Wireless Router

User's Manual

V. 1.2

Copyright

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Trademark Recognition

Microsoft, MS-DOS and Windows are registered trademarks of Microsoft Corp.

Other product names used in this manual are the properties of their respective owners and are acknowledged.

Regulatory compliance

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. This equipment also complies with CE EN55022 Class B and VCCI V3 Class B specifications. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

FCC Statement

This product has been tested and complies with the specifications 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 according to 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 to radio or television reception, which is found 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:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

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

Safety Information

Before installing and using the Wireless Router, take note of the following precautions:

- Read all instructions carefully.
- Do not place the unit on an unstable surface, cart, or stand.
- Only use the supplied power adapter.
- Do not place anything on the power cord. Place the power cord where it will not be in the way of foot traffic.
- Follow all warnings and cautions in this manual and on the unit case.
- Avoid using the system near water, in direct sunlight, or near a heating device.

About this manual

This user's manual describes how to install and operate your Wireless Router. Please read this manual before you install the product.

This manual includes the following topics:

- Product description, features and specifications
- Hardware installation procedure
- Software configuration information
- Technical Specifications
- Troubleshooting procedures

Table of contents

CHAPTER 1
Introduction

Thank you for purchasing the Wireless Router. The Wireless Router is an ideal broadband sharing solution for SOHO and home networks, featuring a wireless LAN function that reduces the necessity of connecting stations via a wired LAN.

The Wireless Router manages all IP address assignments by DHCP, relieving users of the necessity of manually configuring clients for inter-client communication and access to the Internet. A built-in firewall provides extra security from malicious attack.

The intuitive Web browser interface enables users to configure all aspects of the router, including making LAN, WAN, and WLAN settings, making access restrictions, setting administrative and user passwords, and creating status logs.

The router is fully compatible with the IEEE 802.11b wireless standard and supports IEEE 802.3 10 BaseT and 100 BaseTX ports for easy interfacing to a wired Ethernet. Based on direct sequence spread spectrum (DSSS) technology and operating in the 2.4 GHz band, the router accommodates the IEEE 802.11b standard supporting data communications rates of 1/2/5.5/11/22Mbps.

Packing Checklist

Carefully unpack the Wireless Router and check that the following items are included:

- ❑ Wireless Router
- ❑ Power adapter
- ❑ One category-5 UTP Ethernet cable with RJ-45 connectors
- ❑ User's manual or CD-ROM

Contact your dealer immediately if any items appear damaged or if the unit does not work.

System and Setup Requirements

To ensure smooth operation of the Router, the following minimum system and setup requirements should be met:

- WindowsMe/NT4/2000/98/95
- Mac OS
- Netscape Navigator 4.7 or Microsoft Internet Explorer 5.0
- DSL/Cable Modem Broadband Internet connection and ISP account
- PCs equipped with 10Mbps or 10/100Mbps Ethernet connection to support TCP/IP protocol

Applications

- Home SOHO networking for device sharing and wireless multimedia
- Wireless office provides a wider range for home and SOHO Ethernet
- Enables wireless building-to-building data communication
- Built-in infrastructure mode
- Router provides ideal solution for:
  - Difficult-to-wire environments
  - Temporary LANs for scenarios such as trade-exhibitions and meetings
  - Enables LAN adaptability to frequently changing environments
  - Enables remote access to corporate network information, for example e-mail and the company home page

Features

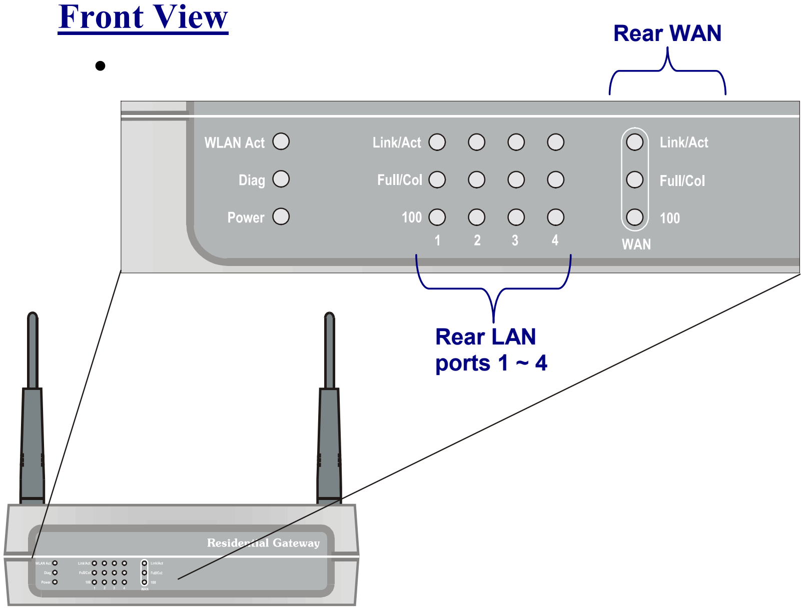
- Wireless Features
  - Compatible with IEEE 802.11b Direct Sequence high data rate specifications
  - Supports high-speed wireless connections up to 22 Mbps
  - Advanced Power Management mode for workstations
  - Auto fallback data rate for long distance communications and noisy environments
  - WEP 64/128/256-bit encryption function
  - Two fixed dipole antennas provide flexible station configuration
  - Plug-and-Play installation
- Security Features
  - Firewall support provides security against unauthorized access and malicious attack
  - Finger Print Identification Authorization (Option)
- Web-based browser configuration for simplified management
- Convenient initial configuration via LAN port
- Connect to cable or ADSL modem through the Ethernet RJ-45 port
- Supports DHCP client and server
- Features Network Address Port Translation (NAPT)
- Web-based firmware upgradeable

Identifying Components

Refer to the following illustrations to familiarize yourself with the Router’s front-panel LEDs and rear-panel ports.

Front View

•

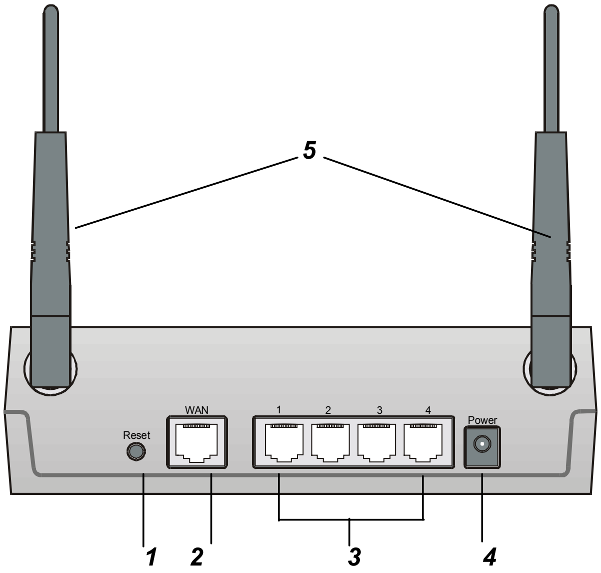


Refer to the table below for the LED meanings.

LED	Color	State	MEANING
WLAN Act	Green	On	Indicates WLAN link status
		Blinking	Indicates WLAN traffic
WLAN Link	Green	On	Indicates that the device is connected to the WLAN.
Power	On	Green	The unit is receiving power.
	Off	—	The unit is not receiving power
LINK/ACT	On	Green	Link is established
	On	Flashing Green	Packet transmit or receive activity
	Off	—	No Link activity
Full/Col	On	Green	Full-duplex mode
	On	Flashing Orange	Collision has occurred
	Off	—	Half-duplex mode
100	On	Green	Indicates link speed (100 Mbps)
Diag	On	Green	Indicates a connection error. When starting up or resetting the router, and updating the firmware this LED flashes indicating that the system is going through a series of self-diagnostics. When the LED turns off, the router is ready.

Rear View

The following illustration shows the router's rear-panel ports:



Item		Function
1	Reset button	Push and hold this button for five seconds to reset the Wireless Router to the factory default settings.
2	WAN port	Connect the Wireless Router to the Internet via your cable or ADSL modem and this RJ-45 port.
3	LAN ports	The four RJ-45 Ethernet ports allow you to connect client PCs or LAN hubs to the Wireless Router.
4	Power port	Plug the AC adapter into this port.
5	Antenna	Two antennas provide wireless LAN functionality and ensure optimal signal strength.

About Wireless LAN

Wireless Local Area Network (WLAN) systems offer a great number of advantages over traditional wired systems. WLANs are flexible, easy to set up and manage, and more economical than wired LAN systems.

WLANs use radio frequency (RF) technology to transmit and receive data through the air using the unlicensed 2.4 GHz frequency band. WLANs combine data connectivity with user mobility. For example, users can roam from a conference room to their office without being disconnected from the LAN.

Using WLANs, users can conveniently access shared information, while network administrators can configure and augment networks without installing or moving network cables.

WLAN technology provides users with many convenient and cost saving features:

Mobility	WLANs provide LAN users with access to real-time information anywhere in their organization, providing service opportunities that are impossible with wired networks.
Scalability	WLANs can be configured in a variety of topologies to adapt to specific applications and installations.
Easy Installation	Installing is easy for novice and expert users alike, eliminating the need to install network cables in walls and ceilings.

Networking Modes

Wireless LANs can be configured in one of two ways:

Ad-hoc Networking

Also known as a peer-to-peer network, an ad-hoc network is one that allows all workstations and computers in the network to act as servers to all other users on the network.

Users on the network can share files, print to a shared printer, and access the Internet with a shared modem.

However, with ad-hoc networking, users can only communicate with other wireless LAN computers that are in the wireless LAN workgroup, and are within range.

Infrastructure Networking

Infrastructure networking differs from ad-hoc networking in that it includes an access point. Unlike the ad-hoc structure where users on the LAN contend the shared bandwidth, on an infrastructure network the access point can manage the bandwidth to maximize bandwidth utilization.

Additionally, the access point enables users on a wireless LAN to access an existing wired network, allowing wireless users to take advantage of the wired networks resources, such as Internet, email, file transfer, and printer sharing.

Infrastructure networking has the following advantages over ad-hoc networking:

- **Extended range**
  Each wireless LAN computer within the range of the access point can communicate with other wireless LAN computers within range of the access point.
- **Roaming**
  The access point enables a wireless LAN computer to move through a building and still be connected to the LAN.
- **Wired to wireless LAN connectivity**
  The access point bridges the gap between wireless LANs and their wired counterparts.

This concludes the first chapter. The next chapter deals with the hardware installation of the Wireless Router.

CHAPTER 2

Hardware installation

This chapter covers plugging in the Wireless Router, and connecting the router to a WAN, LAN, and wireless LAN (WLAN).

Setup Considerations

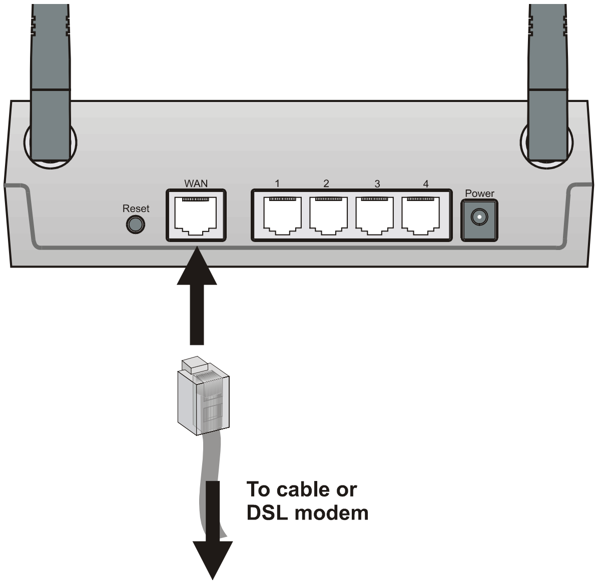
When setting up the Router be sure to note the following points:

- Optimize the performance of the Router by ensuring that the distance between access points is not too far. In most buildings, the Router operates within a range of 100 ~ 300 feet, depending on the thickness and structure of the walls.
- Radio waves can pass through walls and glass but not metal. If there is interference in transmitting through a wall, it may be that the wall has reinforcing metal in its structure. Install another access point to circumvent this problem.
- Floors usually have metal girders and metal reinforcing struts that interfere with transmission.
- Do not place the Router near (within 4 feet) electrical devices that generate RF noise, such as microwave ovens, monitors, and electric motors.

Connecting the Router to the WAN

Follow the procedure below to connect the Wireless Router to the WAN.

1. Plug the supplied straight cable into the WAN RJ-45 jack:



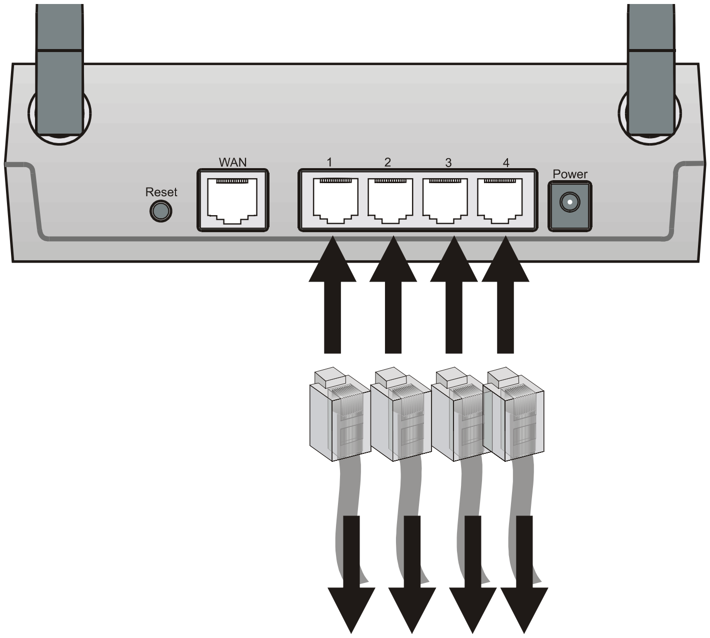
2. Plug the other end of the cable into the RJ-45 jack on your ADSL or cable modem.
3. Plug the AC adapter jack into the connector on the rear of the router, and plug the adapter into a wall socket.

Note!	*Insure that you only use the supplied AC adapter with the wireless router.*

Connecting the Router to the LAN

Follow the procedure below to connect the Wireless Router to the LAN.

4. Plug a straight cable into a free LAN RJ-45 jack at the rear of the router:



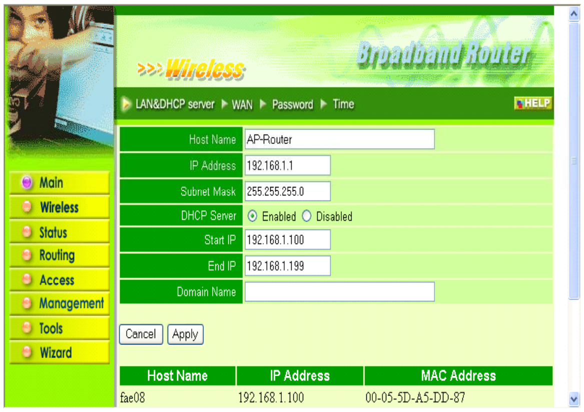
To LAN adapter on PC

5. Plug the other end of the cable into the RJ-45 jack on your computer.

Connecting the Router to the WLAN

Follow the procedure below to connect the Wireless Router to the WLAN.

1. Open the browser interface (refer to page 20).
2. Click **Wireless** to view the WLAN configuration page:



Host Name	AP-Router
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	● Enabled ○ Disabled
Start IP	192.168.1.100
End IP	192.168.1.199
Domain Name	

Host Name	IP Address	MAC Address
fae08	192.168.1.100	00-05-5D-A5-DD-87

3. Click the radio button next to Enabled. For connection to a WLAN client, the client must configure its WLAN interface so that the SSID and channel are the same as the Wireless Router’s.

Note!	*For more information about the browser interface, refer to the online help.*

This concludes Chapter 2. The next chapter covers operating system network configuration.

CHAPTER 3

Network Configuration

The following sections cover setting up the network configuration of your operating system, connecting to the router via the Web browser interface, and running the interface setup wizard.

TCP/IP Configuration Windows and Mac

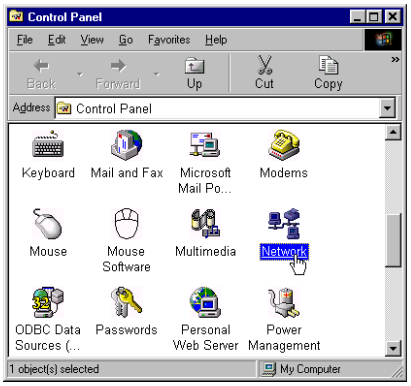
If you want to set up your router with a fixed IP address, you must manually configure your operating system network parameters. Refer to the following sections for instructions on configuring Windows ME/2000/9X and Macintosh operating system TCP/IP networking for both static and fixed IP addresses.

Notes!

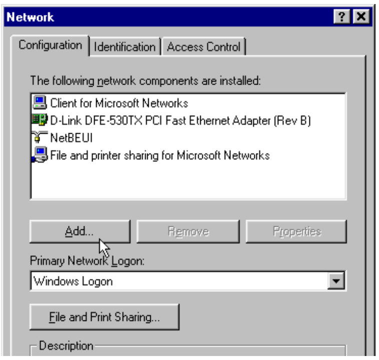
- *If you are configuring the router using a static IP address, contact your ISP for the information you need in the following sections.*
- *Be sure to have your operating system installation CD handy in case the configuration procedure requires you to install files.*

Windows ME/9X

1. Click **Start**, **Settings**, then click **Control Panel**. The Control Panel opens:



2. Double-click the **Network** icon to open the Network configuration dialog:

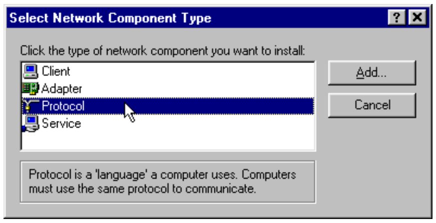


The following network components are installed:

Client for Microsoft Networks
D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev B)
NetBEUI
File and printer sharing for Microsoft Networks

Primary Network Logon:
Windows Logon

3. Go to step six if TCP/IP is shown in the network components installed list. Otherwise, click **Add.** The following screen appears prompting you to select the network component:

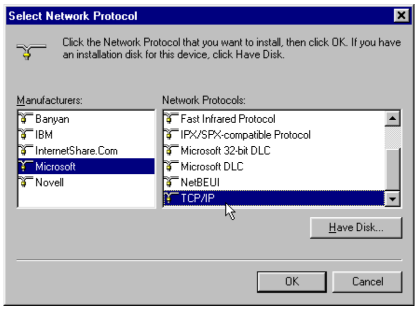


Click the type of network component you want to install:

Client
Adapter
Protocol
Service

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

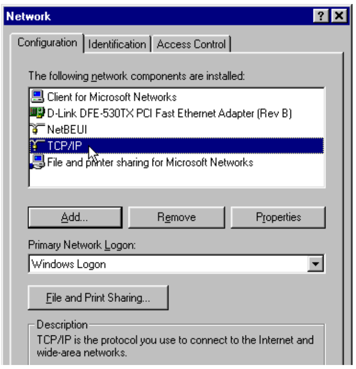
4. Select Protocol and click **Add**. The following screen appears:



Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers:	Network Protocols:
Banyan	Fast Infrared Protocol
IBM	IPX/SPX-compatible Protocol
InternetShare.Com	Microsoft 32-bit DLC
Microsoft	Microsoft DLC
Novell	NetBEUI
	TCP/IP

5. Under “Manufacturers” select Microsoft. In the “Network Protocols” list, select TCP/IP. Click **OK.** You are returned to the Network Configuration screen, and TCP/IP is listed:



Network

Configuration | Identification | Access Control

The following network components are installed:

- Client for Microsoft Networks
- D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev B)
- NetBEUI
- TCP/IP
- File and printer sharing for Microsoft Networks

Add... | Remove | Properties

Primary Network Logon:

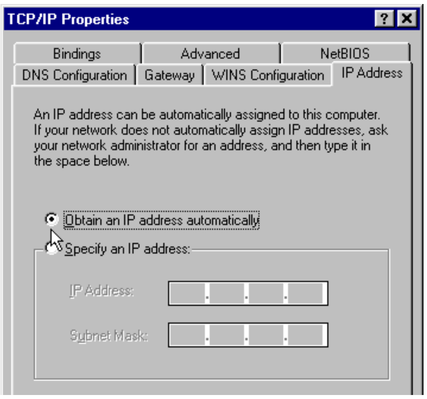
Windows Logon

File and Print Sharing...

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

6. Select TCP/IP and click **Properties**. The TCP/IP properties dialog box opens:



TCP/IP Properties

Bindings | Advanced | NetBIOS

DNS Configuration | Gateway | WINS Configuration | IP Address

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

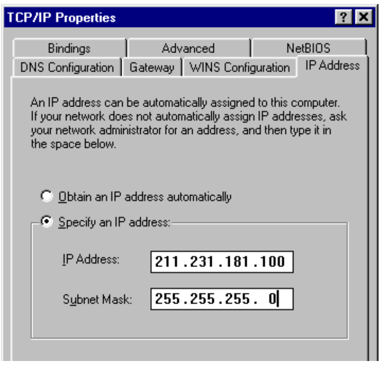
IP Address: . . .

Subnet Mask: . . .

7. Click the radio button next to “Obtain an IP address automatically” and go to step eight if you want the DHCP server to assign the IP address.

   If you want to assign a fixed IP address, follow these steps:

   a. In the TCP/IP Properties dialog box, click the radio button next to **Specify an IP address**:



TCP/IP Properties

Bindings | Advanced | NetBIOS

DNS Configuration | Gateway | WINS Configuration | IP Address

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

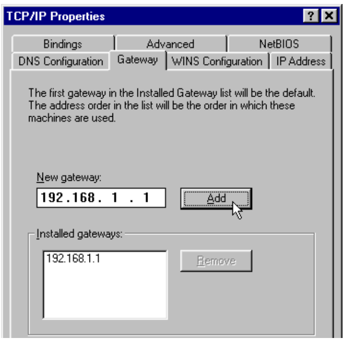
IP Address: 211 .231 .181 .100

Subnet Mask: 255 .255 .255 . 0

   b. Enter an IP address in the IP field.

      In the example shown, all IP addresses from 211.231.181.100 to 211.231.181.254 are available for dynamic IP address assignment, while 211.231.181.2 to 211.231.181.99 are available as static IP addresses.

c. Type a Subnet Mask value for the router. The default value is shown. Click the **Gateway** tab. The following screen appears:



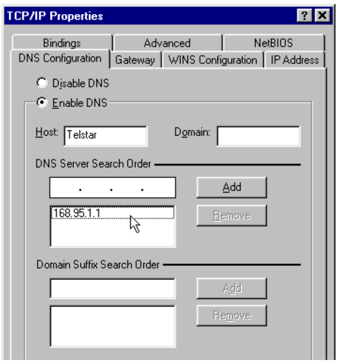
The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168. 1 . 1

Installed gateways: 192.168.1.1

d. Type the router's IP address in the "New gateway" field and click **Add.** The IP address appears under "Installed gateways."

e. Click **OK** and click the **DNS Configuration** tab to configure DNS settings:



○ Disable DNS
● Enable DNS

Host: Telstar Domain:

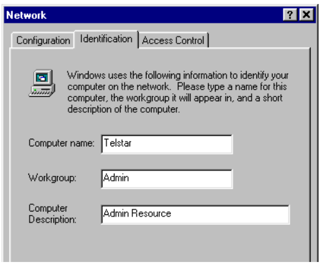
DNS Server Search Order
. . .
168.95.1.1

Domain Suffix Search Order

f. Click the radio button next to **Enable DNS**. Type the computer name in Host.

