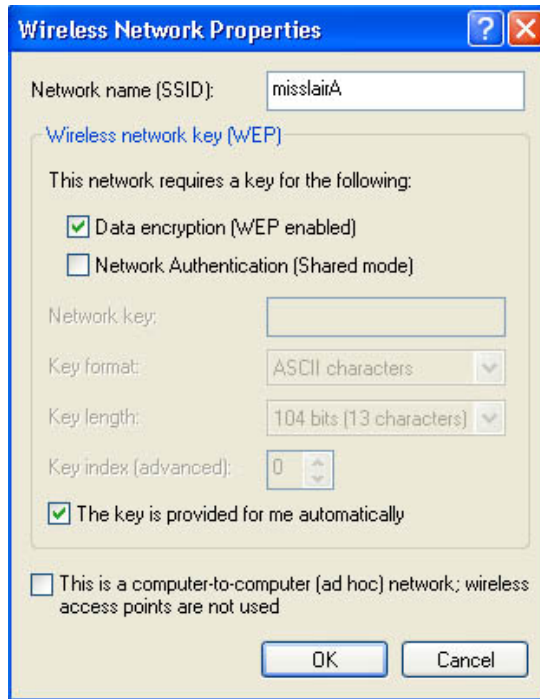


Figure 50: Properties Screen

Setup for Windows XP and 802.1x client is now complete.

Chapter 5

Operation and Status



This Chapter details the operation of the WBR-3407 and the status screens.

Operation

Once both the WBR-3407 and the PCs are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required. Refer to *Chapter 6 - Advanced Features* for further details.

Status Screen

Use the *Status* link on the main menu to view this screen.

The screenshot shows the 'Status' screen with a large 'S' logo and the word 'tatus'. The screen is divided into four sections: Internet, LAN, Wireless, and System. Each section contains a list of status information. At the bottom, there are three buttons: 'Attached Devices', 'Refresh Screen', and 'Help'.

Section	Parameter	Value
Internet	Modem Status	Connecting
	DownStream Connection Speed	0 kbps
	UpStream Connection Speed	0 kbps
	Connection Method:	PPPOA
	Internet Connection:	Idle
	Internet IP Address:	---
LAN	IP Address:	192.168.0.1
	Network Mask:	255.255.255.0
	DHCP Server:	On
	MAC Address	00:c0:02:ff:96:62
Wireless	Name (SSID)	Wireless
	Region	Europe
	Channel	3
	Wireless AP	enable
	Broadcast Name	enable
System	Device Name:	WBR-3407A
	Firmware Version:	0.01.02

Buttons: Attached Devices, Refresh Screen, Help

Figure 51: Status Screen

Data - Status Screen

Internet	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	If connected, displays the speed for the DownStream (download) ADSL Connection.
UpStream Connection Speed	If connected, displays the speed for the UpStream (upload) ADSL Connection.
Connection Method	This indicates the current connection method, as set in the <i>Setup Wizard</i> .
Internet Connection	<p>This indicates the current status of the Internet Connection</p> <ul style="list-style-type: none"> • Active - Connection exists • Idle - No current connection, but no error has been detected. This condition normally arises when an idle connection is automatically terminated. • Failed - The connection was terminated abnormally. This could be caused by Modem failure, or the loss of the connection to the ISP's server. <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If using a dynamic IP address, and no connection currently exists, this information is unavailable.
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
LAN	
IP Address	The IP Address of the WBR-3407.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
MAC Address	This shows the MAC Address for the WBR-3407, as seen on the LAN interface.
Wireless	
Name (SSID)	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the WBR3407 feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.

System	
Device Name	The current name of the WBR-3407. This is also the "hostname" provided to ISPs who request this information.
Firmware Version	The version of the current firmware installed.
Buttons	
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection.
Attached Devices	This will open a sub-window, showing all LAN and Wireless devices currently on the network.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE & PPPoA

If using PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM), a screen like the following example will be displayed when the "Connection Details" button is clicked.