Note!

You can find the computer name by clicking the Identification Tab in the Network Configuration dialog:



Windows uses the following information to identify your computer on the network. Please type a name for this computer, the workgroup it will appear in, and a short description of the computer.

Computer name: Telstar

Workgroup: Admin

Computer Description: Admin Resource

g. Type the ISP/BSP domain name in the Domain text box. Type the ISP/BSP domain name server IP address in DNS Server Search Order and click **Add** to add it to the list.

Note!

Contact your ISP/BSP for the information.

An ISP (Internet Service Provider) or BSP (Broadband Service Provider) is an organization that provides users with Internet access via modem or cable/DSL modem.

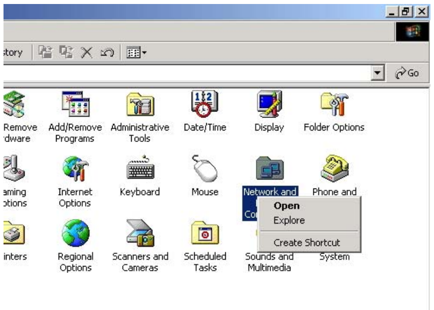
h. Click **OK**. You are returned to the Network configuration dialog box.

8. Click **OK**. Windows copies files and configures the Network settings. If prompted, insert your Windows setup CD or specify the path to your Windows setup files. After Windows has finished setting up the network, you are prompted to restart the computer.

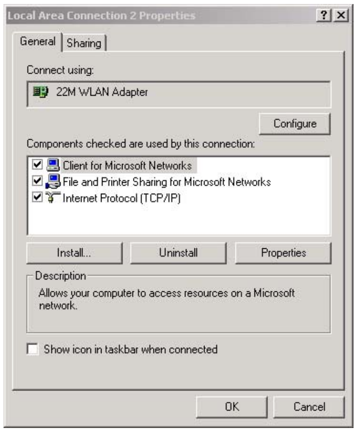
9. Restart the computer.

Windows 2000

1. Click **Start**, **Settings**, then click **Control Panel**. The Control Panel opens:



2. Right-click the **Network and Dial-up Connections** icon and select Open to open the Network and Dial-up configuration dialog.
3. Double-click Local Area Connection 2 to open the following dialog box:



Local Area Connection 2 Properties

General | Sharing

Connect using:

22M WLAN Adapter

Configure

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

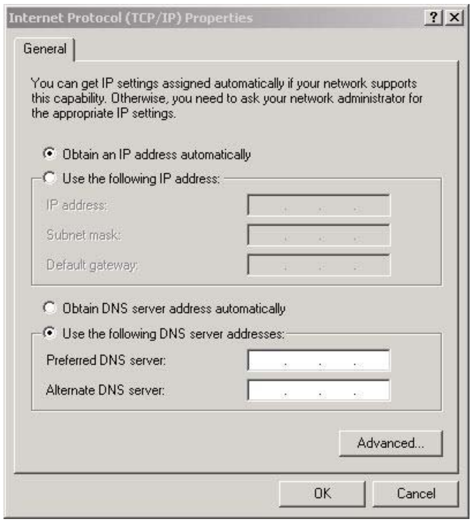
Description

Allows your computer to access resources on a Microsoft network.

☐ Show icon in taskbar when connected

OK | Cancel

4. Check the box next to Internet Protocol (TCP/IP) and click Properties:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

5. If you are going to use DHCP to IP assign settings, click the radio buttons next to “Obtain an IP address automatically” and “Obtain DNS server address automatically and go to step 6.

   If you want to assign a fixed IP address, follow these steps:

   a. In the TCP/IP Properties dialog box, click the radio button next to **Use the following IP address**:
   b. Enter an IP address in the IP field.

      In the example shown, all IP addresses from 211.231.181.100 to 211.231.181.254 are available for dynamic IP address assignment, while 211.231.181.2 to 211.231.181.99 are available as static IP addresses.
   c. Type a Subnet Mask value for the router.

d. Type the router's IP address in the "Default gateway" field.

e. Check the radio button next to "Use the following DNS server addresses" and type the ISP/BSP domain name server IP address.

Note!

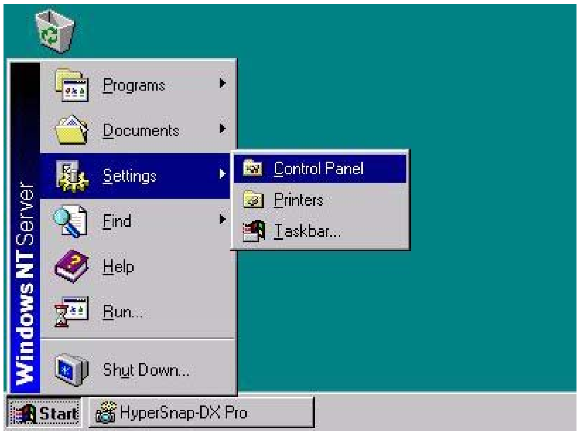
An ISP (Internet Service Provider) or BSP (Broadband Service Provider) is an organization that provides users with Internet access via modem or cable/DSL modem.

f. Click **OK**. You are returned to the Network configuration dialog box.

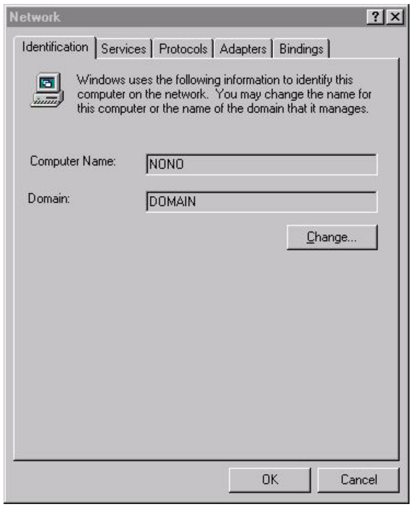
6. Click **OK** to apply the settings and exit the Network configuration dialog box.

Windows NT4.0

1. Click **Start**, **Settings**, then click **Control Panel**. The Control Panel opens:



2. Double-click the **Network** icon to view the Network configuration dialog:

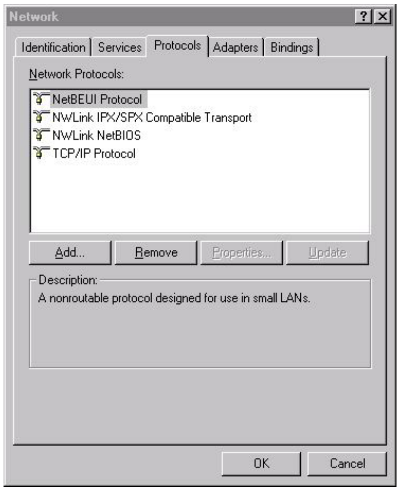


Windows uses the following information to identify this computer on the network. You may change the name for this computer or the name of the domain that it manages.

Computer Name: NONO

Domain: DOMAIN

3. Click the **Protocols** tab:

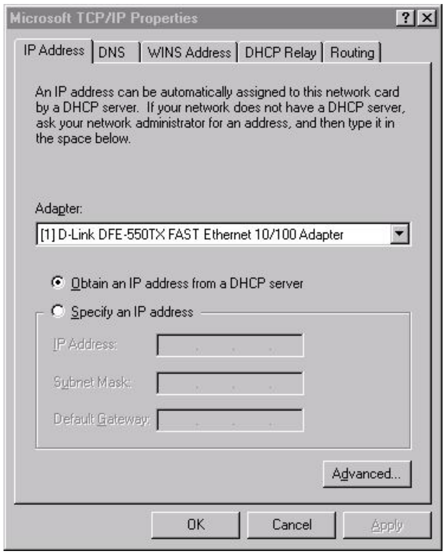


Network Protocols:

- NetBEUI Protocol
- NWLink IPX/SPX Compatible Transport
- NWLink NetBIOS
- TCP/IP Protocol

Description:
A nonroutable protocol designed for use in small LANs.

4. Select TCP/IP Protocol, and click **Properties**:

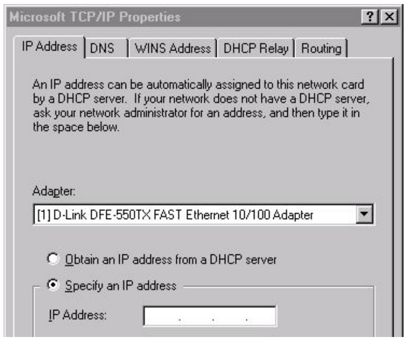


An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:
[1] D-Link DFE-550TX FAST Ethernet 10/100 Adapter

● Obtain an IP address from a DHCP server
○ Specify an IP address

5. If you are going to use DHCP to IP assign settings, click the radio buttons next to “Obtain an IP address from a DHCP server” and go to step 6.
   If you want to assign a fixed IP address, follow these steps:
   a. In the TCP/IP Properties dialog box, click the radio button next to **Specify an IP address**:



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

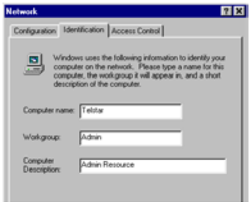
Adapter:
[1] D-Link DFE-550TX FAST Ethernet 10/100 Adapter

○ Obtain an IP address from a DHCP server
● Specify an IP address

   b. Enter an IP address in the IP field.
      In the example shown, all IP addresses from 211.231.181.100 to 211.231.181.254 are available for dynamic IP address assignment, while 211.231.181.2 to 211.231.181.99 are available as static IP addresses.
   c. Type a Subnet Mask value for the router. The default value is shown.
   d. Type the router’s IP address in the “Default gateway” field.
   e. Click the **DNS** tab and type the computer’s name in the Host name field.

Note!

You can find the computer name by clicking the Identification Tab in the Network Configuration dialog:



Windows uses the following information to identify your computer on the network. Please type a name for this computer, the workgroup it will appear in, and a short description of the computer.

Computer name: Telstar

Workgroup: Admin

Computer Description: Admin Resource

f. Type the ISP/BSP domain name server IP address in the Domain field.

Note!

Contact your ISP/BSP for the information.

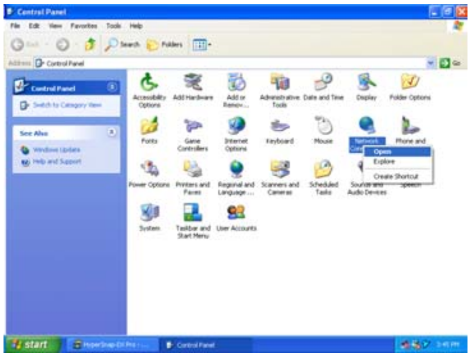
An ISP (Internet Service Provider) or BSP (Broadband Service Provider) is an organization that provides users with Internet access via modem or cable/DSL modem.

g. Click **OK**. You are returned to the Network configuration dialog box.

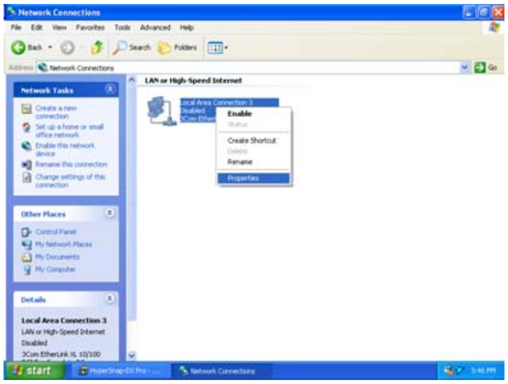
6. Click **OK** to apply the settings and exit the Network configuration dialog box. You are prompted to restart your computer.
7. Click **Yes** to restart the computer and finish the installation.

Windows XP

1. Click **Start**, **Settings**, then click **Control Panel**. The Control Panel opens:

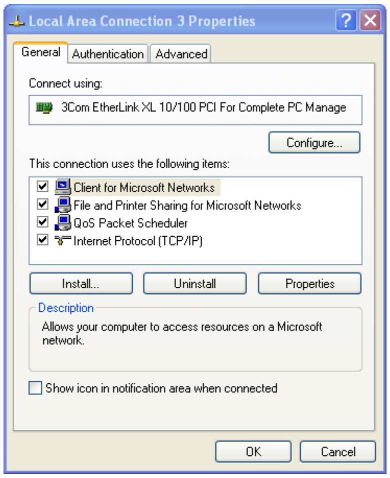


2. Right-click the **Network** icon and select Open to open the Network Connections dialog:



Local Area Connection 3
LAN or High-Speed Internet
Disabled
3Com EtherLink XL 10/100

3. Right-click the appropriate LAN connection and click Properties to open the properties dialog for the connection:



Connect using:

3Com EtherLink XL 10/100 PCI For Complete PC Manage

This connection uses the following items:

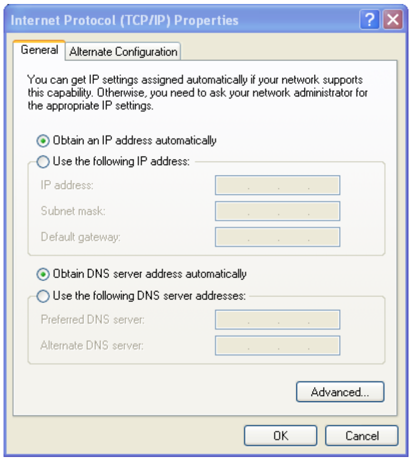
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

□ Show icon in notification area when connected

4. Check the box next to Internet Protocol (TCP/IP) and click Properties:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. If you are going to use DHCP to IP assign settings, click the radio buttons next to “Obtain an IP address automatically” and “Obtain DNS server address automatically and go to step 6.

   If you want to assign a fixed IP address, follow these steps:

   h. In the TCP/IP Properties dialog box, click the radio button next to **Use the following IP address**:

   i. Enter an IP address in the IP field.

      In the example shown, all IP addresses from 211.231.181.100 to 211.231.181.254 are available for dynamic IP address assignment, while 211.231.181.2 to 211.231.181.99 are available as static IP addresses.

   j. Type a Subnet Mask value for the router.

   k. Type the router’s IP address in the “Default gateway” field.

   l. Check the radio button next to “Use the following DNS server addresses” and type the ISP/BSP domain name server IP address.

Note!	*An ISP (Internet Service Provider) or BSP (Broadband Service Provider) is an organization that provides users with Internet access via modem or cable/DSL modem.*

   m. Click **OK**. You are returned to the Network configuration dialog box.

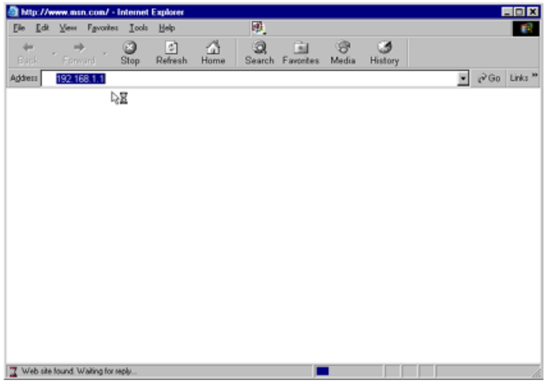
   n. Click **OK** to apply the settings and exit the Network configuration dialog box.

Starting the Web Browser Interface

- Refer to the following instructions for starting the Web browser interface.

Note!	*Before using the Web browser interface, be sure you have set up your computer's network configuration. Refer to page 13.*

1. Open your Web browser and type the router IP address in the address bar, the default is 192.168.1.1

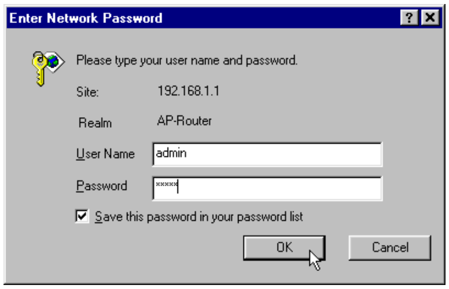


http://www.msn.com/ - Internet Explorer

Address: 192.168.1.1

Web site found. Waiting for reply...

2. Press <Enter>. You are prompted for the user name and password.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

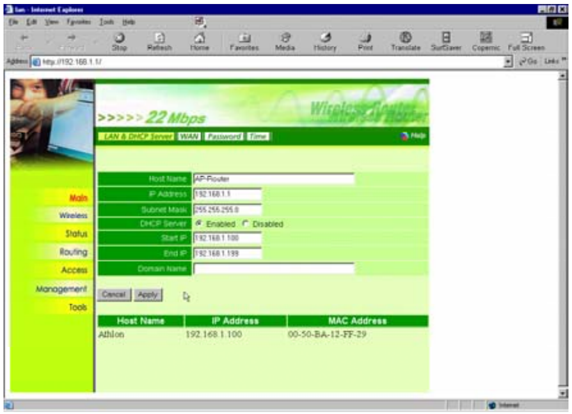
Realm AP-Router

User Name: admin

Password: *****

☑ Save this password in your password list

3. Type the user name and password in the appropriate fields. The default user name and password is "admin."
4. Click **OK**. The router browser interface opens:



lan - Internet Explorer

Address: http://192.168.1.1/

Host Name: AP-Router

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server: ● Enabled ○ Disabled

Start IP: 192.168.1.100

End IP: 192.168.1.199

Domain Name:

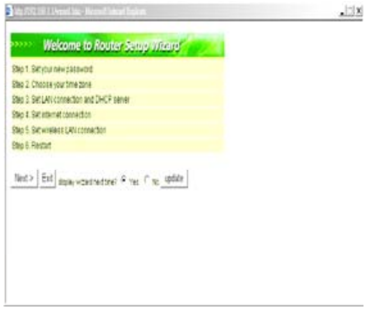
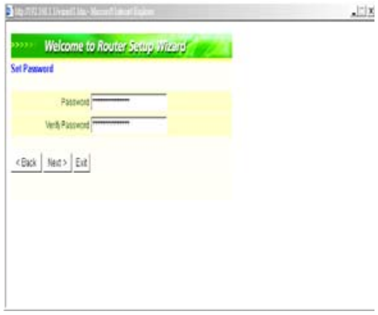
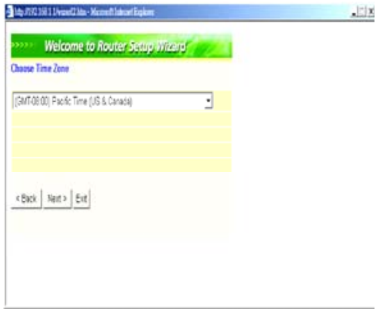
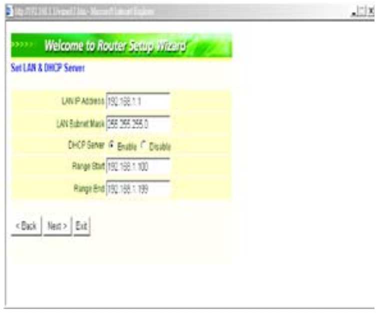
Host Name	IP Address	MAC Address
Athlon	192.168.1.100	00-50-BA-12-FF-29

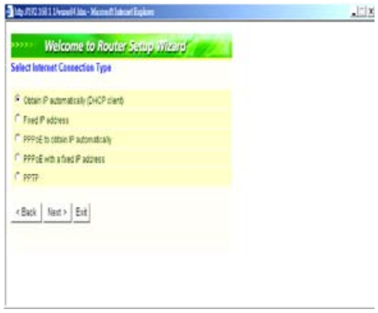
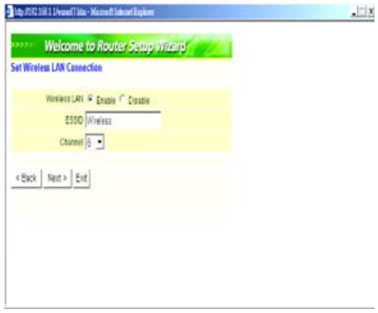
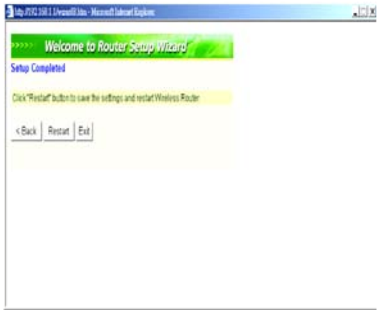
Using the browser interface, you can set network parameters, configure wireless LAN settings, view status reports and logs, create access restrictions, and use other tools and features.

Note!	*For information on using the browser interface, refer to the browser interface online help.*

Setup Wizard

The setup wizard enables you to configure the router quickly and conveniently. Follow these instructions:

1. Open the browser interface as described in the previous section. 2. In the Settings screen Setup Wizard page, click Run Wizard. The screen shown to the right appears.	 Welcome to Router Setup Wizard Step 1. Set your new password Step 2. Choose your time zone Step 3. Set LAN connection and DHCP server Step 4. Set internet connection Step 5. Set wireless LAN connection Step 6. Restart display wizard next time? ● Yes ○ No
3. Click **Next**. You are prompted to select a password. Type a password in the text box, and then type it again for verification.	 Welcome to Router Setup Wizard Set Password Password ************** Verify Password **************
4. Click **Next**. Select your time zone from the drop-down list.	 Welcome to Router Setup Wizard Choose Time Zone (GMT-08:00) Pacific Time (US & Canada)
5. Click **Next**. 6. Type the LAN IP address in the text box. The default IP address 192.168.1.1. 7. Type the subnet mask in the text box. 8. Enable DHCP Server if you want DHCP to automatically assign IP addresses. Type a beginning IP address and an end IP address for the DHCP server to use in assigning IP addresses.	 Welcome to Router Setup Wizard Set LAN & DHCP Server LAN IP Address 192.168.1.1 LAN Subnet Mask 255.255.255.0 DHCP Server ● Enable ○ Disable Range Start 192.168.1.100 Range End 192.168.1.199

9. Click **Next**. Select how the router will set up the Internet connection. If you have enabled DHCP server, choose "Obtain IP automatically (DHCP client)" to have the router assign IP addresses automatically.	 Welcome to Router Setup Wizard Select Internet Connection Type ● Obtain IP automatically (DHCP client) ○ Fixed IP address ○ PPPoE to obtain IP automatically ○ PPPoE with a fixed IP address ○ PPTP
10. Click to enable or disable wireless LAN. If you enable the wireless LAN, type the SSID in the text box and select a communications channel. The SSID and channel must be the same as wireless devices attempting communication to the router.	 Welcome to Router Setup Wizard Set Wireless LAN Connection Wireless LAN ● Enable ○ Disable SSID Wireless Channel 6
11. Click **Next**. You are prompted to restart save the settings and restart the router interface. Click **Restart** to complete the wizard.	 Welcome to Router Setup Wizard Setup Completed Click "Restart" button to save the settings and restart Wireless Router

This completes Chapter 3.

CHAPTER 4

Using the Interface

This chapter covers the router user interface functions, settings, and parameters.

Refer to the glossary in Appendix A for unfamiliar terms.