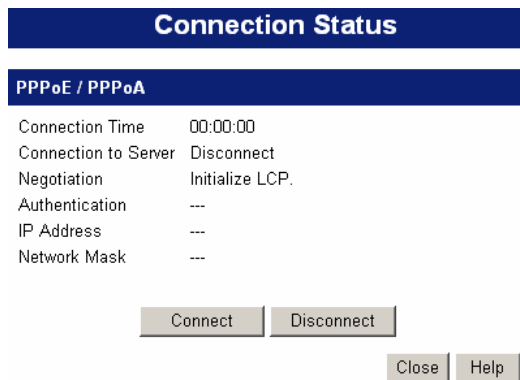


Figure 52: PPPoE Status Screen

Data – PPPoE/PPPoA Screen

Connection Time	This indicates how long the current connection has been established.
PPPoE Link Status	This indicates whether or not the connection is currently established. <ul style="list-style-type: none"> • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection.
Negotiation	This indicates the status of the PPPoE Server login.
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.

Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Close	Close this window.

Connection Details - Dynamic IP Address

If your access method is "Direct" (no login), with a Dynamic IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

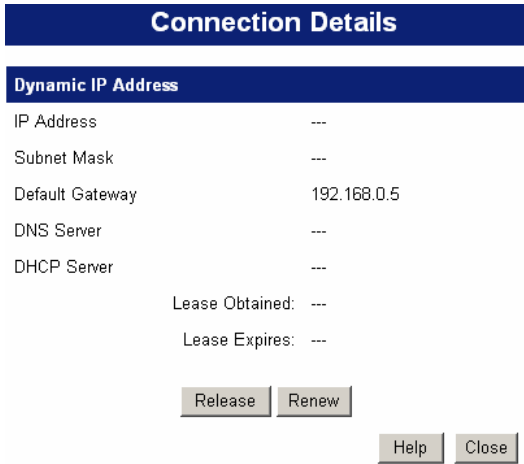


Figure 53: Connection Details - Fixed/Dynamic IP Address

Data - Dynamic IP address

Internet	
IP Address	The current IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP address of the remote Gateway or Router associated with the IP Address above.
DHCP Server	The IP address of your ISP's DHCP Server.
DNS Server	The IP address of the Domain Name Server which is currently used.
Lease Obtained Lease Expires	This indicates when the current IP address was obtained, and how long before this IP address allocation (the DHCP lease) expires.
Buttons	
Release	If an IP Address has been allocated to the WBR-3407 (by the ISP's DHCP Server, clicking the "Release" button will break the connection and release the IP Address.
Renew	If the ISP's DHCP Server has NOT allocated an IP Address for the WBR-3407, clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP

	Server.
Close	Close this window.

Connection Details - Fixed IP Address

If your access method is "Direct" (no login), with a fixed IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Status	
Fixed IP Address	
IP Address	192.168.0.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.5
DNS Server	254.255.255.254

Figure 54: Connection Details - Fixed/Dynamic IP Address

Data - Fixed IP address Screen

Internet	
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS Server	The IP Address of the Domain Name Server which is currently used.

Chapter 6

Advanced Features

6

This Chapter explains when and how to use the WBR-3407's "Advanced" Features.

Overview

The following advanced features are provided:

- Internet:
 - DMZ
 - URL filter
- Dynamic DNS
- Firewall Rules
- Firewall Services
- Schedule
- Virtual Servers

Internet

This screen provides access to the DMZ and URL Filter features.

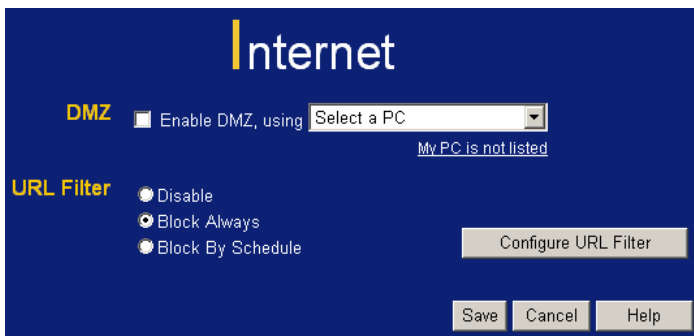


Figure 55: Advanced Internet Screen

DMZ

This feature, if enabled, allows the DMZ computer on your LAN to be exposed to all users on the Internet.

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data.
- If the DMZ feature is enabled, you must select the PC to be used as the "DMZ PC".



The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

URL Filter

If you want to limit access to certain sites on the Internet, you can use this feature. The URL filter will check each Web site access. If the address, or part of the address, is included in the block site list, access will be denied.

On the *Advanced Internet* screen, select the desired setting:

- **Disable** - disable this feature.
- **Block By Schedule** - block according to the settings on the *Schedule* page.
- **Block Always** - allow blocking all of the time, independent of the *Schedule* page.

Click the **Configure URL Filter** button to open the URL Filter screen, allowing you to create or modify the filter strings which determine which sites will be blocked.

URL Filter Screen

This screen is displayed when the **Configure URL Filter** button on the *Advanced Internet* screen is clicked.

Figure 56: URL Filter Screen

Data - URL Filter Screen

Current Filter Strings	
Current Filter Strings	<p>The list contains the current list of items to block.</p> <ul style="list-style-type: none"> • To add to the list, use the "Add" option below. • To delete an entry, select it and click Delete button. • To delete all entries, click the Delete All button.
Add Filter String	<p>To add to the current list, type the word or domain name you want to block into the field provided, then click the Add button.</p> <p>Filter strings should be as specific as possible. Otherwise, you may block access to many more sites than intended.</p>

Trusted PC	
Allow Trusted PC	Enable this to allow one computer to have unrestricted access to the Internet. For this PC, the URL filter will be ignored. If enabled, you must select the PC to be the trusted PC.
Trusted PC	Select the PC to be the Trusted PC.

Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

The DynDNS Service works as follows:

1. You must register for the service at <http://www.dyndns.org> (Registration is free). Your password will be E-mailed to you.
2. After registration, use the "Create New Host" option (at www.dyndns.org) to request your desired Domain name.
3. Enter your data from www.dyndns.org in the WBR-3407's DDNS screen.
4. The WBR-3407 will then automatically ensure that your current IP Address is recorded at <http://www.dyndns.org>
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select *Advanced* on the main menu, then *Dynamic DNS*, to see a screen like the following:

Figure 57: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
DDNS Data	
Service Provider	Select the desired DDNS Service provider.
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
User Name	Enter your Username for the DDNS Service.
Password	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
DDNS Status	<ul style="list-style-type: none"> This message is returned by the DDNS Server Normally, this message should be "Update successful" If the message is "No host", this indicates the host name entered was not allocated to you. You need to connect to DDNS Service provider and correct this problem.

Firewall Rules

The **Firewall Rules** screen allows you to define "Firewall Rules" which can allow or prevent certain traffic.

By default:

- All Outgoing traffic is permitted.
- All Incoming traffic is denied.

"Traffic" means incoming connection attempts, not packets.

Because of this default behavior, any **Outgoing** rules will generally **Block** traffic, and **Incoming** rules will generally **Allow** traffic.

Firewall Rules Screen

An example screen is shown below.