Main Screen

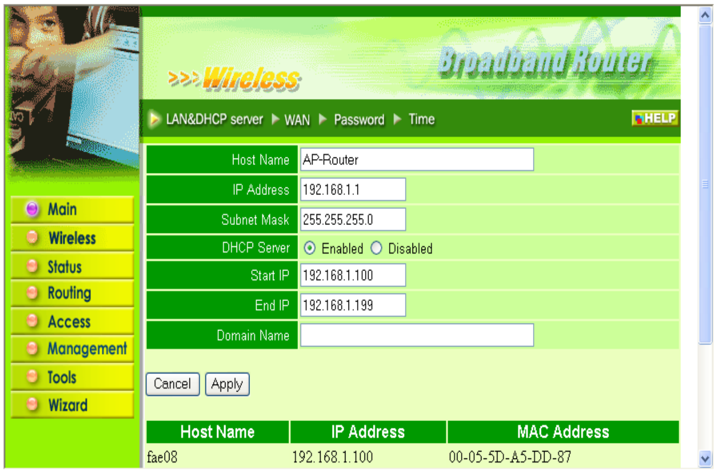
The main screen enables you to configure the LAN & DHCP Server, set WAN parameters, create Administrator and User passwords, and set the local time, time zone, and default NTP server.

The following functions are covered in this section:

- LAN & DHCP Server
- WAN
- Password
- Time

LAN & DHCP Server

This page enables you to set LAN and DHCP properties, such as the host name, IP address, subnet mask, and domain name. LAN and DHCP profiles are listed in the DHCP table at the bottom of the screen.



Host Name: AP-Router

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server: ● Enabled ○ Disabled

Start IP: 192.168.1.100

End IP: 192.168.1.199

Domain Name:

Host Name	IP Address	MAC Address
fae08	192.168.1.100	00-05-5D-A5-DD-87

Host Name: Type the host name in the text box. The host name is required by some ISPs. The default host name is 'AP-Router.'

IP Address: This is the IP address of the router. The default IP address is 192.168.1.1.

Subnet Mask: Type the subnet mask for the router in the text box. The default subnet mask is 255.255.255.0

DHCP Server: Enables the DHCP server to allow the router to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default.

All DHCP client computers are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of the client.

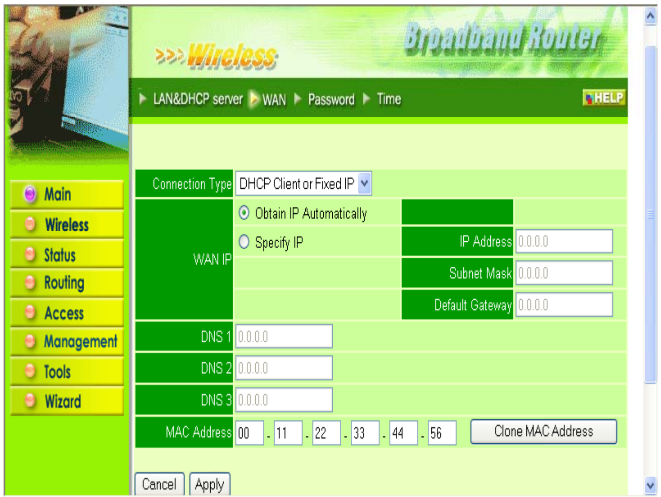
Start IP: Type an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

End IP: Type an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

Domain Name: Type the local domain name of the network in the text box. This item is optional.

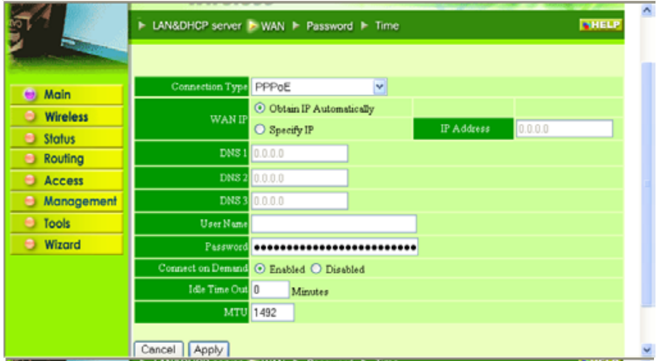
WAN

This screen enables you to set up the router WAN connection, specify the IP address for the WAN, add DNS numbers, enter the MAC address, and set the MTU.



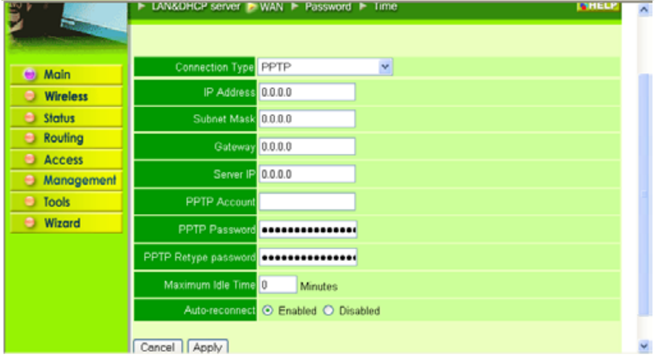
Connection Type	DHCP Client or Fixed IP		
WAN IP	● Obtain IP Automatically		
	○ Specify IP	IP Address	0.0.0.0
		Subnet Mask	0.0.0.0
		Default Gateway	0.0.0.0
DNS 1	0.0.0.0		
DNS 2	0.0.0.0		
DNS 3	0.0.0.0		
MAC Address	00 - 11 - 22 - 33 - 44 - 56	Clone MAC Address	

Cancel Apply



Connection Type	PPPoE		
WAN IP	● Obtain IP Automatically		
	○ Specify IP	IP Address	0.0.0.0
DNS 1	0.0.0.0		
DNS 2	0.0.0.0		
DNS 3	0.0.0.0		
User Name			
Password	●●●●●●●●●●●●●●●●●●●●●●●●●		
Connect on Demand	● Enabled ○ Disabled		
Idle Time Out	0 Minutes		
MTU	1492		

Cancel Apply



Connection Type	PPTP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Server IP	0.0.0.0
PPTP Account	
PPTP Password	●●●●●●●●●●●●●●●
PPTP Retype password	●●●●●●●●●●●●●●●
Maximum Idle Time	0 Minutes
Auto-reconnect	● Enabled ○ Disabled

Cancel Apply

Connection Type: Select the connection type, either DHCP client/Fixed IP or PPPoE from the drop-down list.

When using DHCP client/Fixed IP, enter the following information in the fields (some information is provided by your ISP):

WAN IP: Select whether you want to specify an IP address manually, or want DHCP to obtain an IP address automatically. When *Specify IP* is selected, type the IP address, subnet mask, and default gateway in the text boxes. Your ISP will provide you with this information.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. Your ISP will provide you with this information.

MAC Address: If required by your ISP, type the MAC address of the router WAN interface in this field.

MTU: Type the MTU value in the text box.

When using PPPoE, enter the following information in the fields (some information is provided by your ISP):

WAN IP: Select whether you want the ISP to provide the IP address automatically, or whether you want to assign a static IP address to the router WAN. When *Specify IP* is selected, type the PPPoE IP address in the text box. Your ISP will provide you with this information.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. Your ISP will provide you with this information.

User Name: Type your PPPoE user name.

Password: Type your PPPoE password.

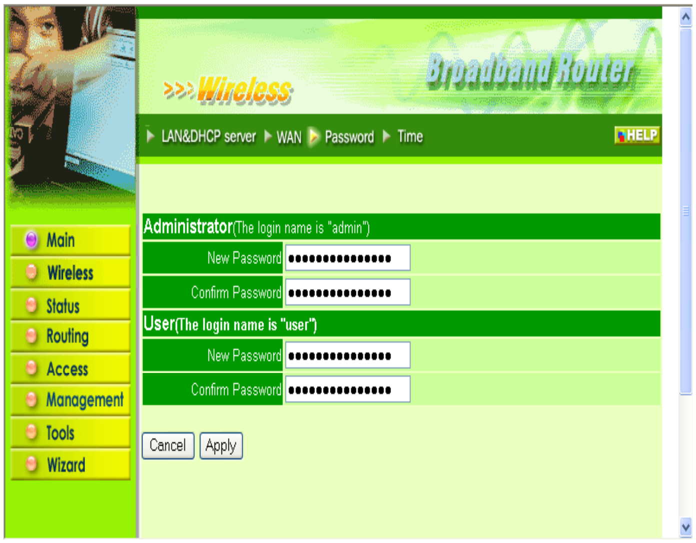
Connect on Demand: Enables or disables the connect on demand function, which enables the the router to initiate a connection with your ISP when an Internet request is made to the router. When enabled, the router automatically connects to the Internet when you open your default browser.

Idle Time Out: Specify the time that will elapse before the router times out of a connection.

MTU: Type the MTU value in the text box.

Password

This screen enables you to set administrative and user passwords. These passwords are used to gain access to the router interface.



Administrator(The login name is "admin")

New Password ••••••••••••••••

Confirm Password ••••••••••••••••

User(The login name is "user")

New Password ••••••••••••••••

Confirm Password ••••••••••••••••

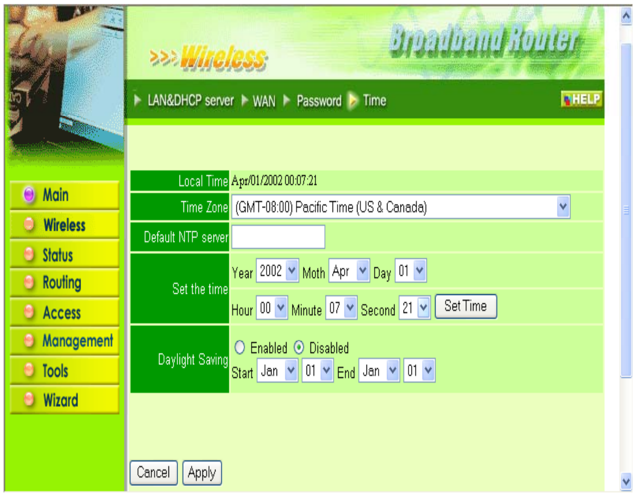
Administrator: Type the password the Administrator will use to log in to the system. The password must be typed again for confirmation.

User: Users can type a password to be used for logging in to the system. The password must be typed again for confirmation.

Note!	*Users do not have permission to configure router options.*

Time

This screen enables you to set the time and date for the router's realtime clock, select your time zone, specify an NTP server, and enable or disable daylight saving.



Local Time Apr/01/2002 00:07:21

Time Zone (GMT-08:00) Pacific Time (US & Canada)

Default NTP server

Set the time: Year 2002 Moth Apr Day 01; Hour 00 Minute 07 Second 21

Daylight Saving: ○ Enabled ● Disabled; Start Jan 01 End Jan 01

Local Time: Displays the local time and date.

Time Zone: Select your time zone from the drop-down list.

Default NTP Server: Type the NTP server address in the text box to enable the router to automatically set the time from the Internet NTP server.

Set the Time: Select the date and time from the drop-down lists, and click *Set Time* to set the router's internal clock to the correct date and time.

Daylight Saving: Enables you to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

Wireless

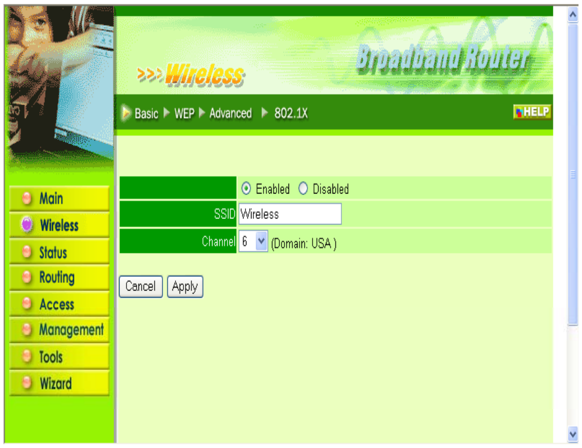
This page enables you to set wireless communications parameters for the router's wireless LAN feature.

The following functions are covered in this section:

- Basic
- WEP
- Advanced

Basic

This page enables you to enable and disable the wireless LAN function, enter a SSID, and set the channel for wireless communications.



● Enabled ○ Disabled

SSID: Wireless

Channel: 6 (Domain: USA)

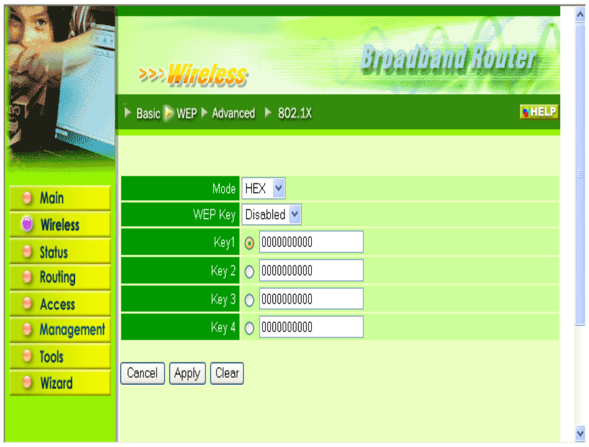
Enable/Disable: Enables and disables wireless LAN via the router.

SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the router.

Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the router.

WEP

This screen enables you to set WEP parameters for secure wireless communications.



Mode: HEX

WEP Key: Disabled

Key1 ● 0000000000

Key 2 ○ 0000000000

Key 3 ○ 0000000000

Key 4 ○ 0000000000

Mode: Select the level of encryption you want from the drop-down list. The router supports, 64-, 128-, and 256-bit encryption.

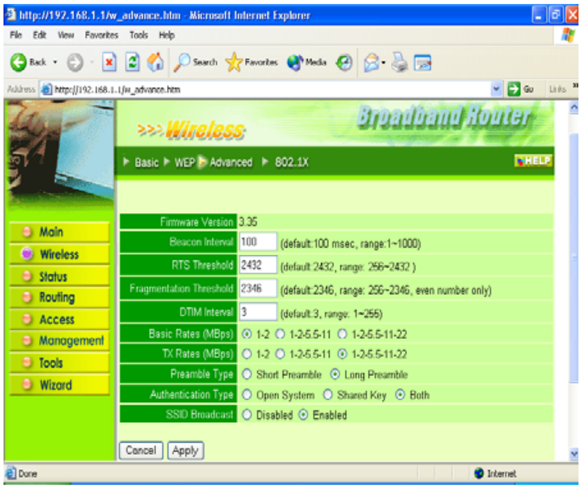
WEP Key: Select WEP Key, 64, 128 or 256 bit from the drop-down list.

Key 1 ~ Key 4: Enables you to create an encryption scheme for Wireless LAN transmissions. Manually enter a set of values for each key. Select which key you want to use by clicking the radio button next to the key. Click **Clear** to erase key values.

Note!	*256- and 128-bit encryption require more system resources than 64-bit encryption. Use 64-bit encryption for better performance.*

Advanced

This screen enables you to configure advanced wireless functions.


http://192.168.1.1/w_advance.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/w_advance.htm
Go Links
>>> Wireless
Broadband Router
Basic WEP Advanced 802.1X
HELP
Main
Wireless
Status
Routing
Access
Management
Tools
Wizard
Cancel
Apply
Done
Internet

Firmware Version	3.35
Beacon Interval	100 (default:100 msec, range:1~1000)
RTS Threshold	2432 (default:2432, range: 256~2432)
Fragmentation Threshold	2346 (default:2346, range: 256~2346, even number only)
DTIM Interval	3 (default:3, range: 1~255)
Basic Rates (MBps)	● 1-2 ○ 1-2-5.5-11 ○ 1-2-5.5-11-22
TX Rates (MBps)	○ 1-2 ○ 1-2-5.5-11 ● 1-2-5.5-11-22
Preamble Type	○ Short Preamble ● Long Preamble
Authentication Type	○ Open System ○ Shared Key ● Both
SSID Broadcast	○ Disabled ● Enabled

Firmware Version: Displays the wireless function firmware version. The wireless firmware is updated when you update the router firmware.

Beacon Interval: Type the beacon interval in the text box. You can specify a value from 1 to 1000. The default beacon interval is 100.

RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2432 until data flow is normalized.

Fragmentation Threshold: Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 256 and 2432 until packet transfer rates are minimized.

Note!	***Note:** Setting the fragmentation threshold value may diminish system performance.*

DTIM Interval: Type a DTIM (Delivery Traffic Indication Message) interval in the text box. You can specify a value between 1 and 65535. The default value is 3.

Basic Rates (MBps): Select one of the wireless LAN receive rates, measured in megabytes per second.

TX Rates (MBps): Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

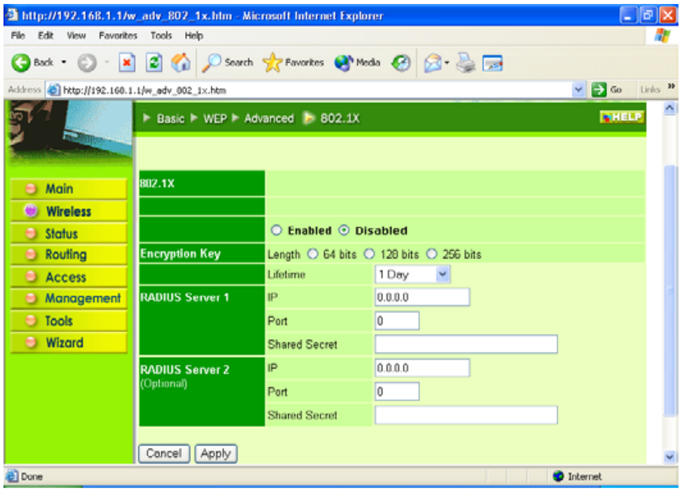
Preamble Type: Select either a short preamble or long preamble. Select a short preamble for WLANs with high network traffic; select a long preamble when the network traffic is low.

Authentication Type: Select the authentication type. Open System allows public access to the router via wireless communications.

Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key.

802.1x

There are three essential components to the 802.1x infrastructure: (1) Supplicant, (2) Authenticator and (3) Server. The Router serves as an Authenticator, and the EAP methods used must be supported by the backend Radius Server. The 802.1x security supports both MD5 and TLS Extensive Authentication Protocol (EAP). Please follow the steps below to configure 802.1x security.


http://192.168.1.1/w_adv_802_1x.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/w_adv_802_1x.htm Go Links
Basic WEP Advanced 802.1X
HELP
Main
Wireless
Status
Routing
Access
Management
Tools
Wizard
Cancel
Apply
Done
Internet

802.1X

○ Enabled ● Disabled

Encryption Key: Length ○ 64 bits ○ 128 bits ○ 256 bits

Lifetime: 1 Day

RADIUS Server 1: IP 0.0.0.0; Port 0; Shared Secret

RADIUS Server 2 (Optional): IP 0.0.0.0; Port 0; Shared Secret

1. Enable 802.1x security by selecting “**Enable**”.
2. Select the **Encryption Key Length Size** ranging from 64 to 256 Bits that you would like to use.

   Select the **Lifetime of the Encryption Key** from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.
3. Enter the **IP address** of and the **Port** used by the **Primary** Radius Server

   Enter the **Shared Secret**, which is used by the Radius Server.
4. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.

   Click “**Help**” to get interpretation for Encryption Key and Radius Server

5. Click “**Apply**” button for the 802.1x settings to take effect after Access Point reboots itself.

Note! As soon as 802.1x security is enabled, all the wireless client stations that are connected to the Router currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.

Status

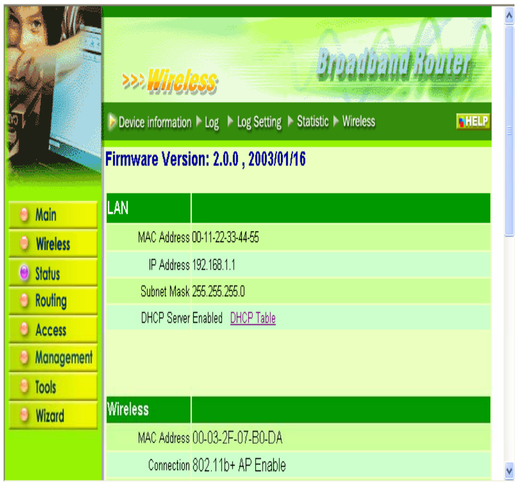
This screen enables you to view the status of the router LAN, WAN and wireless LAN connections, and view logs and statistics pertaining to connections and packet transfers.

The following functions are covered in this section:

- Device Information
- Log
- Log Settings
- Statistics
- Wireless

Device Information

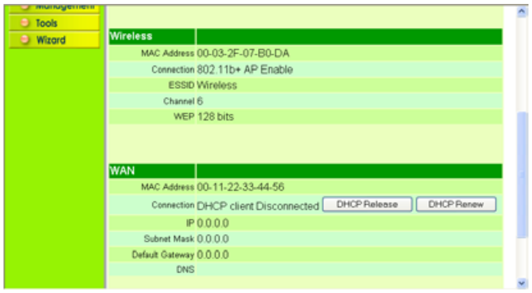
This screen enables you to view the router LAN, wireless LAN, and WAN configuration.



Firmware Version: 2.0.0 , 2003/01/16

LAN	
MAC Address	00-11-22-33-44-55
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled DHCP Table

Wireless	
MAC Address	00-03-2F-07-B0-DA
Connection	802.11b+ AP Enable



Wireless	
MAC Address	00-03-2F-07-B0-DA
Connection	802.11b+ AP Enable
ESSID	Wireless
Channel	6
WEP	128 bits

WAN	
MAC Address	00-11-22-33-44-56
Connection	DHCP client Disconnected
IP	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS	

Firmware Version: Displays the latest build of the wireless router firmware interface. After updating the firmware in Tools - Firmware, check this to ensure that your firmware was successfully updated.

LAN: This field displays the router's LAN interface MAC address, IP address, subnet mask, and DHCP server status. Click *DHCP Table* to view a list of client stations currently connected to the router LAN interface.

Wireless: Displays the router's wireless connection information, including the router's wireless interface MAC address, the connection status, the SSID status, which channel is being used, and whether WEP is enabled or not.

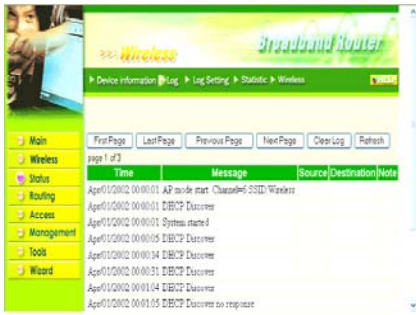
WAN: This field displays the router's WAN interface MAC address, DHCP client status, IP address, subnet mask, default gateway, and DNS.

Click *DHCP Release* to release all IP addresses assigned to client stations connected to the WAN via the router. Click *DHCP Renew* to reassign IP addresses to client stations connected to the WAN.

Log

This screen enables you to view a running log of router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries. You can save logs via the Log Settings screen (Send to). The Log screen commands are as follows:

- Click *First Page* to view the first page of the log
- Click *Last Page* to view the final page of the log
- Click *Previous Page* to view the page just before the current page
- Click *Next Page* to view the page just after the current page
- Click *Clear Log* to delete the contents of the log and begin a new log
- Click *Refresh* to renew log statistics



page 1 of 3

Time	Message	Source	Destination	Note
Apr/01/2002 00:00:01	AP mode start. Channel=6 SSID:Wireless			
Apr/01/2002 00:00:01	DHCP Discover			
Apr/01/2002 00:00:01	System started			
Apr/01/2002 00:00:05	DHCP Discover			
Apr/01/2002 00:00:14	DHCP Discover			
Apr/01/2002 00:00:31	DHCP Discover			
Apr/01/2002 00:01:04	DHCP Discover			
Apr/01/2002 00:01:05	DHCP Discover no response			

Time: Displays the time and date that the log entry was created.

Message: Displays summary information about the log entry.

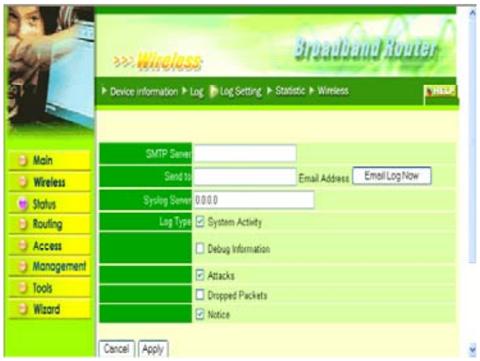
Source: Displays the source of the communication.

Destination: Displays the destination of the communication.

Note: Displays the IP address of the communication.

Log Settings

This screen enables you to set router logging parameters.



SMTP Server

Send to Email Address

Syslog Server 0.0.0.0

Log Type ☑ System Activity

□ Debug Information

☑ Attacks

□ Dropped Packets

☑ Notice

SMTP Server: Type the SMTP server address for the email that the log will be sent to in the next field.

Send to: Type an email address for the log to be sent to. Click *Email Log Now* to immediately send the current log.

Syslog Server: Type the IP address of the Syslog Server if you want the router to listen and receive incoming SysLog messages.

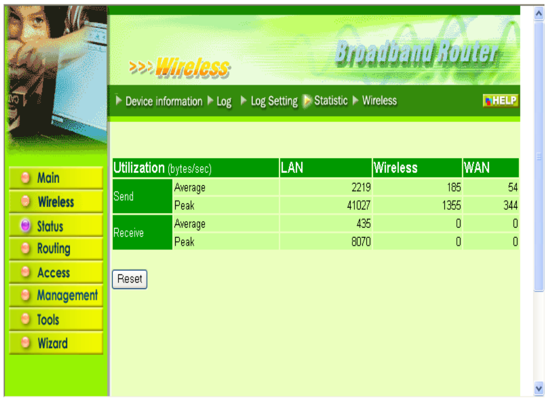
Log Type: Enables you to select what items will be included in the log:

- **System Activity:** Displays information related to router operation.
- **Debug Information:** Displays information related to errors and system malfunction.
- **Attacks:** Displays information about any malicious activity on the network.
- **Dropped Packets:** Displays information about packets that have not been transferred successfully.
- **Notice:** Displays important notices by the system administrator.

Statistic

This screen displays a table that shows the rate of packet transmission via the router LAN, wireless LAN, and WAN ports (in bytes per second).

Click *Reset* to erase all statistics and begin logging statistics again.

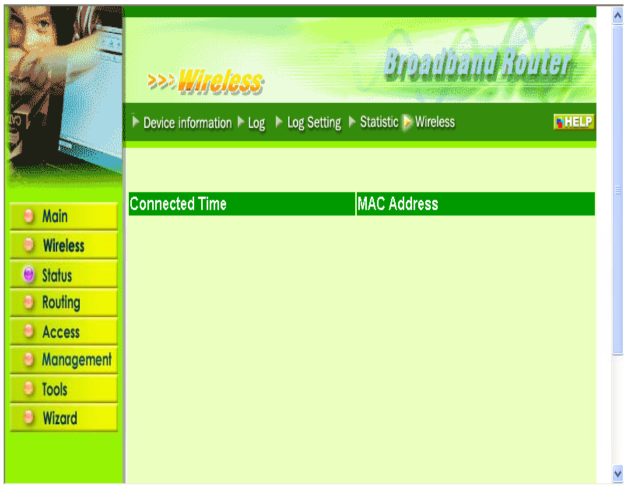


Utilization (bytes/sec)		LAN	Wireless	WAN
Send	Average	2219	185	54
	Peak	41027	1355	344
Receive	Average	435	0	0
	Peak	8070	0	0

Utilization: Separates packet transmission statistics into send and receive categories. Peak indicates the maximum packet transmission recorded since logging began, while Average indicates the average of the total packet transmission since recording began.

Wireless

This screen enables you to view information about wireless devices that are connected to the router wireless interface.



Connected Time	MAC Address

Connected Time: Displays how long the wireless device has been connected to the LAN via the router.

MAC Address: Displays the devices wireless LAN interface MAC address.

Routing

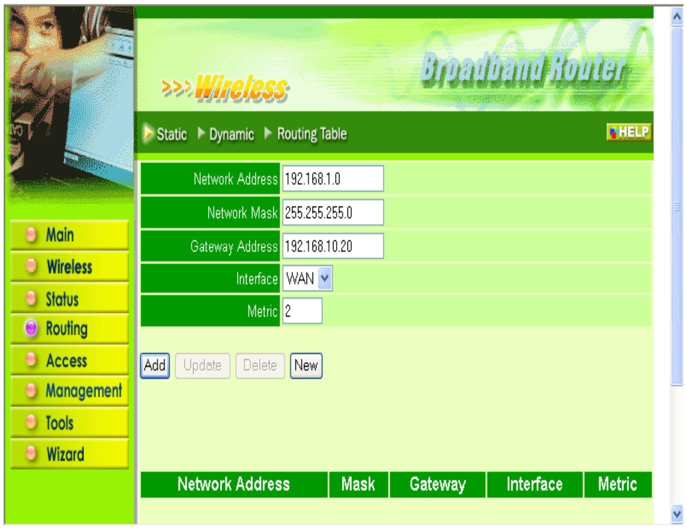
This page enables you to set how the router forwards data.

The following functions are covered in this section:

- Static
- Dynamic
- Routing Table

Static

This screen enables you to set parameters by which the router forwards data to its destination if your network has a static IP address.



Network Address 192.168.1.0

Network Mask 255.255.255.0

Gateway Address 192.168.10.20

Interface WAN

Metric 2

Network Address	Mask	Gateway	Interface	Metric

Network Address: Type the static IP address your network uses to access the Internet. Your ISP or network administrator provides you with this information.

Network Mask: Type the network (subnet) mask for your network. If you do not type a value here, the network mask defaults to 255.255.255.255. Your ISP or network administrator provides you with this information.

Gateway Address: Type the gateway address for your network. Your ISP or network administrator provides you with this information.

Interface: Select which interface, WAN or LAN, you use to connect to the Internet.

Metric: Select which metric you want to apply to this configuration.

Add: Click to add the configuration to the static IP address table at the bottom of the page.

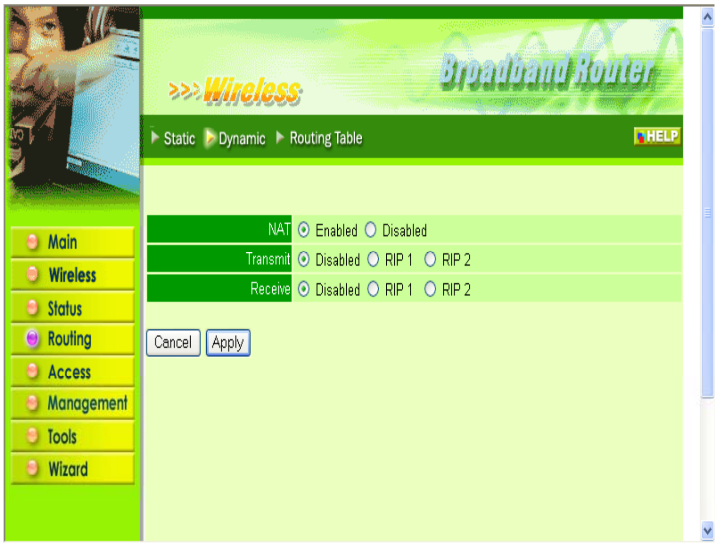
Update: Select one of the entries in the static IP address table at the bottom of the page and, after changing parameters, click *Update* to confirm the changes.

Delete: Select one of the entries in the static IP address table at the bottom of the page and click *Delete* to remove the entry.

New: Click *New* to clear the text boxes and add required information to create a new entry.

Dynamic

This screen enables you to set up NAT parameters.



NAT ● Enabled ○ Disabled

Transmit ● Disabled ○ RIP 1 ○ RIP 2

Receive ● Disabled ○ RIP 1 ○ RIP 2

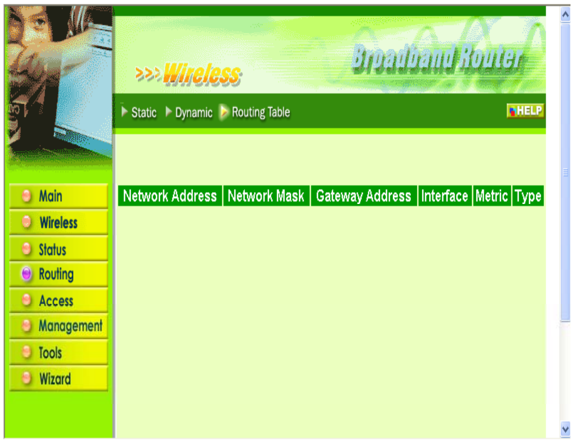
NAT: Click the radio buttons to enable or disable NAT.

Transmit: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1 or RIP 2.

Receive: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1 or RIP 2.

Routing Table

This screen enables you to view the routing table for the router. The routing table is a database created by the router that displays the network interconnection topology.



Network Address	Network Mask	Gateway Address	Interface	Metric	Type

Network Address: Displays the network IP address of the connected node.

Network Mask: Displays the network (subnet) mask of the connected node.

Gateway Address: Displays the gateway address of the connected node.

Interface: Displays whether the node is connected via a WAN or LAN.

Metric: Displays the metric of the connected node.

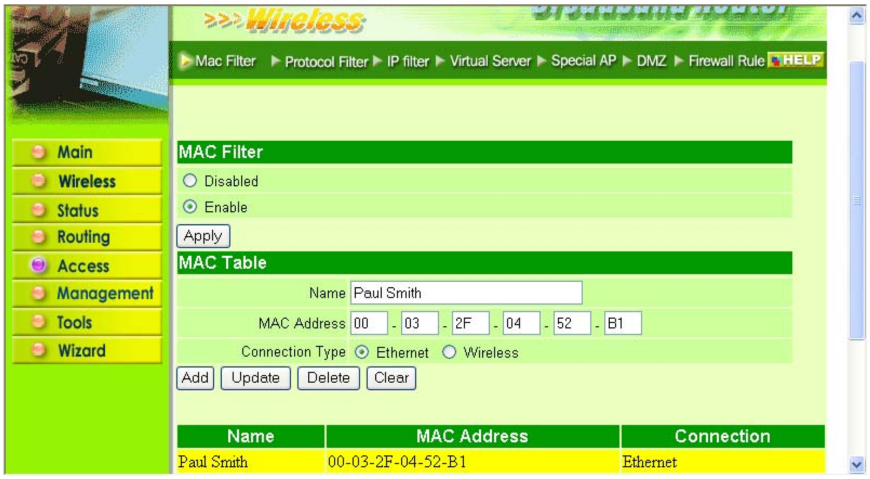
Type: Displays whether the node has a static or dynamic IP address.

Access

This page enables you to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

The following functions are covered in this section:

- MAC Filter
- Protocol Filter
- IP Filter
- Virtual Server
- Special AP
- DMZ
- Firewall Rule



MAC Filter

○ Disabled
● Enable

MAC Table

Name: Paul Smith

MAC Address: 00 - 03 - 2F - 04 - 52 - B1

Connection Type: ● Ethernet ○ Wireless

Name	MAC Address	Connection
Paul Smith	00-03-2F-04-52-B1	Ethernet

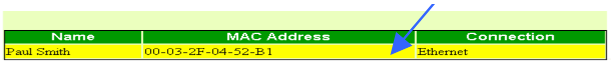
MAC Filter: Enables you to allow or deny Internet access to users within the LAN based upon the MAC address of their network interface. Click the radio button next to *Disabled* to disable the MAC filter.

- **Enable:** All users are allowed Internet access except those users you have assigned to groups 1 to 4 in the User Table are allowed Internet access.
- **Disable:** All users in all groups except for those you have assigned to Deny in the User Table are allowed Internet access.

MAC Table: Use this section to create a user profile to which Internet access is denied or allowed.

The user profiles are listed in the table at the bottom of the page.

> Note!
>
> *When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:*

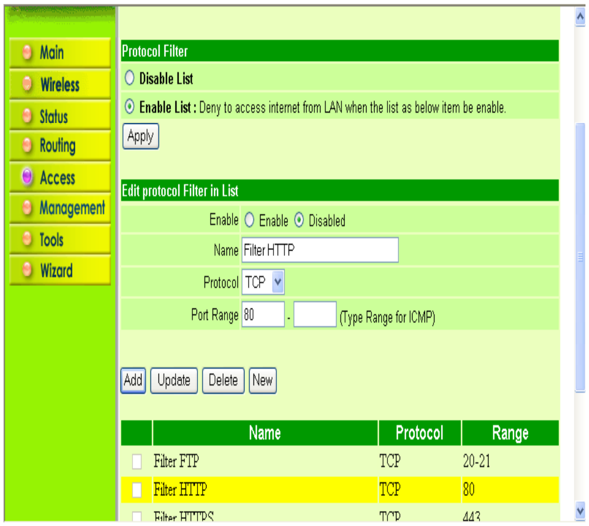


Name	MAC Address	Connection
Paul Smith	00-03-2F-04-52-B1	Ethernet

- **Name:** Type the name of the user to be permitted/denied access.
- **MAC Address:** Type the MAC address of the user's network interface.
- **Connection Type:** Select whether the user's access is via a wired Ethernet, or a wireless LAN connection.
- **Group:** Select a group from the drop-down list to apply this user to.
- **Add:** Click to add the user to the list at the bottom of the page.
- **Update:** Click to update information for the user, if you have changed any of the fields.
- **Delete:** Select a user from the table at the bottom of the list and click *Delete* to remove the user profile.
- **New:** Click *New* to erase all fields and enter new information.

Protocol Filter

This screen enables you to allow and deny access based upon a communications protocol list you create.



Protocol Filter

○ Disable List

● Enable List : Deny to access internet from LAN when the list as below item be enable.

Apply

Edit protocol Filter in List

Enable ○ Enable ● Disabled

Name Filter HTTP

Protocol TCP

Port Range 80 - (Type Range for ICMP)

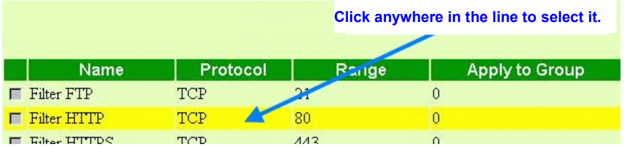
Add Update Delete New

	Name	Protocol	Range
□	Filter FTP	TCP	20-21
□	Filter HTTP	TCP	80
□	Filter HTTPS	TCP	443

The protocol filter profiles are listed in the table at the bottom of the page.

Note!

When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:



Click anywhere in the line to select it.

	Name	Protocol	Range	Apply to Group
□	Filter FTP	TCP	21	0
□	Filter HTTP	TCP	80	0
□	Filter HTTPS	TCP	443	0

Protocol Filter: Enables you to allow or deny Internet access to users based upon the communications protocol of the origin. Click the radio button next to *Disabled* to disable the protocol filter.

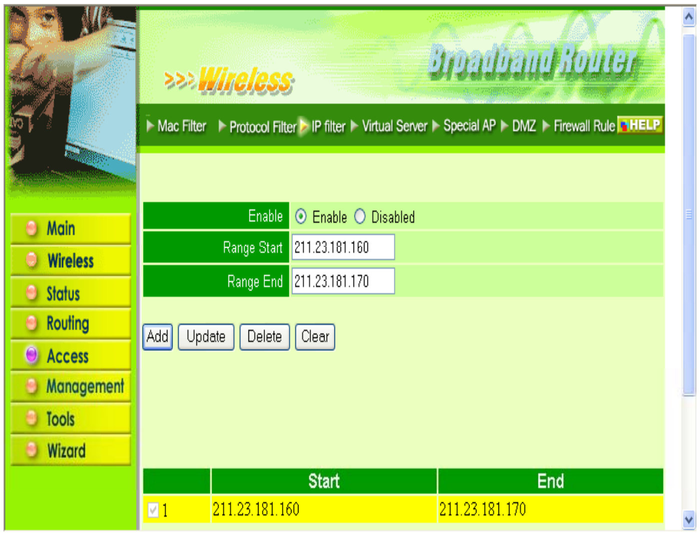
- **Allow:** All protocols in the list are allowed to connect to the Internet via the LAN. (Create list items in section under 'Add Protocol Filter.)
- **Deny:** All protocols in the list are not allowed to connect to the Internet via the LAN. (Create list items in section under 'Add Protocol Filter.)

Add Protocol Filter: Use this section to create a profile for the protocol you want to permit or deny Internet access.

- **Enable:** Click to enable or disable the protocol filter.
- **Name:** Type a descriptive name for the protocol filter.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) you want to allow/deny Internet access to from the drop-down list.
- **Port Range:** If you are creating a profile for ICMP, type a minimum and maximum port range in the two text boxes.
- **Apply to Group:** Select which user group you want to apply the profile to. You define the user groups in the User Group screen.
- **Add:** Click to add the protocol filter to the list at the bottom of the page.
- **Update:** Click to update information for the protocol filter, if you have changed any of the fields.
- **Delete:** Select a filter profile from the table at the bottom of the list and click *Delete* to remove the profile.
- **New:** Click *New* to erase all fields and enter new information.

IP Filter

This screen enables you to define a minimum and maximum IP address range filter; all IP addresses falling in the range are not allowed Internet access.



Enable: ● Enable ○ Disabled

Range Start: 211.23.181.160

Range End: 211.23.181.170

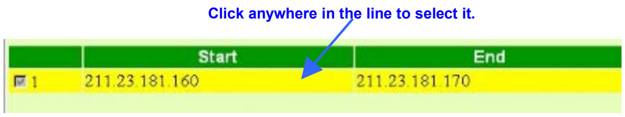
Add | Update | Delete | Clear

	Start	End
☑ 1	211.23.181.160	211.23.181.170

The IP filter profiles are listed in the table at the bottom of the page.

Note!

When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:



Click anywhere in the line to select it.

	Start	End
☑ 1	211.23.181.160	211.23.181.170

Enable: Click to enable or disable the IP address filter.

Range Start: Type the minimum address for the IP range. IP addresses falling between this value and the Range End are not allowed to access the Internet.

Range End: Type the minimum address for the IP range. IP addresses falling between this value and the Range Start are not allowed to access the Internet.

Add: Click to add the IP range to the table at the bottom of the screen.

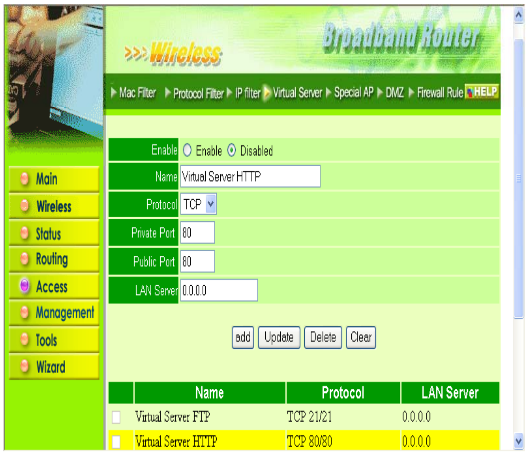
Update: Click to update information for the range if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

Clear: Click Clear to erase all fields and enter new information.

Virtual Server

This screen enables you to create a virtual server via the router. If the router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The router re-directs the request via the protocol and port numbers to the correct LAN server.



Enable ○ Enable ● Disabled

Name: Virtual Server HTTP

Protocol: TCP

Private Port: 80

Public Port: 80

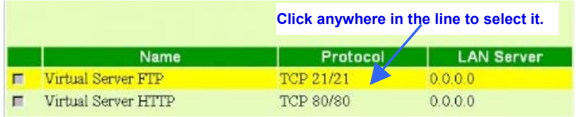
LAN Server: 0.0.0.0

	Name	Protocol	LAN Server
□	Virtual Server FTP	TCP 21/21	0.0.0.0
□	Virtual Server HTTP	TCP 80/80	0.0.0.0

The Virtual Sever profiles are listed in the table at the bottom of the page.

Note!

When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:



	Name	Protocol	LAN Server
□	Virtual Server FTP	TCP 21/21	0.0.0.0
□	Virtual Server HTTP	TCP 80/80	0.0.0.0

Enable: Click to enable or disable the virtual server.

Name: Type a descriptive name for the virtual server.

Protocol: Select the protocol (TCP or UDP) you want to use for the virtual server.

Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.

Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.

LAN Server: Type the LAN IP address that will be assigned to the virtual server.

Add: Click to add the virtual server to the table at the bottom of the screen.

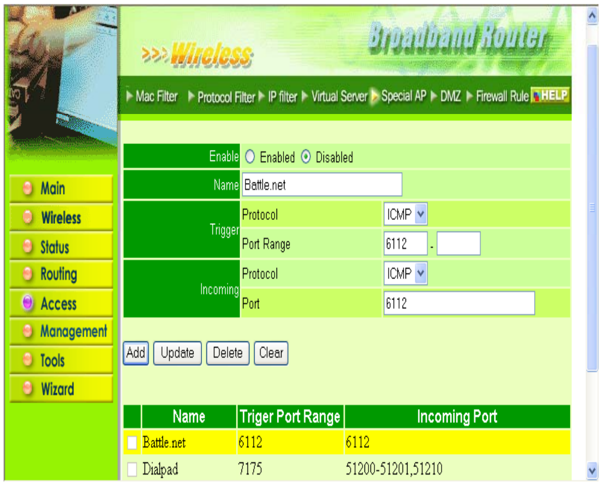
Update: Click to update information for the virtual server if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

Clear: Click Clear to erase all fields and enter new information.

Special AP

This screen enables you to specify special applications, such as games that require multiple connections that are inhibited by NAT.



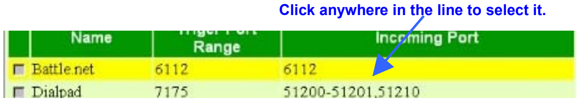
Enable	○ Enabled ● Disabled	
Name	Battle.net	
Trigger	Protocol	ICMP
	Port Range	6112 -
Incoming	Protocol	ICMP
	Port	6112

Name	Triger Port Range	Incoming Port
□ Battle.net	6112	6112
□ Dialpad	7175	51200-51201,51210

The special applications profiles are listed in the table at the bottom of the page.

Note!

When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:


Click anywhere in the line to select it.

Name	Triger Port Range	Incoming Port
□ Battle.net	6112	6112
□ Dialpad	7175	51200-51201,51210

Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the router WAN connection. Click Disabled on a profile to prevent users from accessing the application on the WAN.

Name: Type a descriptive name for the application.

Trigger: Defines the outgoing communication that determines whether the user has legitimate access to the application.

- **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used to access the application.
- **Port Range:** Type the port range that can be used to access the application in the text boxes.

Incoming: Defines which incoming communications users are permitted to connect with.

- **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used by the incoming communication.
- **Port:** Type the port number that can be used for the incoming communication.

Add: Click to add the special application profile to the table at the bottom of the screen.