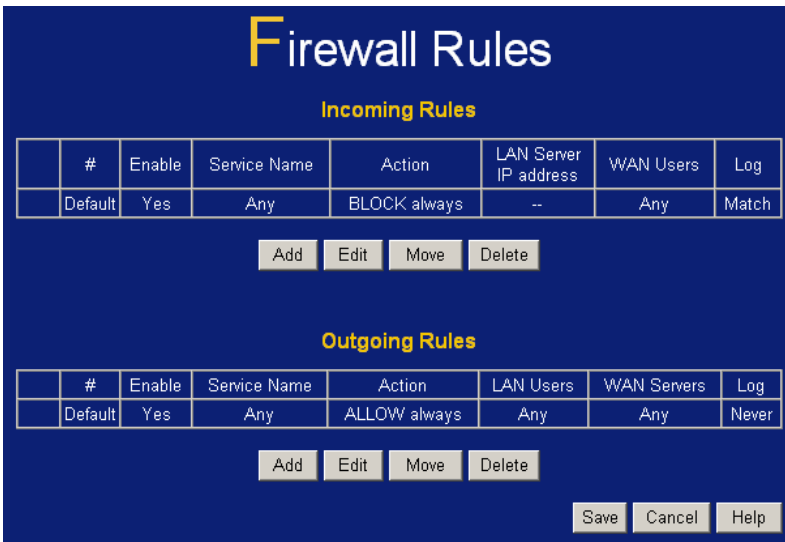


Figure 58 Firewall Screen

Data – Firewall Rules

Incoming Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.
LAN Server	The PC or Server on your LAN to which traffic covered by this rule will be sent.

WAN Users	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the <i>Add</i> button to create a new rule. The other buttons - <i>Edit</i> , <i>Move</i> , or <i>Delete</i> - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.
Outgoing Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.
LAN Users	The LAN PC or PCs covered by this rule.
WAN Servers	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the <i>Add</i> button to create a new rule. The other buttons - <i>Edit</i> , <i>Move</i> , or <i>Delete</i> - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.

Incoming Rules

This screen is displayed when the "Add" or "Edit" button for Incoming Rules is clicked.

Inbound Services

Service:

Action:

Send to LAN Server:

WAN Users:

Single/Start: . . .

Finish: . . .

Log:

Figure 59: Inbound Services Screen

Data – Incoming Rules Screen

Inbound Services	
Service	Select the desired Service. This determines which packets are covered by this rule. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.
Action	<p>Select the desired action for packets covered by this rule:</p> <ul style="list-style-type: none"> • ALLOW always • ALLOW by schedule, otherwise Block • BLOCK always • BLOCK by schedule, otherwise Allow <p>Note:</p> <ul style="list-style-type: none"> • Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule. • BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you wish to block a sub-set of traffic which is currently allowed by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
Send to LAN Server	Select the PC or Server on your LAN which will receive the inbound traffic covered by this rule.
WAN Users	<p>These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:</p> <ul style="list-style-type: none"> • Any - All IP addresses are covered by this rule. • Address range - If this option is selected, you must enter the desired values in the "Single/Start" and "Finish" fields to determine the address range. • Single address - Enter the required address in the "Single/Start" fields.

Log	<p>This determines whether packets covered by this rule are logged. Select the desired action.</p> <ul style="list-style-type: none"> • Always - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • Never - never log traffic considered by this rule, whether it matches or not. • Match - Log traffic only if it matches this rule. (The action is determined by this rule.) • Not Match - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)
------------	--

Outgoing Rules

This screen is displayed when the "Add" or "Edit" button for Outgoing Rules is clicked.

Figure 60: Outbound Services Screen

Data - Outbound Rules Screen

Outbound Services	
Service	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the "Services" menu option
Action	<p>Select the desired action for packets covered by this rule:</p> <ul style="list-style-type: none"> • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block <p>Note:</p> <ul style="list-style-type: none"> • Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule. • ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you wish to allow a subset of traffic which is currently blocked by another rule.)

	<ul style="list-style-type: none"> To define the Schedule used in these selections, use the "Schedule" screen.
LAN Users	<p>Select the desired option to determine which PCs are covered by this rule:</p> <ul style="list-style-type: none"> Any - All PCs are covered by this rule. Single PC - Only the selected PC is covered by this rule. If selected, you must select the PC. <p>PC - If using Single PC above, select the PC or Server on your LAN which will be covered by this rule.</p>
WAN Users	<p>These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:</p> <ul style="list-style-type: none"> Any - All IP addresses are covered by this rule. Address range - If this option is selected, you must enter the "Start" and "Finish" fields. Single address - Enter the required address in the "Single/Start" fields.
Log	<p>This determines whether packets covered by this rule are logged. Select the desired action.</p> <ul style="list-style-type: none"> Always - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) Never - never log traffic considered by this rule, whether it matches or not. Match - Log traffic only it matches this rule. (The action is determined by this rule.) Not Match - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Firewall Services

This screen is used to modify the list of *Services* which are available when creating Firewall Rules.