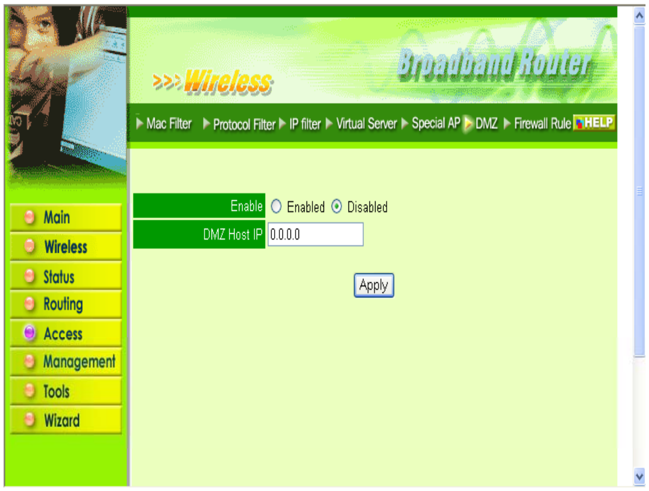
Update: Click to update information for the special application if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

Clear: Click Clear to erase all fields and enter new information.

DMZ

This screen enables you to create a DMZ for those computers that cannot access Internet applications properly through the router and associated security settings.



Enable ○ Enabled ● Disabled

DMZ Host IP 0.0.0.0

Enable: Click to enable or disable the DMZ.

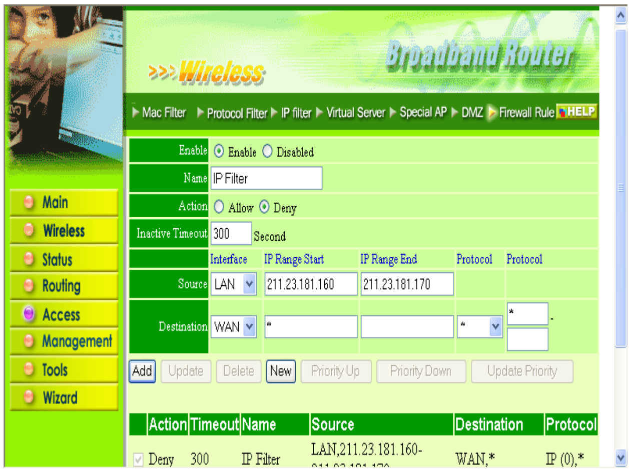
DMZ Host IP: Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

Note!	*Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.*

Apply: Click to save the settings.

Firewall Rule

This screen enables you to set up the firewall. The router provides basic firewall functions, by filtering all the packets that enter the router using a set of rules. The rules are in an order sequence list--the lower the rule number, the higher the priority the rule has.



Enable ● Enable ○ Disabled

Name IP Filter

Action ○ Allow ● Deny

Inactive Timeout 300 Second

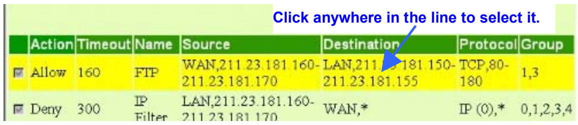
	Interface	IP Range Start	IP Range End	Protocol	Protocol
Source	LAN	211.23.181.160	211.23.181.170		
Destination	WAN	*		*	* -

	Action	Timeout	Name	Source	Destination	Protocol
☑	Deny	300	IP Filter	LAN,211.23.181.160-	WAN,*	IP (0),*

The rule profiles are listed in the table at the bottom of the page.

Note!

When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:



Click anywhere in the line to select it.

	Action	Timeout	Name	Source	Destination	Protocol	Group
☑	Allow	160	FTP	WAN,211.23.181.160-211.23.181.170	LAN,211.23.181.150-211.23.181.155	TCP,80-180	1,3
☑	Deny	300	IP Filter	LAN,211.23.181.160-211.23.181.170	WAN,*	IP (0),*	0,1,2,3,4

Enable: Click to enable or disable the firewall rule profile.

Name: Type a descriptive name for the firewall rule profile.

Action: Select whether to allow or deny packets that conform to the rule.

Inactive Timeout: Type the number of seconds of network inactivity that elapse before the router refuses the incoming packet.

Source: Defines the source of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.

Destination: Defines the destination of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.
- **Port Range:** Select the port range.

Add: Click to add the rule profile to the table at the bottom of the screen.

Update: Click to update information for the rule if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

New: Click *New* to erase all fields and enter new information.

Priority Up: Select a rule from the list and click *Priority Up* to increase the priority of the rule.

Priority Down: Select a rule from the list and click *Priority Down* to decrease the priority of the rule.

Update Priority: After increasing or decreasing the priority of a rule, click *Update Priority* to save the changes.

Management

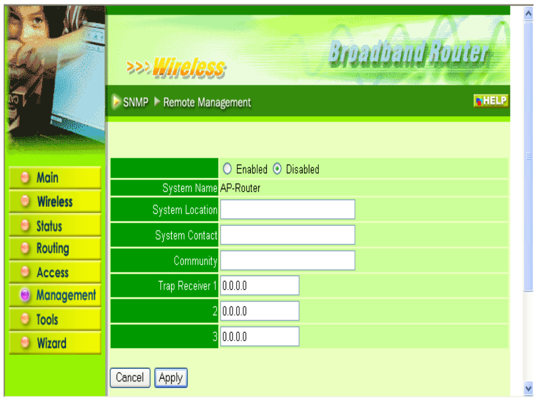
This screen enables you to set up SNMP and remote management features.

The following functions are covered in this section:

- SNMP
- Remote Management

SNMP

This screen enables you to configure SNMP.



	○ Enabled ● Disabled
System Name	AP-Router
System Location	
System Contact	
Community	
Trap Receiver 1	0.0.0.0
2	0.0.0.0
3	0.0.0.0

Enabled/Disabled: Click to enable or disable SNMP.

System Name: Displays the name given to the router.

System Location: Displays the location of the router (normally, the DNS name).

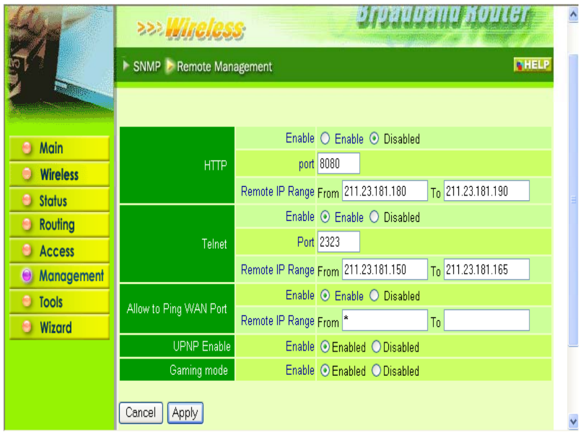
System Contact: Displays the contact information for the person responsible for the router.

Community: SNMP system name for exchanging SNMP community messages. The name can be used to limit SNMP messages passing through the network. The default name is 'public.'

Trap Receiver: Type the name of the destination PC that will receive trap messages.

Remote Management

This screen enables you to set up remote management. Using remote management, the router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.



HTTP	Enable	○ Enable ● Disabled
	port	8080
	Remote IP Range	From 211.23.181.180 To 211.23.181.190
Telnet	Enable	● Enable ○ Disabled
	Port	2323
	Remote IP Range	From 211.23.181.150 To 211.23.181.165
Allow to Ping WAN Port	Enable	● Enable ○ Disabled
	Remote IP Range	From * To
UPNP Enable	Enable	● Enabled ○ Disabled
Gaming mode	Enable	● Enabled ○ Disabled

HTTP: Enables you to set up HTTP access for remote management.

- **Enable:** Click to enable or disable HTTP access for remote management.
- **Remote IP Range:** Type the range of IP addresses that can be used for remote access.

Telnet: Enables you to set up Telnet access for remote management.

- **Enable:** Click to enable or disable Telnet access for remote management.
- **Remote IP Range:** Type the range of IP addresses that can be used for remote access.

Allow to Ping WAN Port: Type a range of router IP addresses that can be pinged from remote locations.

UPNP Enable: Click to enable or disable UPNP.

Gaming mode: Click to enable or disable Game mode.

Tools

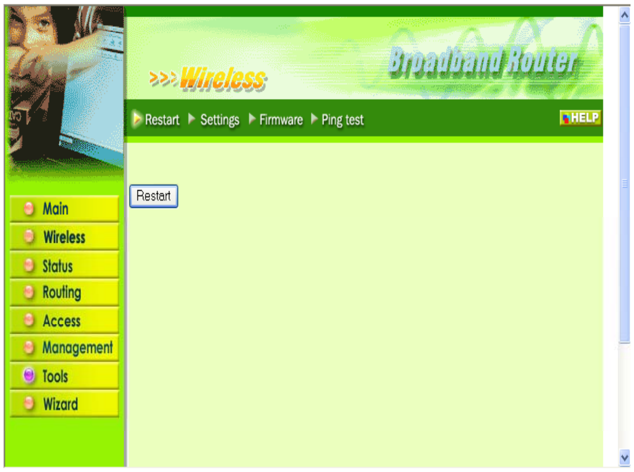
This page enables you to restart the system, save and load different settings as profiles, restore factory default settings, run a setup wizard to configure router settings, upgrade the firmware, and ping remote IP addresses.

The following functions are covered in this section:

- Restart
- Settings
- Firmware
- Ping Test
- Setup Wizard

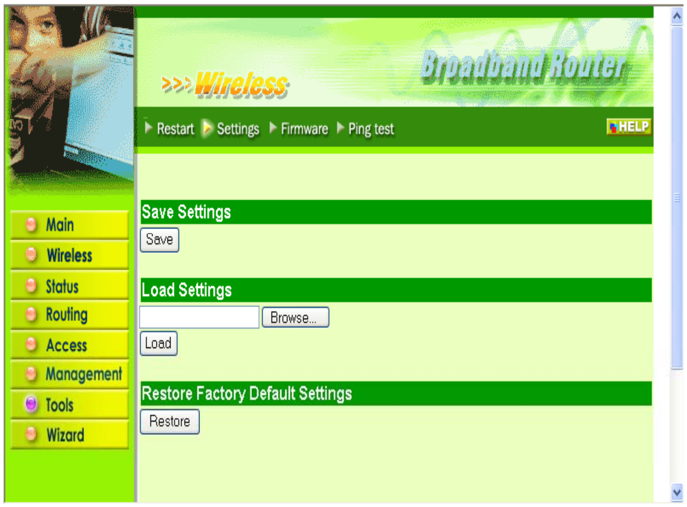
Restart

Click *Restart* to restart the system in the event the system is not performing correctly.



Settings

This screen enables you to save your settings as a profile and load profiles for different circumstances. You can also load the factory default settings, and run a setup wizard to configure the router and router interface.



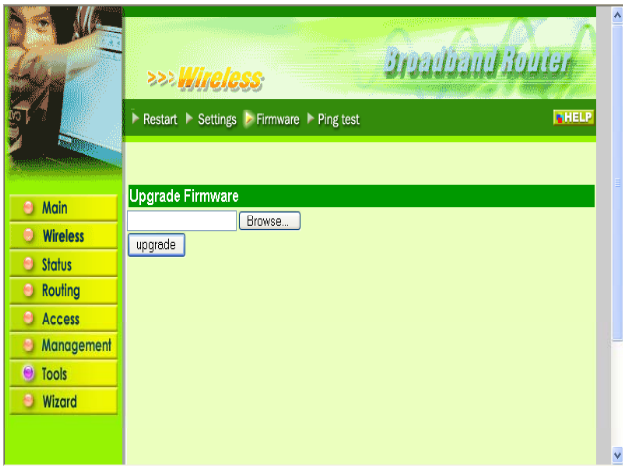
Save Settings: Click to save the current configuration as a profile that you can load when necessary.

Load Settings: Click *Browse* and go to the location of a stored profile. Click *Load* to load the profile's settings.

Restore Factory Default Settings: Click to restore the default settings. All configuration changes you have made will be lost.

Firmware

This screen enables you to keep the router firmware up to date.

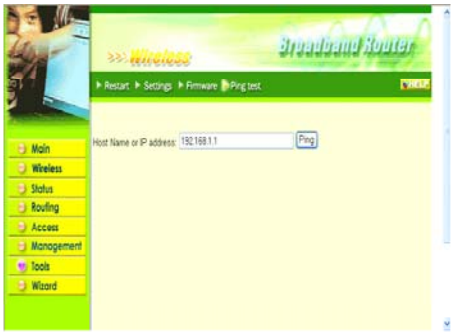


Follow these instructions:

1. Download the latest firmware from the manufacturer's Web site, and save it to your disk.
2. Click *Browse* and go to the location of the downloaded firmware file.
3. Select the file and click Upgrade to update the firmware to the latest release.

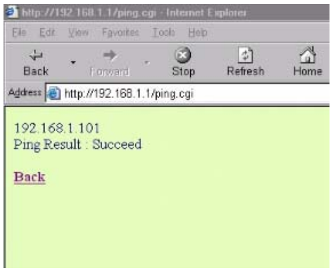
Ping Test

The ping test enables you to determine whether an IP address or host is present on the Internet.



Host Name or IP address: 192.168.1.1

Type the host name or IP address in the text box and click Ping. If the ping is successful, you see a screen similar to the one shown here:

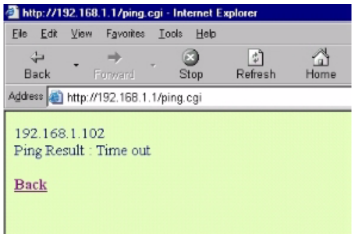

http://192.168.1.1/ping.cgi - Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Address

http://192.168.1.1/ping.cgi

192.168.1.101
Ping Result : Succeed

Back

If the ping is unsuccessful, you see a screen like the the one shown:


http://192.168.1.1/ping.cgi - Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Address

http://192.168.1.1/ping.cgi

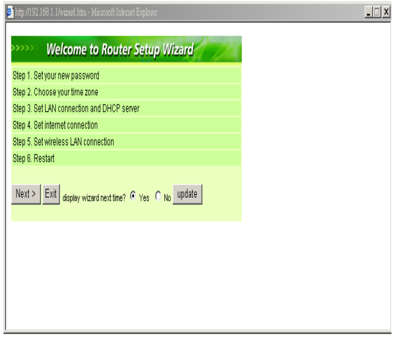
192.168.1.102
Ping Result : Time out

Back

Setup Wizard

The setup wizard enables you to configure the router quickly and conveniently. Follow these instructions:

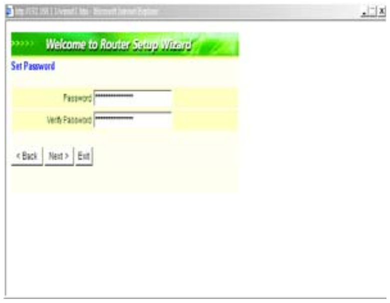
1. In the Settings screen Setup Wizard section, click Run Wizard. The screen shown to the right appears.


http://192.168.1.1/wizard.htm - Microsoft Internet Explorer
Welcome to Router Setup Wizard
Next >
Exit
update

Step 1. Set your new password
Step 2. Choose your time zone
Step 3. Set LAN connection and DHCP server
Step 4. Set internet connection
Step 5. Set wireless LAN connection
Step 6. Restart

display wizard next time? ● Yes ○ No

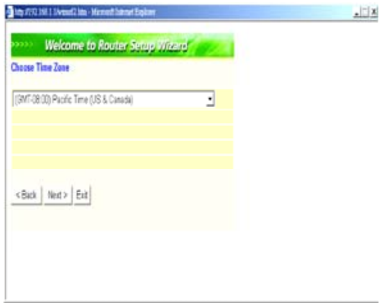
2. Click *Next*. You are prompted to select a password. Type a password in the text box, and then type it again for verification.



Set Password

Password: ***************
Verify Password: ***************

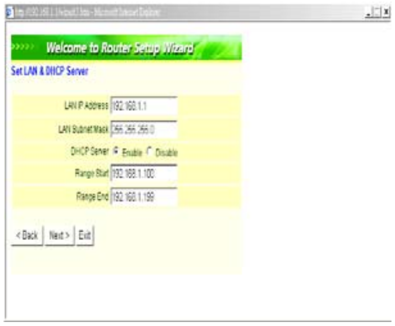
3. Click *Next*. Select your time zone from the drop-down list.



Choose Time Zone

(GMT-08:00) Pacific Time (US & Canada)

4. Click *Next*.
5. Type the LAN IP address in the text box. The default IP address 192.168.1.1.
6. Type the subnet mask in the text box.
7. Enable DHCP Server if you want DHCP to automatically assign IP addresses. Type a beginning IP address and an end IP address for the DHCP server to use in assigning IP addresses.



Set LAN & DHCP Server

LAN IP Address 192.168.1.1

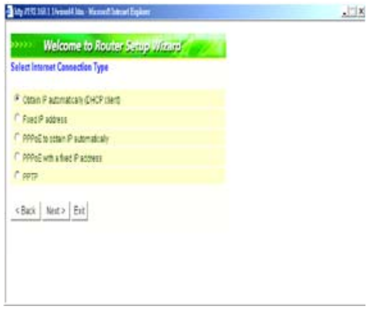
LAN Subnet Mask 255.255.255.0

DHCP Server ● Enable ○ Disable

Range Start 192.168.1.100

Range End 192.168.1.199

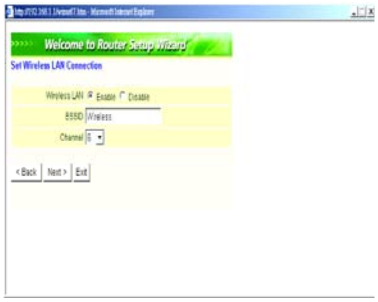
8. Click *Next*. Select how the router will set up the Internet connection. If you have enabled DHCP server, choose "Obtain IP automatically (DHCP client)" to have the router assign IP addresses automatically.



Select Internet Connection Type

● Obtain IP automatically (DHCP client)
○ Fixed IP address
○ PPPoE to obtain IP automatically
○ PPPoE with a fixed IP address
○ PPTP

9. Click to enable or disable wireless LAN. If you enable the wireless LAN, type the SSID in the text box and select a communications channel. The SSID and channel must be the same as wireless devices attempting communication to the router.



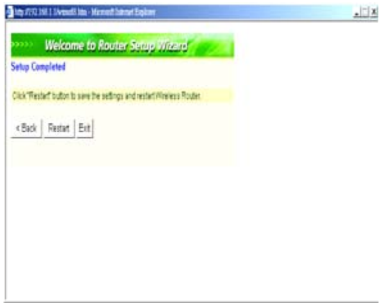
Set Wireless LAN Connection

Wireless LAN ● Enable ○ Disable

SSID Wireless

Channel 6

10. Click *Next*. You are prompted to restart save the settings and restart the router interface. Click restart to complete the wizard.



Setup Completed

Click "Restart" button to save the settings and restart Wireless Router.

— This page left blank intentionally —

APPENDIX A: GLOSSARY

The following glossary of networking terms is provided for your convenience.

Access Point	Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.
Authentication	Authentication refers to the verification of a transmitted message's integrity.
DMZ	DMZ (DeMilitarized Zone) is a part of an network that is located between a secure LAN and an insecure WAN. DMZs provide a way for some clients to have unrestricted access to the Internet.
Beacon Interval	Refers to the interval between packets sent sent by access points for the purposes of synchronizing wireless LANs.
DHCP	DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.
DNS	DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.
Domain Name	The domain name typically refers to an Internet site address.
DTIM	DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.

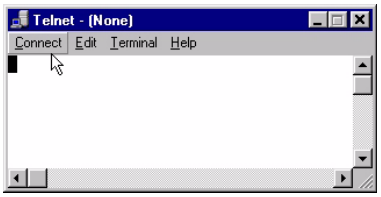
Filter	Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.
Firewall	Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.
Firmware	Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.
Fragmentation	Refers to the breaking up of data packets during transmission.
FTP	FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server.
Gateway	Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.
Host Name	The name given to a computer or client station that acts as a source for information on the network.
HTTP	HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example*, http://www.yahoo.com*).
ICMP	ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP	IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.
IP Address	The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).
ISP	An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.
LAN	LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router.
MAC Address	A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.
Metric	A number that indicates how long a packet takes to get to its destination.
MTU	MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.
NAT	NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator	The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.
NTP	NTP (Network Time Protocol) is used to synchronize the realtime clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).
Packet	A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.
Ping	Ping (Packet INternet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.
Port	Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE	PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.
Preamble	Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors communications between roaming wireless enabled devices and access points.
Protocol	A protocol is a rule that governs the communication of data.
RIP	RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.
RTS	RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server	Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.
SMTP	SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.
SNMP	SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hardware or software components transmit network device activity data to the workstation used to oversee the network.
SSID	SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.
Subnet Mask	Subnet Masks (SUBNETwork masks) are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet.
SysLog Server	A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.
TCP	(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.
TCP/IP	TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in real-time video and audio transmission).

Telnet	Telnet is a terminal emulation protocol commonly used on the Internet and TCP- or IP-based networks:  **Windows Telnet Client** Telnet is used for connecting to remote devices and running programs. Telnet is an integral component of the TCP/IP communications protocol.
UDP	(User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, realtime video and audio where packets can be dumped as there is no time for retransmitting the data).
Virtual Servers	Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).
WEP	WEP (Wired Equivalent Privacy) is the de facto security protocol for wireless LANs, providing the "equivalent" security available in hardwired networks.
Wireless LAN	Wireless LANs (WLANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WLAN	WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.
WAN	WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).

— This page left blank intentionally —

APPENDIX B: TROUBLESHOOTING

Q&A for Windows environments

These guidelines give you tips to deal with some problems you may encounter while using the Wireless Router. If the problems remain unsolved, contact your dealer for assistance.

Common problems and solutions

These guidelines give you tips to deal with some problems you may encounter while using the Wireless Router. If the problems remain unsolved, contact your dealer for assistance.

All LEDs are off

1. Check that the power adapter is firmly seated.
2. Use some other electrical device to confirm that the electrical outlet is working.

The power LED is on but the Link LEDs are off

1. Check that all RJ-45 connectors are firmly seated.
2. Check the RJ-45 cable with a source that you know is active to be sure the cable or connectors are not damaged.

Cannot connect to the Wireless Router

1. Check that the IP address in the URL field is correct. The default IP address is 192.168.1.1.
2. Check the TCP/IP settings in the Network Control Panel on the client computer.
3. Check that you are within range for wireless operation. The maximum range is typically 200 meters, depending on ambient noise, thickness of walls and other environmental characteristics.

APPENDIX C: NETWORKING BASIS

This chapter will help you learn the basics of home networking.

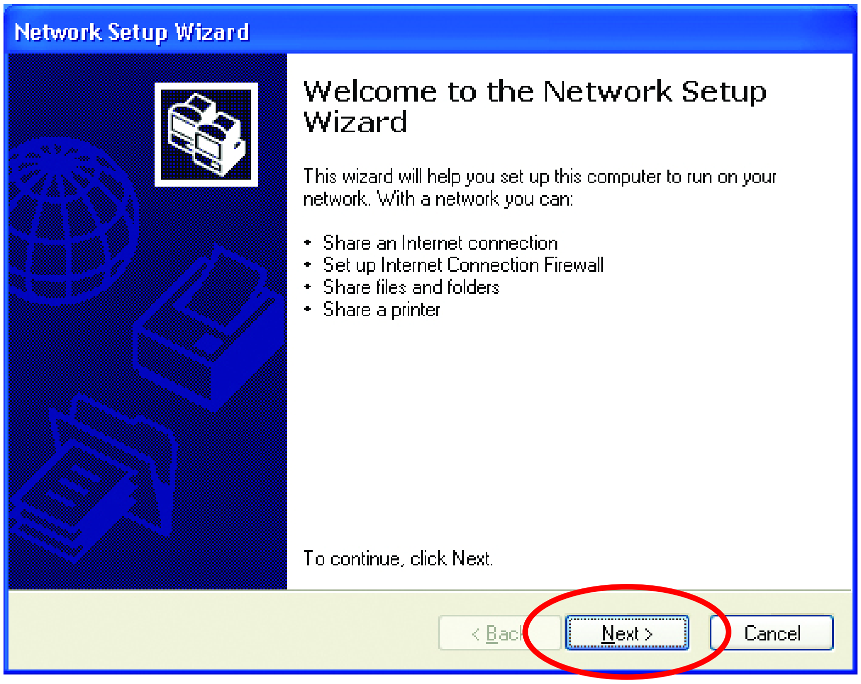
Using the Windows XP Network Setup Wizard

Go to **Start menu** > **Control Panel** >

Network Connections

In the menu on the left side of the window, select "**Set up a home or small office network**"

Click "**Next**" to procced



Network Setup Wizard

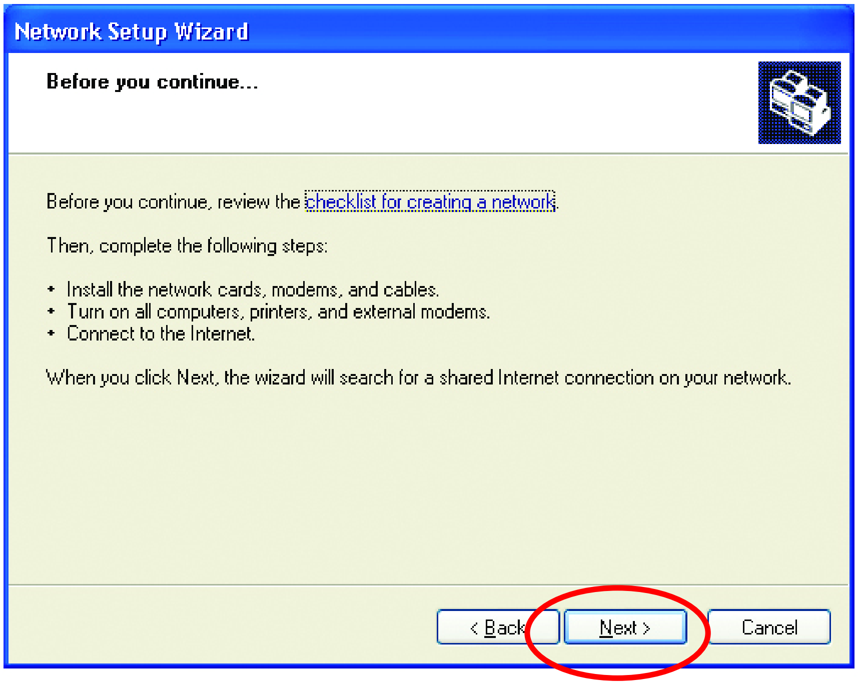
Welcome to the Network Setup Wizard

This wizard will help you set up this computer to run on your network. With a network you can:

- Share an Internet connection
- Set up Internet Connection Firewall
- Share files and folders
- Share a printer

To continue, click Next.

Click "**Next**" to continue



Network Setup Wizard

Before you continue...

Before you continue, review the checklist for creating a network.

Then, complete the following steps:

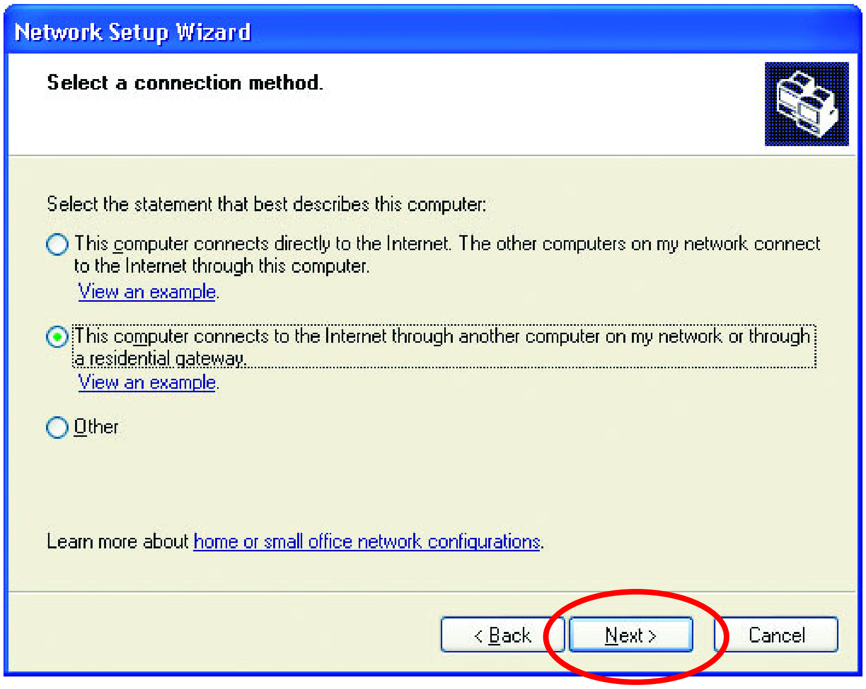
- Install the network cards, modems, and cables.
- Turn on all computers, printers, and external modems.
- Connect to the Internet.

When you click Next, the wizard will search for a shared Internet connection on your network.

Select the option that best describes how you connect your computer to the Internet.

In the case of using router in the network, choose the second option.

Click "**Next**" to continue.



Network Setup Wizard

Select a connection method.

Select the statement that best describes this computer:

○ This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.

● This computer connects to the Internet through another computer on my network or through a residential gateway.
View an example.

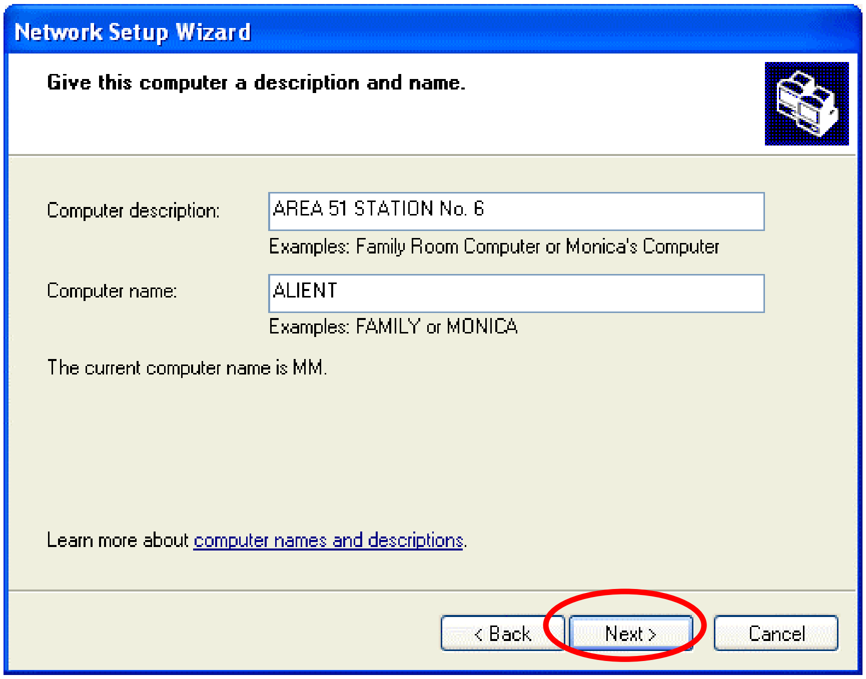
○ Other

Learn more about home or small office network configurations.

1. Enter a short description for your computer.

2. Enter a name for your computer to be recognized among the network.

3. Click "**Next**" to continue.



Network Setup Wizard

Give this computer a description and name.

Computer description: AREA 51 STATION No. 6

Examples: Family Room Computer or Monica's Computer

Computer name: ALIENT

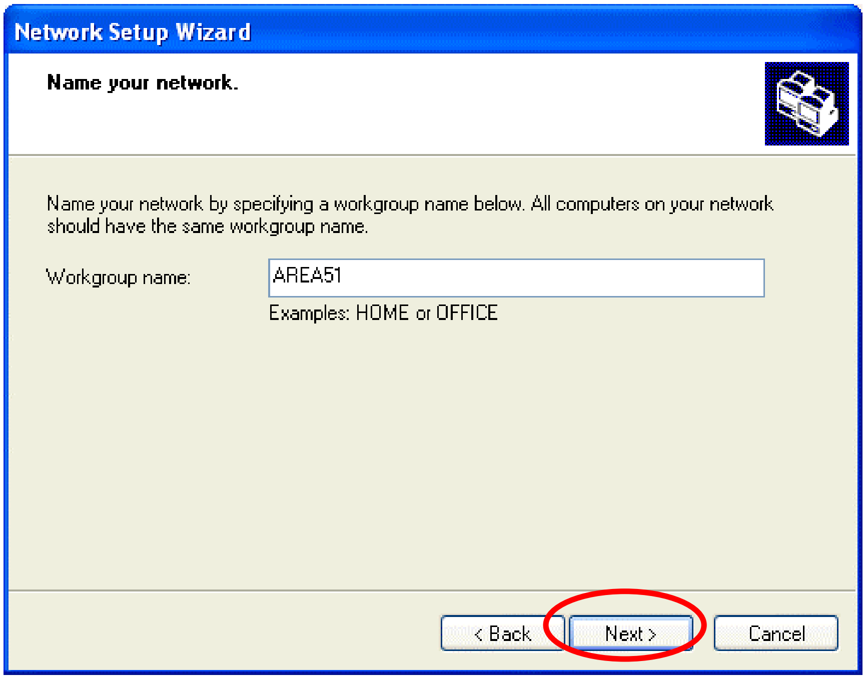
Examples: FAMILY or MONICA

The current computer name is MM.

Learn more about computer names and descriptions.

Enter "**Workgroup name**" for your home network.

Click "**Next**" to continue"



Network Setup Wizard

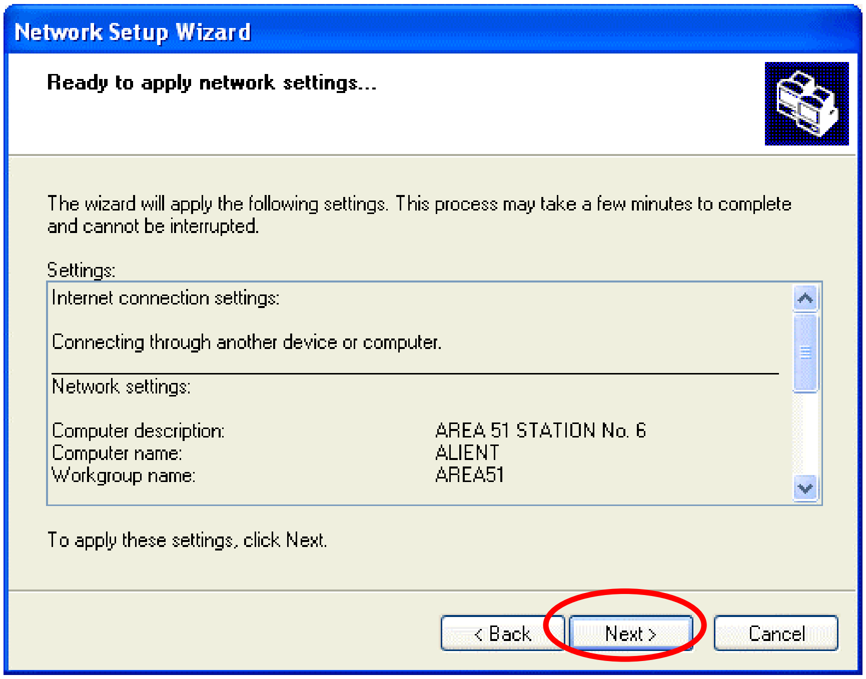
Name your network.

Name your network by specifying a workgroup name below. All computers on your network should have the same workgroup name.

Workgroup name: AREA51

Examples: HOME or OFFICE

Click "**Next**" and wait for the wizard to apply the settings.



Network Setup Wizard

Ready to apply network settings...

The wizard will apply the following settings. This process may take a few minutes to complete and cannot be interrupted.

Settings:

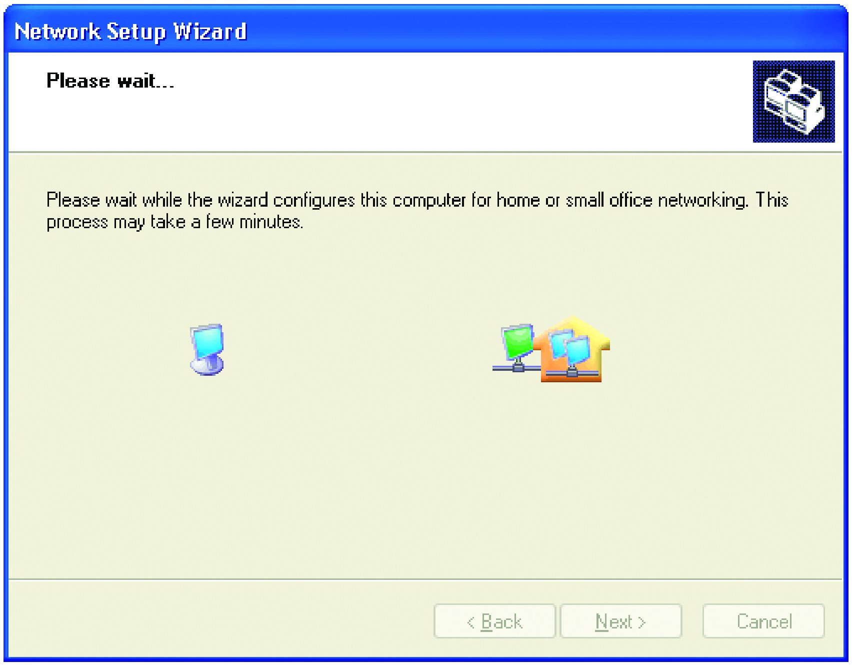
Internet connection settings:

Connecting through another device or computer.

Network settings:

Computer description: AREA 51 STATION No. 6
Computer name: ALIENT
Workgroup name: AREA51

To apply these settings, click Next.



Network Setup Wizard

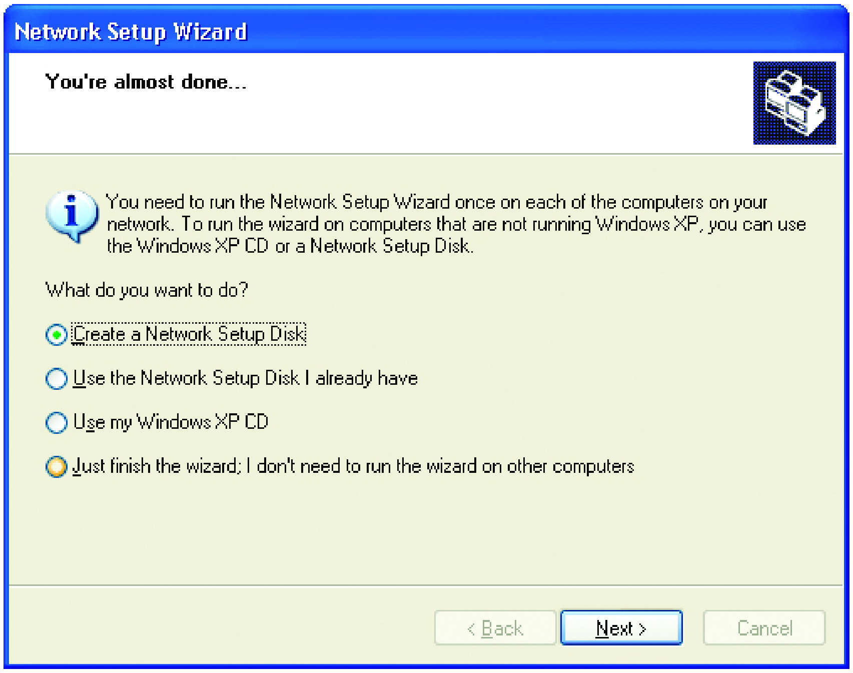
Please wait...

Please wait while the wizard configures this computer for home or small office networking. This process may take a few minutes.

You may create a network setup disk which saves you the trouble of having to configure every PCs in your network.

Select the first choice, and insert a floppy disk into your disk drive

Click "**Next**" to continue.



Network Setup Wizard

You're almost done...

You need to run the Network Setup Wizard once on each of the computers on your network. To run the wizard on computers that are not running Windows XP, you can use the Windows XP CD or a Network Setup Disk.

What do you want to do?

● Create a Network Setup Disk

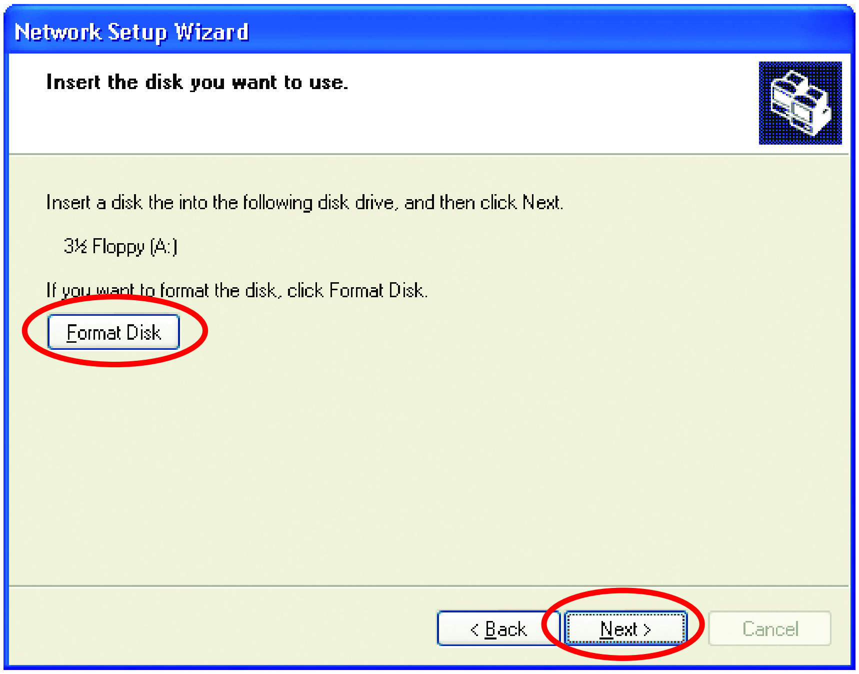
○ Use the Network Setup Disk I already have

○ Use my Windows XP CD

○ Just finish the wizard; I don't need to run the wizard on other computers

Click "**Format Disk**" if you wish to format the disk.

Click "**Next**" to copy the necessary files to the disk.



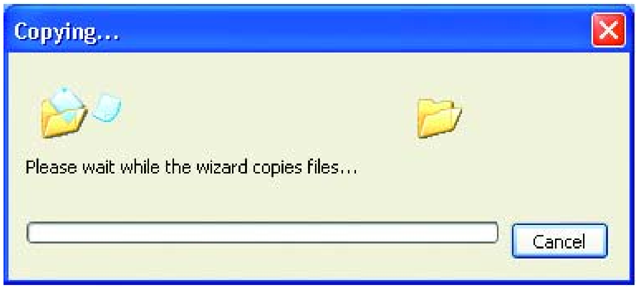
Network Setup Wizard

Insert the disk you want to use.

Insert a disk the into the following disk drive, and then click Next.

3½ Floppy (A:)

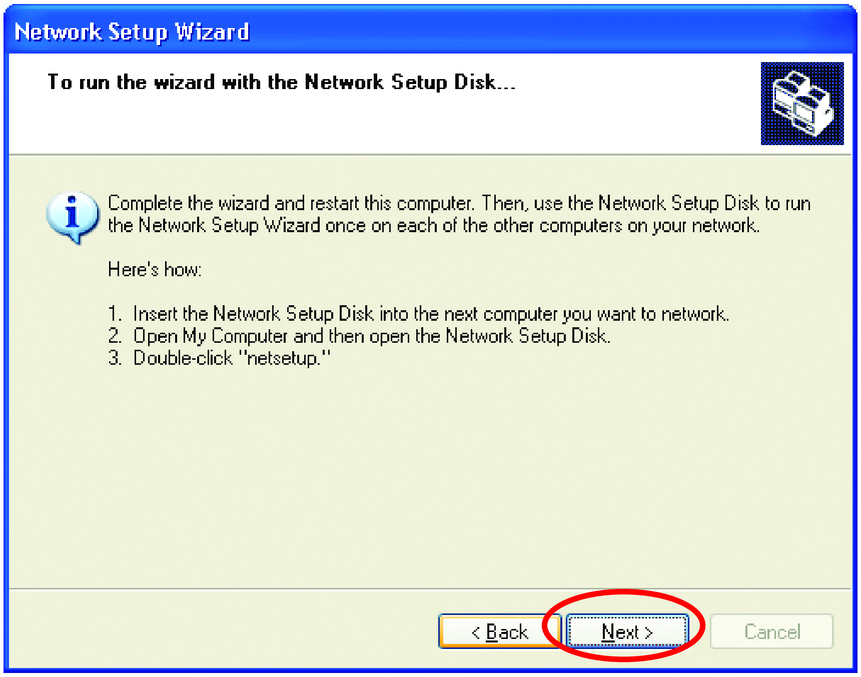
If you want to format the disk, click Format Disk.



Copying...

Please wait while the wizard copies files...

Click “**Next**” to continue with the Network Setup Wizard



Network Setup Wizard

To run the wizard with the Network Setup Disk...

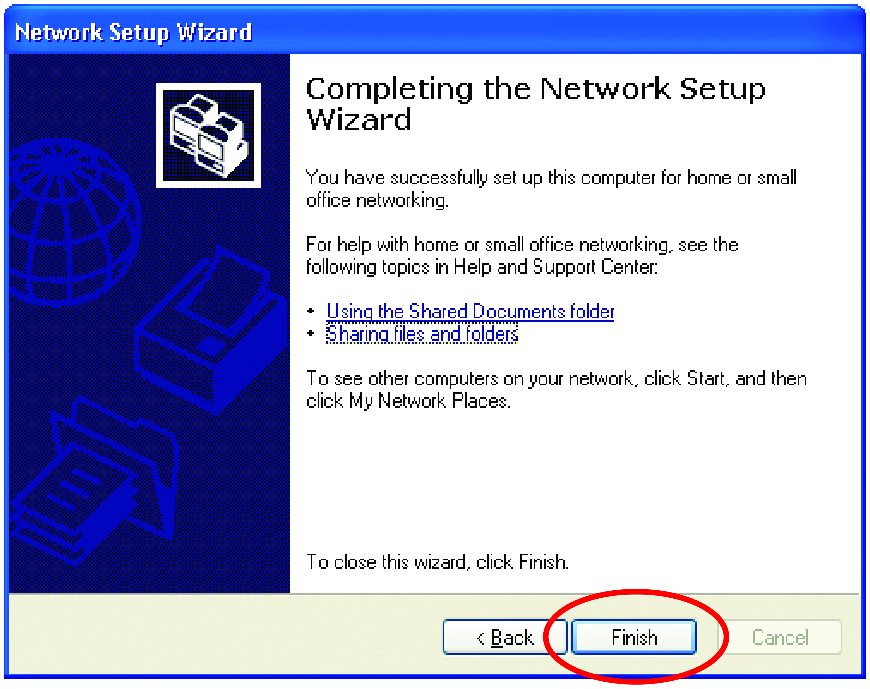
Complete the wizard and restart this computer. Then, use the Network Setup Disk to run the Network Setup Wizard once on each of the other computers on your network.