Figure 61: Add Services Screen

Data – Add Services

Services	
Services List	This lists all defined Services.
Add	Use this to open a sub-screen where you can add a new service.
Edit	To modify a service, select it, and then click this button.
Delete	Pre-defined Services can not be deleted, but you can use this button to delete any services you have defined.

Add/Edit Service

This screen is displayed when the *Add* or *Edit* button on the *Services* screen is clicked.

Figure 62 : Add/Edit Service

Data – Add/Edit Service

Services	
Name	If editing, this shows the current name of the Service. If adding a new service, this will be blank, and you should enter a suitable name.
Type	Select the protocol used by the Service.
Start Port	Enter the beginning of the port range used by the Service.
Finish Port	Enter the end of the port range used by the Service.

Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example *Options* screen is shown below.

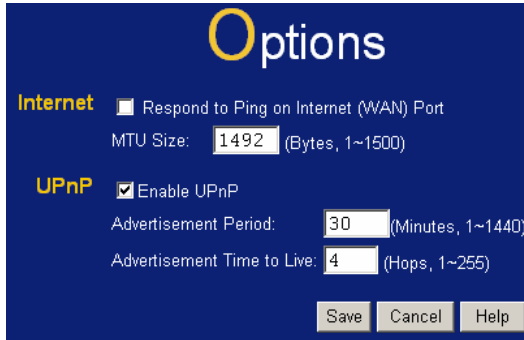


Figure 63: Options Screen

Data - Options Screen

Internet	
Respond to Ping	<ul style="list-style-type: none"> If checked, the WBR-3407 will respond to Ping (ICMP) packets received from the Internet. If not checked, Ping (ICMP) packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
MTU Size	Enter a value between 1 and 1500. Note: MTU (Maximum Transmission Unit) size should only be changed if advised to do so by Technical Support.
UPnP	
UPnP	<ul style="list-style-type: none"> UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported Windows ME, XP, or later. If Enabled, this device will be visible via UPnP. If Disabled, this device will not be visible via UPnP.
Advertisement Period	Enter the desired value, in minutes. The valid range is from 1 to 1440.
Advertisement Time to Live	Enter the desired value, in hops. The valid range is from 1 to 255.

Schedule

This Schedule can be used for the Firewall Rules and the URL filter.