Here's how:

1. Insert the Network Setup Disk into the next computer you want to network.
2. Open My Computer and then open the Network Setup Disk.
3. Double-click "netsetup."

!Note: Now you may use the Network Setup Disk you just created in any PCs in your network that you wish to setup. Simply insert the Network Setup Disk into the disk drive of a PC, and open to browse the content of the disk with "My Computer" or "Windows File Manager". Double-click and run the file "netsetup" for the program to handle the rest.

Click "**Finish**" to complete the Network Setup Wizard.



Completing the Network Setup Wizard

You have successfully set up this computer for home or small office networking.

For help with home or small office networking, see the following topics in Help and Support Center:

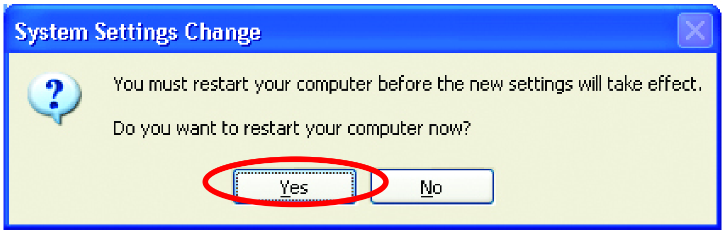
- Using the Shared Documents folder
- Sharing files and folders

To see other computers on your network, click Start, and then click My Network Places.

To close this wizard, click Finish.

System will now have to restart in order for the new settings to be effective.

Click "**Yes**" to restart the computer



You must restart your computer before the new settings will take effect.

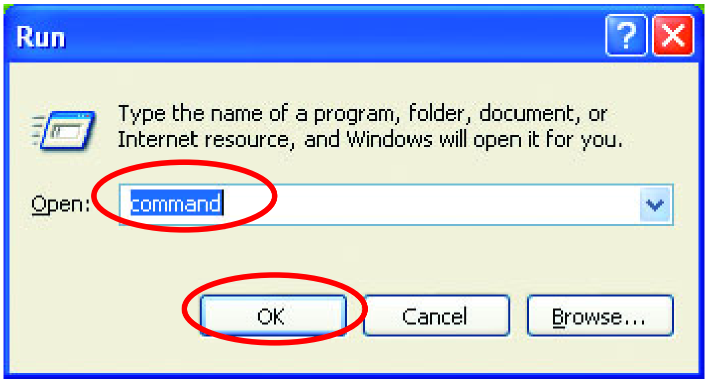
Do you want to restart your computer now?

Checking IP Address of Your Computer In Windows XP

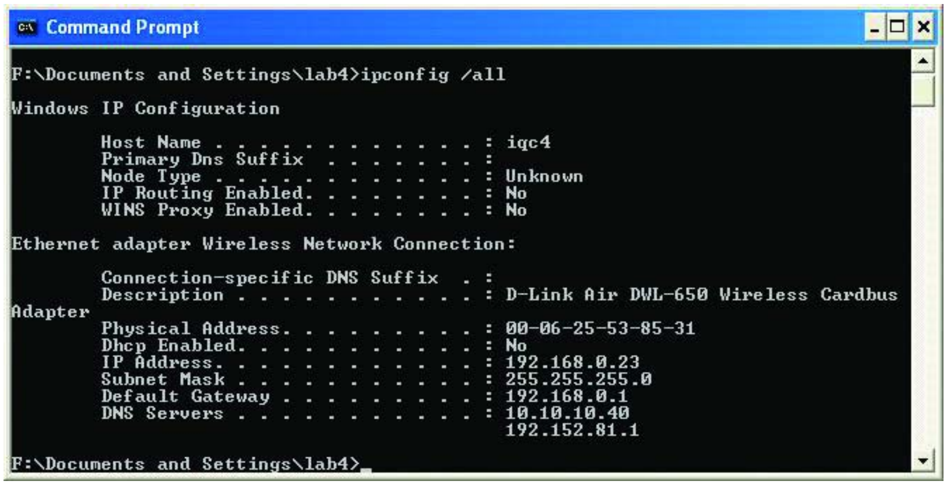
Sometimes you will need to know the IP address of the computer that you are using. For example, when you want to make sure that your computer is in the same network domain as that of your Access Point for you can configure and access the AP.

Go to **Start** menu > **Run** > type "**command**"

Click "**OK**"


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
command
OK
Cancel
Browse...

When the command prompt window appears, type command "ipconfig /all" and press Enter. This command will display the IP addresses of all the network adapters in your computer.



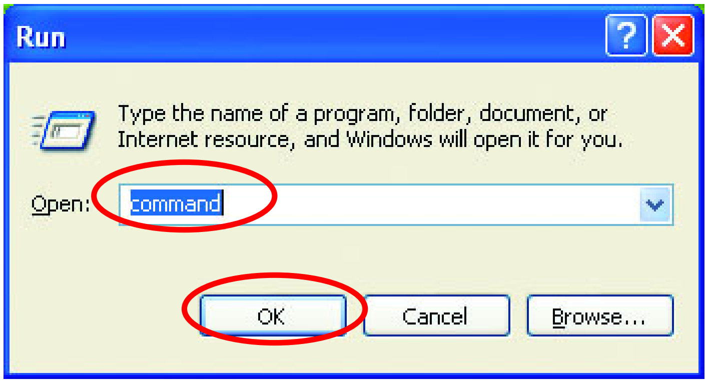
```
F:\Documents and Settings\lab4>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : iqc4
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : D-Link Air DWL-650 Wireless Cardbus
Adapter
        Physical Address. . . . . . . . . : 00-06-25-53-85-31
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.0.23
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 10.10.10.40
                                            192.152.81.1

F:\Documents and Settings\lab4>_
```

In this case, the IP address of your network adapter is 192.168.0.23, which means your Access Point must have an IP address of 192.168.0.xxx in order for you to be able to access it.

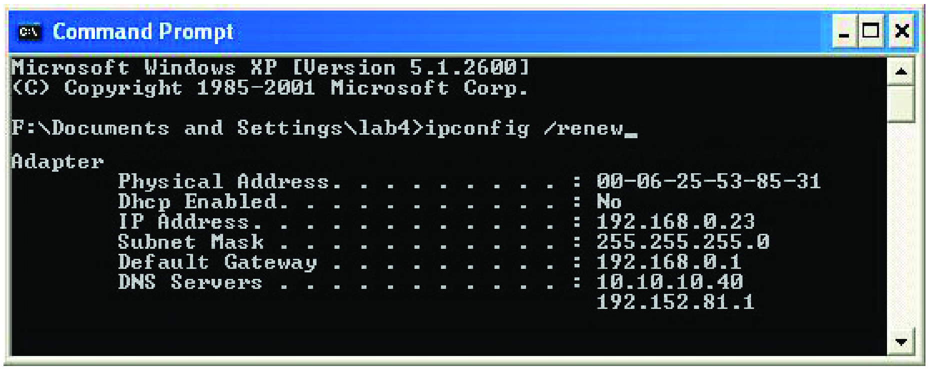
If the IP address is assigned by DHCP server on the network, there are chances you might have to release the IP and acquire it from DHCP server again. Here is how you do it.

Go to **Start** menu > **Run** > type "**command**"

Click "**OK**"


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
command
OK
Cancel
Browse...

Type command, "ipconfig /renew" in the command prompt window and press Enter. This command releases the current IP address and acquire it from the network, i.e. DHCP server, once more.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lab4>ipconfig /renew_