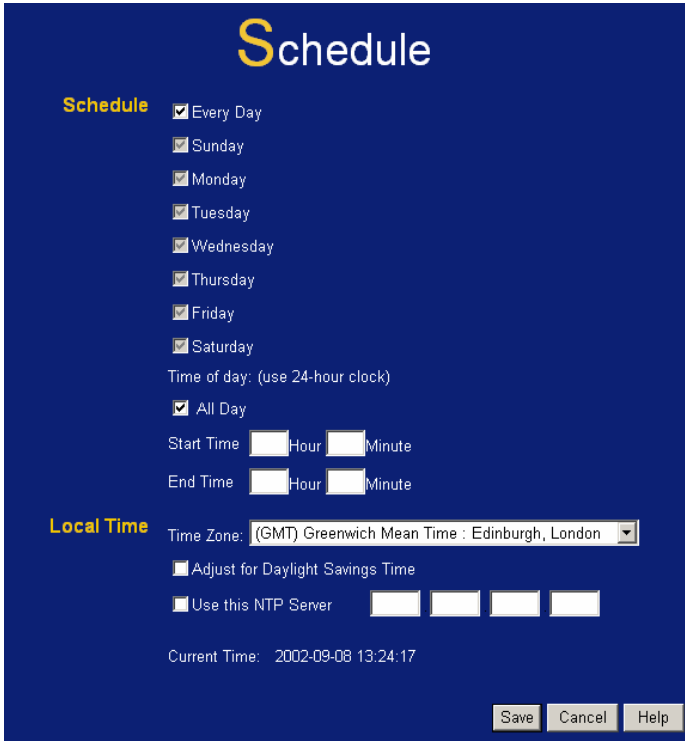


Figure 64: Schedule Screen

Data - Schedule Screen

Schedule	
Sunday, Monday...	Use these checkboxes to select the desired days.
Start Time	Enter the start using a 24 hr clock.
Finish Time	Enter the finish time using a 24 hr clock.
Local Time	
Time Zone	In order to display your local time correctly, you must select your "Time Zone" from the list.
Adjust for Daylight Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.
Use this NTP Server	If you prefer to use a particular NTP server as the primary server, check the checkbox "Use this NTP Server" and enter the Server's IP address in the fields provided.. If this setting is not enabled, the default NTP Servers are used.
Current Time	This displays the current time on the WBR-3407.

Virtual Servers

This feature, sometimes called *Port Forwarding*, allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

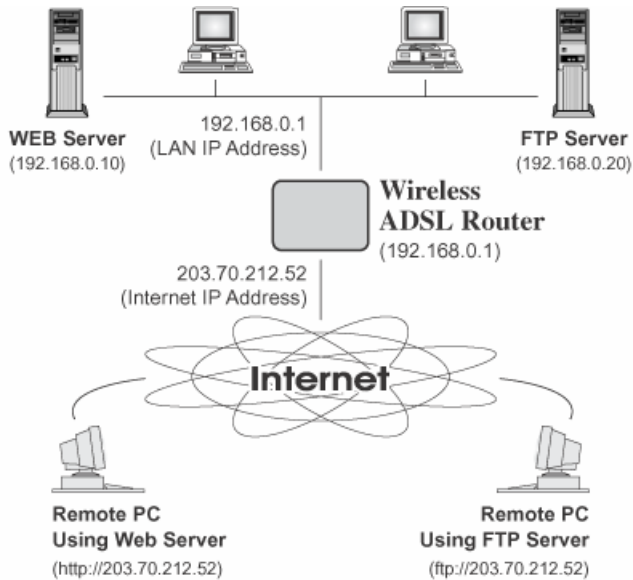


Figure 65: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

Virtual Servers Screen

- The "Virtual Servers" feature allows Internet Users to access PCs on your LAN.
- The PCs must be running the appropriate Server Software.
- For Internet Users, ALL of your Servers have the same IP address. This IP address is allocated by your ISP.
- To make it easier for Internet users to connect to your Servers, you can use the "DDNS" feature. This allows Internet users to connect to your Servers with a URL, rather than an IP address. This technology works even if your ISP allocates dynamic IP addresses (IP address is allocated upon connection, so it may change each time you connect).



Figure 66: Virtual Servers Screen

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of common Server types. If the desired Server type is not listed, you can create a Firewall Rule to achieve the same effect as the Virtual Server function.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. If Enabled, you must select the PC to which this traffic will be sent.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.



For each entry, the PC must be running the appropriate Server software.

If the desired Server type is not listed, you can define your own Servers, using the Firewall Rules.

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP).

e.g.

http://203.70.212.52

ftp://203.70.212.52

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.



From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP

Chapter 7



Advanced Administration

This Chapter explains the settings available via the "Administration" section of the menu.

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The available settings and features are:

PC Database	This is the list of PCs shown when you select the "DMZ PC" or a "Virtual Server". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
Config File	Backup or restore the configuration file for the WBR-3407. This file contains all the configuration data.
Logging & Email	View or clear all logs, set E-Mailing of log files and alerts.
Diagnostics	Perform a Ping or DNS Lookup.
Remote Admin	Allow settings to be changed from the Internet..
Routing	Only required if your LAN has other Routers or Gateways.
Upgrade Firmware	Upgrade the Firmware (software) installed in your WBR-3407.

PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC).

- It eliminates the need to enter IP addresses.
- Also, you do not need to use fixed IP addresses on your LAN.

However, if you do use a fixed IP address on some devices on your LAN, you should enter details of each such device into the PC database, using the PC Database screen.

PC Database Screen

An example *PC Database* screen is shown below.

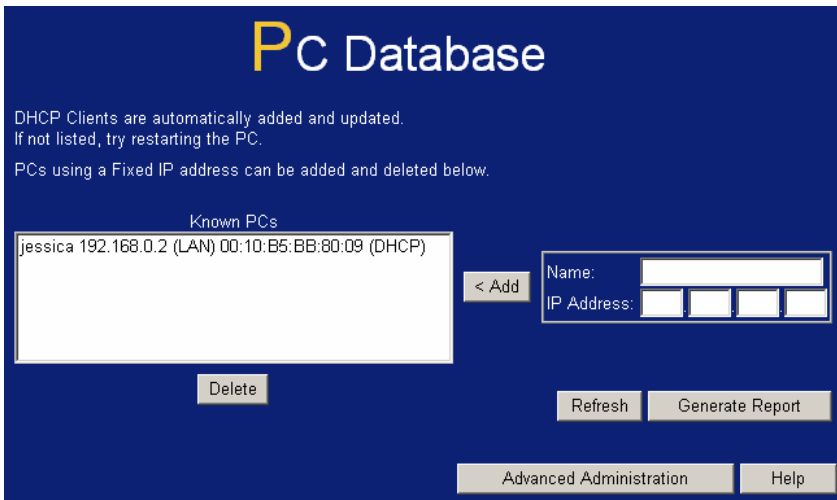


Figure 67: PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The WBR-3407 uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.
- This system means you do NOT need to use Fixed (static) IP addresses on your LAN. However, you can add PCs using Fixed (static) IP Addresses to the PC database if required.

Data - PC Database Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Add	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Delete	Delete the selected PC from the list. This should be done in 2 situations: <ul style="list-style-type: none"> • The PC has been removed from your LAN. • The entry is incorrect.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Advanced Administration	View the Advanced version of the PC database screen - <i>PC Database (Admin)</i> . See below for details.

PC Database (Admin)

This screen is displayed if the "Advanced Administration" button on the *PC Database* is clicked. It provides more control than the standard *PC Database* screen.

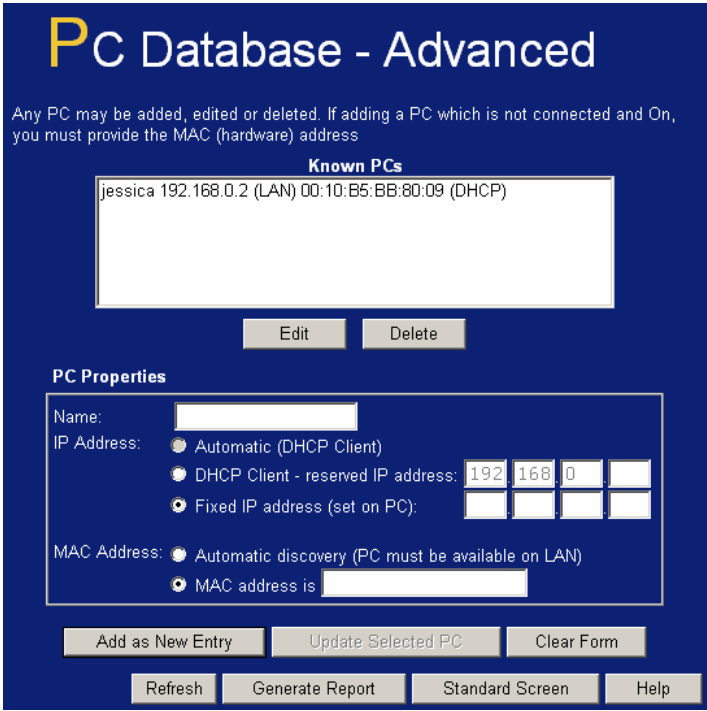


Figure 68: PC Database (Admin)

Data - PC Database (Admin) Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> • Automatic - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The WBR-3407 will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • DCHP Client - Reserved IP Address - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the WBR-3407 will always allocate the same IP Address to this PC. Enter the required IP address. • Fixed IP Address - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC itself must be configured to use this IP address.)