Adapter
        Physical Address. . . . . . . . . : 00-06-25-53-85-31
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.0.23
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 10.10.10.40
                                            192.152.81.1
```

In this case, the IP address that we acquired is the same as previous one, 192.

168.0.23. However, it's often that the acquired IP address of the network adapter might would not be the same.

!Note: To renew IP under Windows 98 and Windows ME, you will have to go to the **Start** menu > **Run** > type **winipcfg** and click "**OK**". The Windows IP Configuration Menu window would appear, where you first click "release" button to release the current IP address, followed by clicking of "Renew" to acquire a new IP address from network.

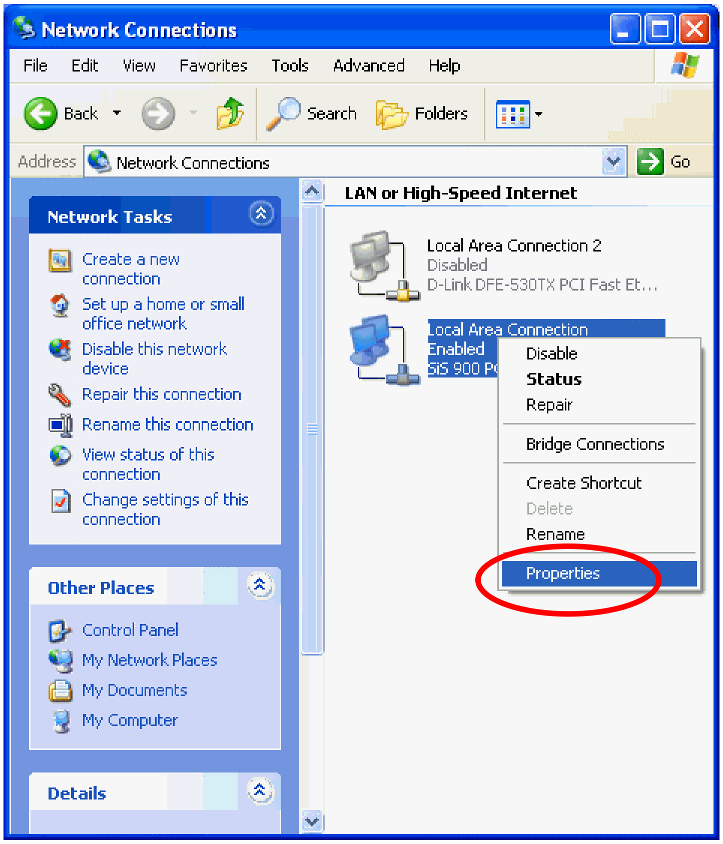
If the above methods for IP renew fail, you will have to try and restart the computer, which will reinitializes the network adapter settings during startup including renewing IP address. If you still have problems getting an IP address after computer restarts, you will have to consult with your MIS in your office or call computer and network technicians.

Dynamic IP Address V.S. Static IP Address

By definition Dynamic IP addresses are the IP addresses that are being automatically assigned to a network device on the network. These Dynamically assigned IP addresses will expire and may be changed over time.

Static IP addresses are the IP addresses that users manually enter for each of the network adapters.

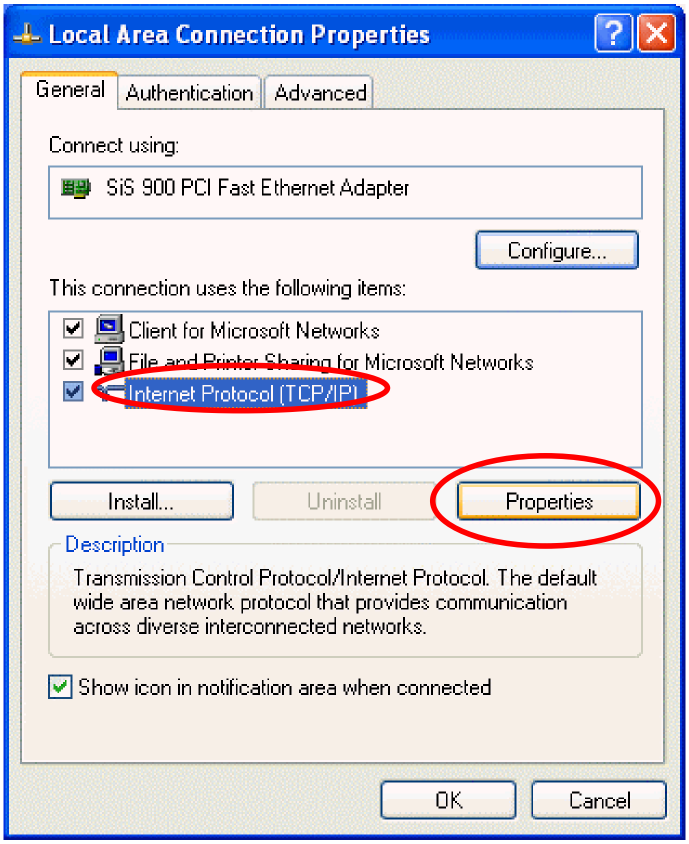
Go to **Start** menu > **Control Panel** > **Network Connections** > Right-click on the active **Local Area connection** > Select "**Properties**"



!Note: There might be two or more Local Area Connection to choose from. You must select the one that you will use to connect to the network.

The Local Area Connection Properties would appear.

Select "**Internet Protocol (TCP/IP)**" and Click "**Properties**" to continue.



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

SiS 900 PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

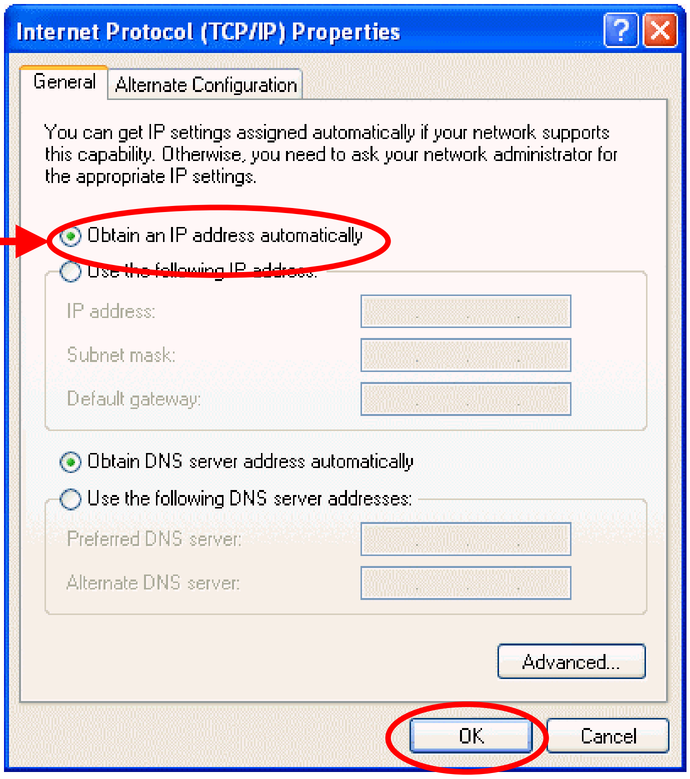
☑ Show icon in notification area when connected

Dynamically Assigned IP Address

The TCP/IP Properties window appears.

Select "**Obtain an IP address automatically**" if you are on a DHCP enabled network.

Click "**OK**" to close the window with the changes made



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Static IP Address

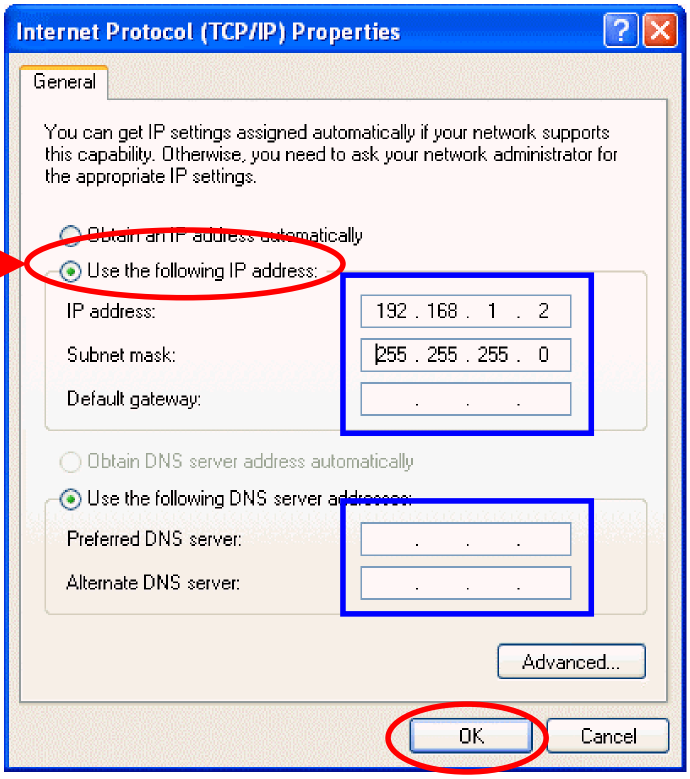
Select “**Use the following IP address**”

Enter the **IP address** and **subnet** mask fields.

Enter the IP address of the Router in the **Default gateway** field.

Enter the IP address of the Router in the **DNS server** field

Click “**Ok**” to close the window



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

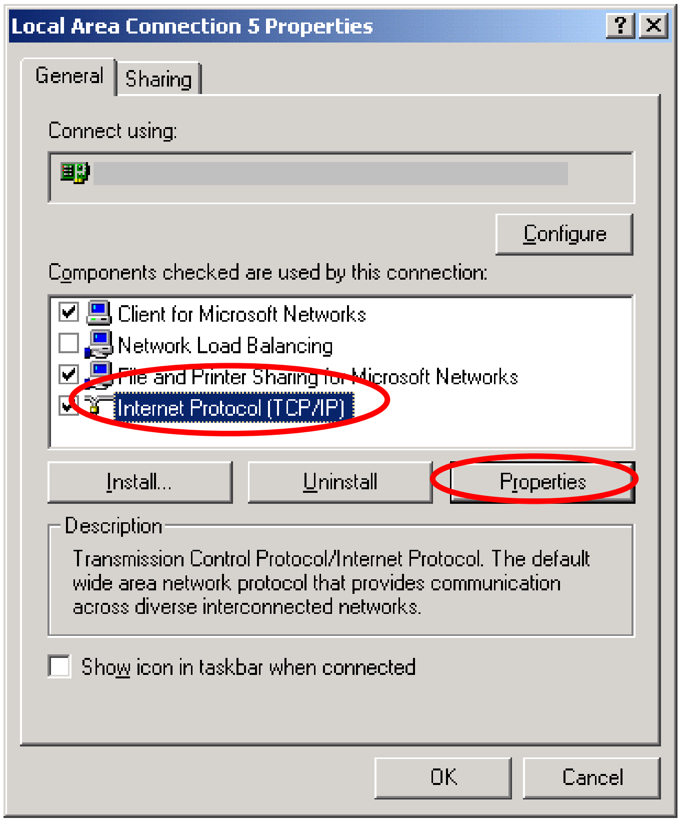
Alternate DNS server: . . .

!Note: The IP address must be within the same range as the wireless route or Access Point.

Wireless Network in Windows 2000

Go to **Start** menu > **Settings** > **Network and Dial-up Connections** > Double-click on the **Local Area Connection**

Select “**Internet Protocol (TCP/IP)**” and click “**Properties**”



Local Area Connection 5 Properties

General | Sharing

Connect using:

Components checked are used by this connection:

☑ Client for Microsoft Networks

☐ Network Load Balancing

☑ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

Description

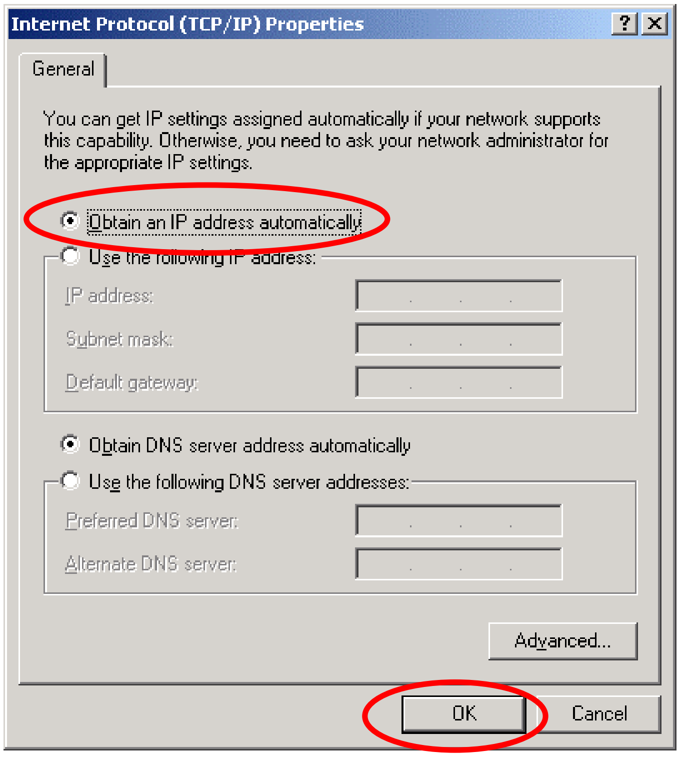
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

The TCP/IP Properties window appears.

Select "**Obtain an IP address automatically**" if you are on a DHCP enabled network.

Click "**OK**" to close the window with the changes made



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

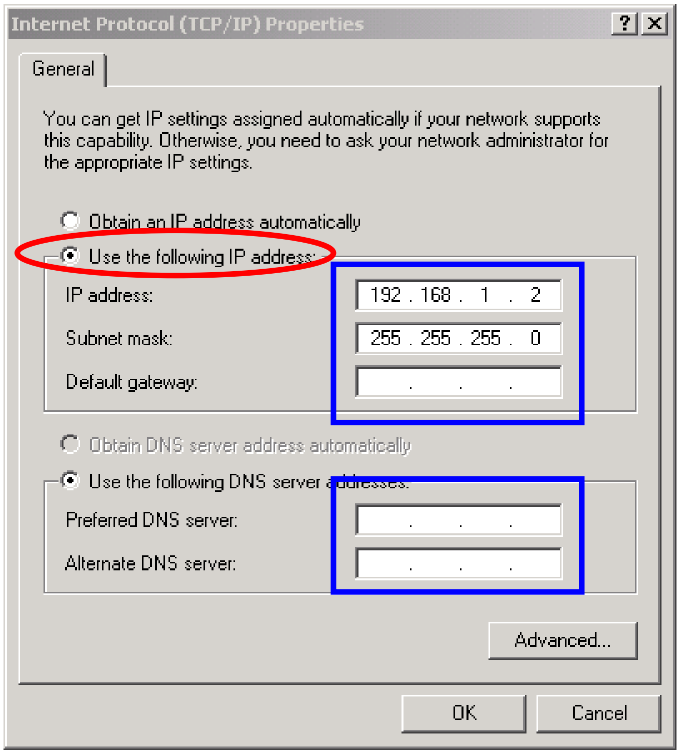
Select "**Use the following IP address**"

Enter the **IP address** and **sub-net** mask fields.

Enter the IP address of the Router in the **Default gateway** field.

Enter the IP address of the Router in the **DNS server** field

Click "**Ok**" to close the window



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

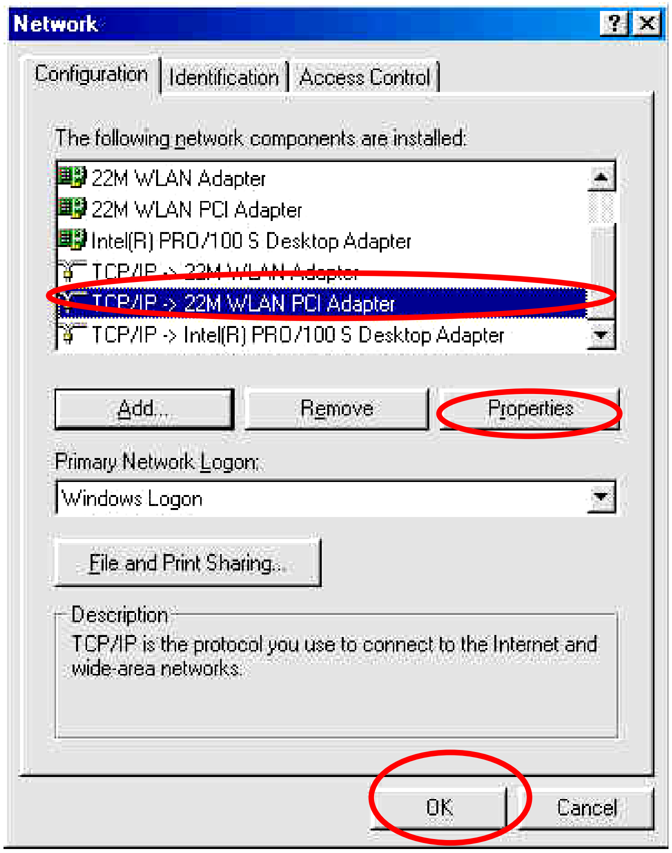
Alternate DNS server: . . .

Wireless Network In Windows 98 and Windows ME

Go to **Start** menu > **Settings** > **Control Panel** > Double-click on **Network**

Select **TCP/IP** of the network device

Click “**Properties**” to continue



Network

The following network components are installed:

- 22M WLAN Adapter
- 22M WLAN PCI Adapter
- Intel(R) PRO/100 S Desktop Adapter
- TCP/IP -> 22M WLAN Adapter
- TCP/IP -> 22M WLAN PCI Adapter
- TCP/IP -> Intel(R) PRO/100 S Desktop Adapter

Primary Network Logon:

Windows Logon

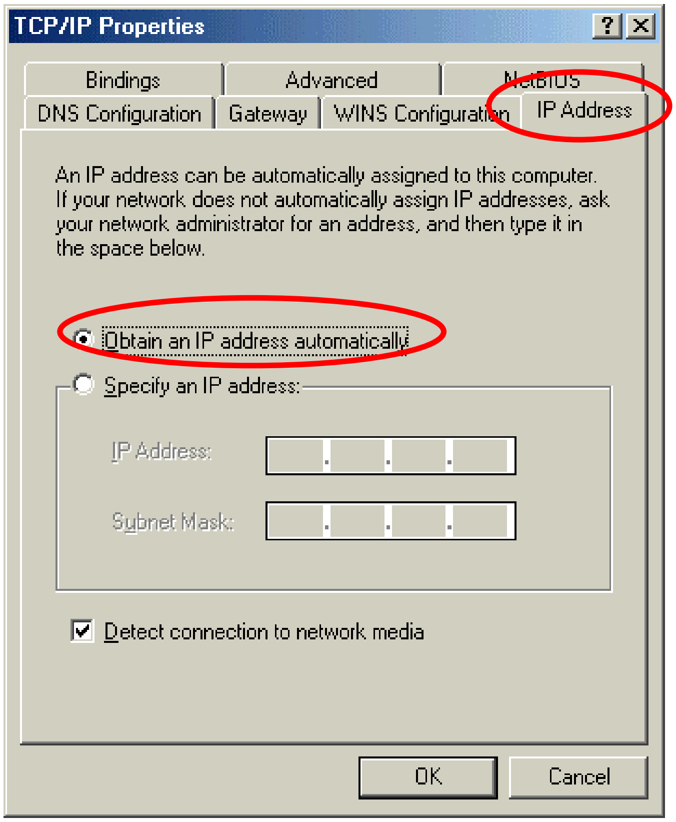
Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

The TCP/IP Properties window appears.

Select “**Obtain an IP address automatically**” if you are on a DHCP enabled network.

Click “**OK**” to close the window with the changes made



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

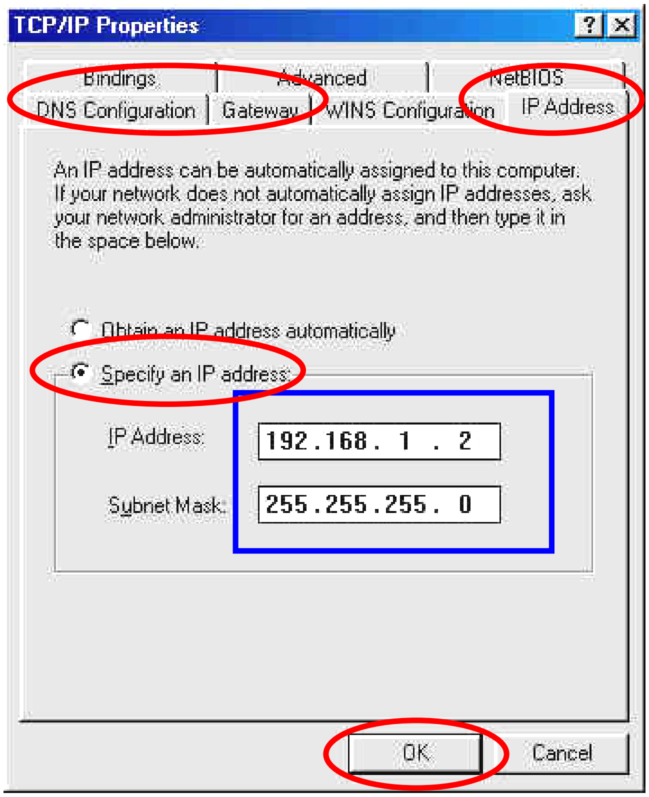
☑ Detect connection to network media

Select "**Use the following IP address**"

Enter the **IP address** and **sub-net** mask fields.

In the **DNS Configuration** Tab Page, (1) enter the IP address of the Router in the **Default gateway** field.

(2) Enter the IP address of the Router in the **DNS server** field



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

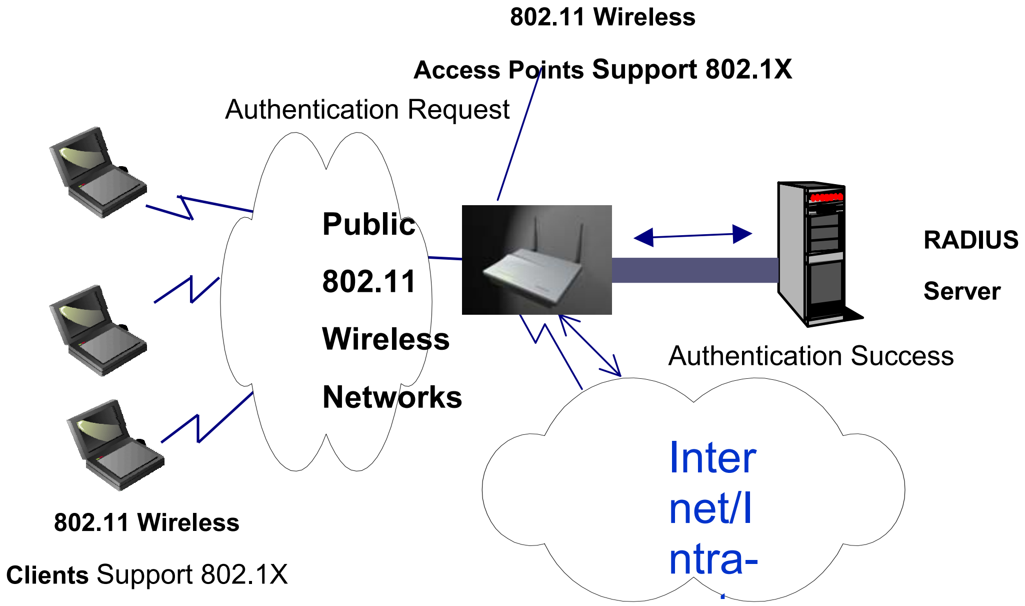
IP Address: 192.168. 1 . 2

Subnet Mask: 255.255.255. 0

APPENDIX D: 802.1X AUTHENTICATION SETUP

There are three essential components to the 802.1x infrastructure: (1) Supplicant, (2) Authenticator and (3) Server. The 802.1x security supports both MD5 and TLS Extensive Authentication Protocol (EAP). The 802.1x Authentication is a complement to the current WEP encryption used in wireless network. The current security weakness of WEP encryption is that there is no key management and no limitation for the duration of key lifetime. 802.1x Authentication offers key management, which includes key per user and key per session, and limits the lifetime of the keys to certain duration. Thus, key decryption by unauthorized attacker becomes extremely difficult, and the wireless network is safely secured. We will introduce the 802.1x Authentication infrastructure as a whole and going into details of the setup for each essential component in 802.1x authentication.

802.1x Authentication Infrastructure



The Infrastructure diagram showing above illustrates that a group of 802.11 wireless clients is trying to form a 802.11 wireless network with the Access Point in order to have access to the Internet/Intranet. In 802.1x authentication infrastructure, each of these wireless clients would have to be authenticated by the Radius server, which would grant the authorized client and notified the Access Point to open up a communication port to be used for the granted client. There are 2 Extensive Authentication Protocol (EAP) methods supported: (1) MD5 and (2) TLS.

MD5 authentication is simply a validation of existing user account and password that is stored in the server with what are keyed in by the user. Therefore, wireless client user will be prompted for account/password validation every time when he/she is trying to get connected. TLS authentication is a more complicated authentication, which involves using certificate that is issued by the Radius server, for authentication. TLS authentication is a more secure authentication, since not only the Radius server authenticates the wireless client, but also the client can validate the Radius server by the certificate that it issues. The authentication request from wireless clients and reply by the Radius Server and Access Point process can be briefed as follows:

1. The client sends an EAP start message to the Access Point
2. The Access Point replies with an EAP Request ID message
3. The client sends its Network Access Identifier (NAI) – its user name – to the Access Point in an EAP Respond message.
4. The Access Point forwards the NAI to the RADIUS server with a RADIUS Access Request message.

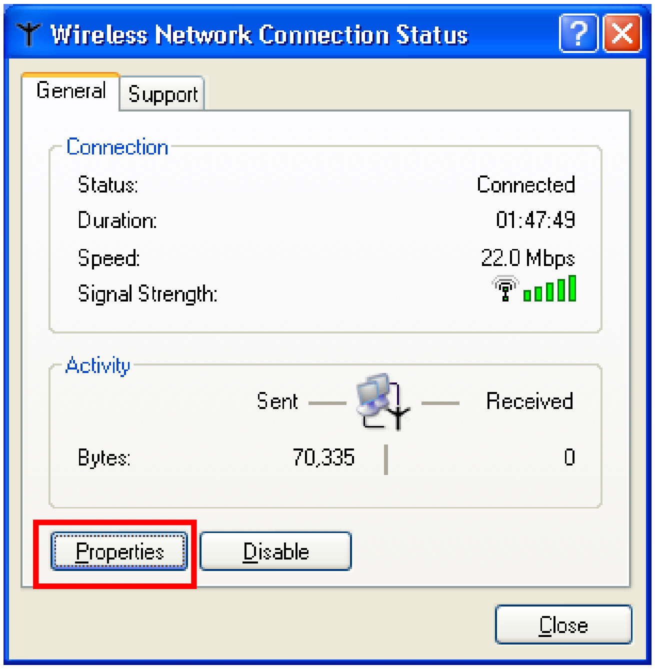
5. The RADIUS server responds to the client with its digital certificate.
6. The client validates the digital certificate, and replies its own digital certificate to the RADIUS server.
7. The RADIUS server validates client's digital certificate.
8. The client and RADIUS server derive encryption keys.
9. The RADIUS server sends the access point a RADIUS ACCEPT message, including the client's WEP key.
10. The Access Point sends the client an EAP Success message along with the broadcast key and key length, all encrypted with the client's WEP key.

Supplicant: Wireless Network PC Card

Here is the setup for the Wireless Network PC Card under Windows XP, which is the only Operating System that our driver supports for 802.1x. Microsoft is planning on supporting 802.1x security in all common Windows Operating System including Win98SE/ME/2000 by releasing Service Pack in 2003.

Please note that the setup illustration is based on our 22Mbps wireless PC Card.

1. Go to **Start** > **Control Panel**
2. double-click on "**Network Connections**"
3. right-click on the Wireless Network Connection that you use with our 22Mbps wireless PC Card.
4. Click "**Properties**" to open up the Properties setting window.



Wireless Network Connection Status

Connection

Status: Connected

Duration: 01:47:49

Speed: 22.0 Mbps

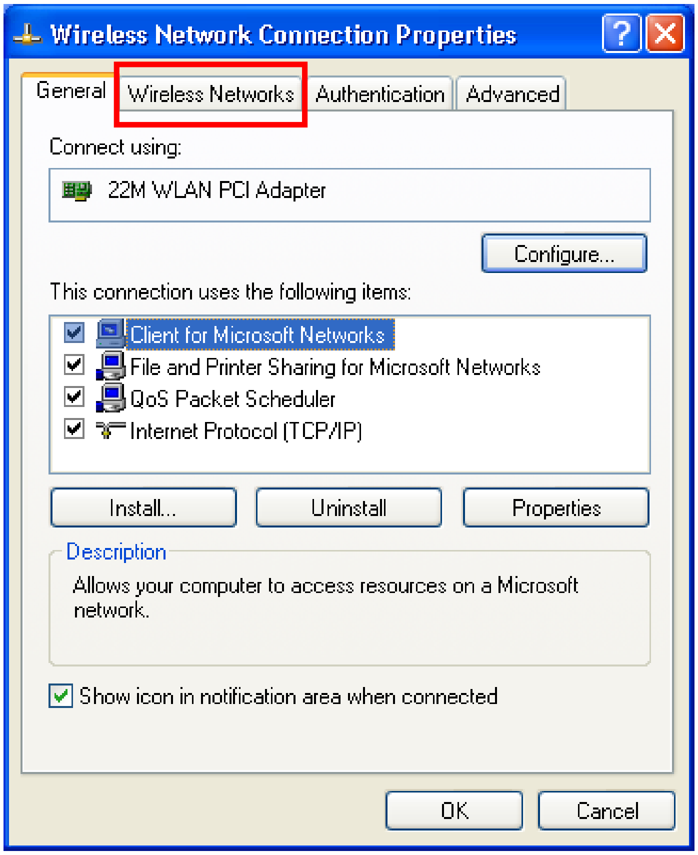
Signal Strength:

Activity

Sent — — Received

Bytes: 70,335 | 0

5. Click on the "**Wireless Network**" tab.



Connect using:

22M WLAN PCI Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

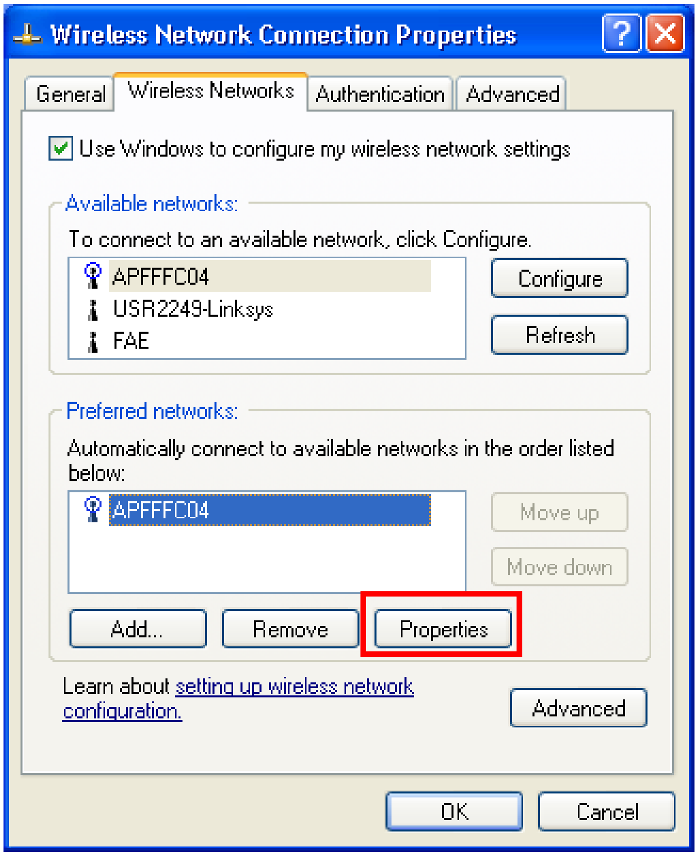
Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

6. Click "**Properties**" of the available wireless network, which you wish to connect or configure.

Please note that if you are going to change to a different 802.1x authentication EAP method, i.e. switch from using MD5 to TLS, , you must remove the current existing wireless network from your Preferred networks first, and add it in again.



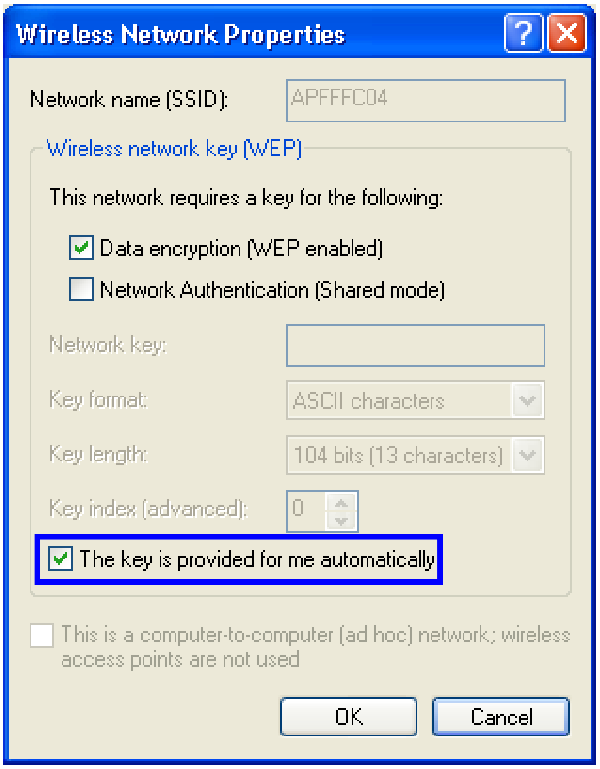
Wireless Network Connection Properties
General
Wireless Networks
Authentication
Advanced
☑ Use Windows to configure my wireless network settings
Available networks:
To connect to an available network, click Configure.
APFFFC04
USR2249-Linksys
FAE
Configure
Refresh
Preferred networks:
Automatically connect to available networks in the order listed below:
APFFFC04
Move up
Move down
Add...
Remove
Properties
Learn about setting up wireless network configuration.
Advanced
OK
Cancel

To configure for using TLS authentication method, please follow steps 7 ~ 25.

Please follow steps 26 ~ for using MD5 authentication method.

TLS Authentication

7. Select "**The key is provided for me automatically**" option



Network name (SSID): APFFFC04

Wireless network key (WEP)

This network requires a key for the following:

☑ Data encryption (WEP enabled)

☐ Network Authentication (Shared mode)

Network key:

Key format: ASCII characters

Key length: 104 bits (13 characters)

Key index (advanced): 0

☑ The key is provided for me automatically

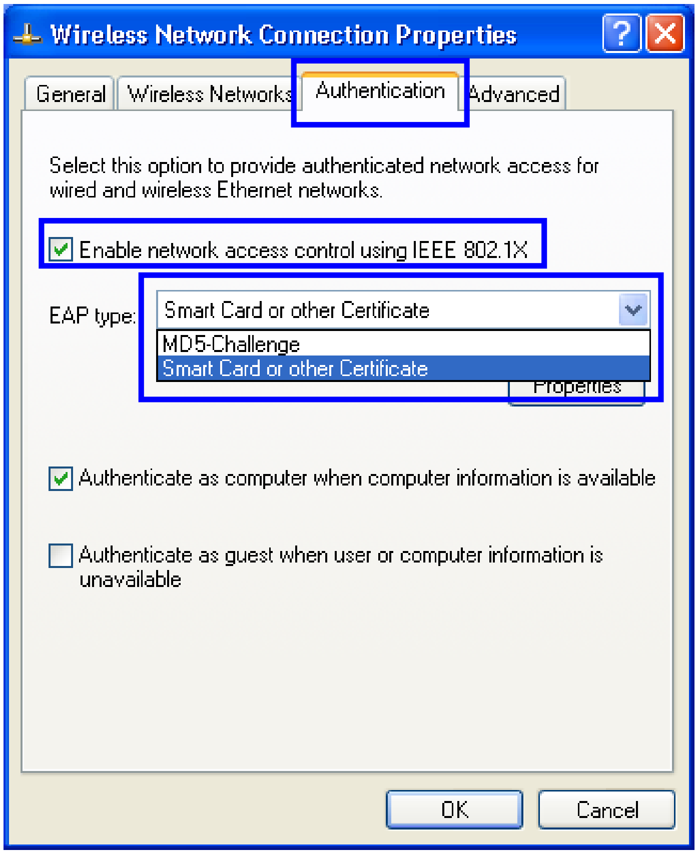
☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

8. Click "**OK**" to close the Wireless Network Properties window.

9. Click “**Authentication**” tab

10. Select “**Enable network access control using IEEE 802.1x**” option to enable 802.1x authentication.

11. Select “**Smart Card or other Certificate**” from the drop-down list box for EAP type.



Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: Smart Card or other Certificate

MD5-Challenge
Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

12. Click “**OK**” to close the Wireless Network Connection Properties window, thus make the changes effective.

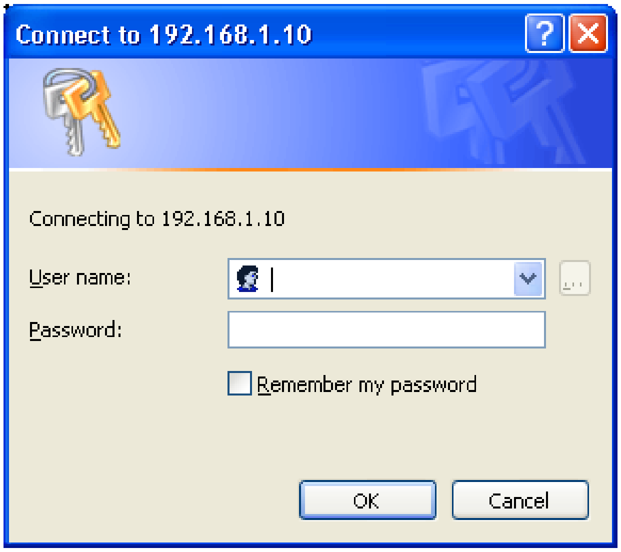
The wireless client configuration in the zero-configuration utility provided in Windows XP is now completed for TLS configuration. Before you can enable IEEE 802.1x authentication and have wireless client authenticated by the Radius server, you have to download the certificate to your local computer first.

TLS Authentication – Download Digital Certificate from Server

In most corporations, it requires internal IT or MIS staff's help to have the certificated downloaded to your local computer. One of the main reasons is that each corporation uses its own server systems, and you will need the assistance from your IT or MIS for account/password, CA server location and etc. The following illustration is based on obtaining a certificate from Windows 2000 Server which can act as a CA server, assuming you have a valid account/password to access the server.

13. Connect to the server and ask for access, and the server will prompt you to enter your user name and password.

14. Enter your **user name** and **password**, then click "**OK**" to continue.



Connect to 192.168.1.10

Connecting to 192.168.1.10

User name:

Password:

□ Remember my password

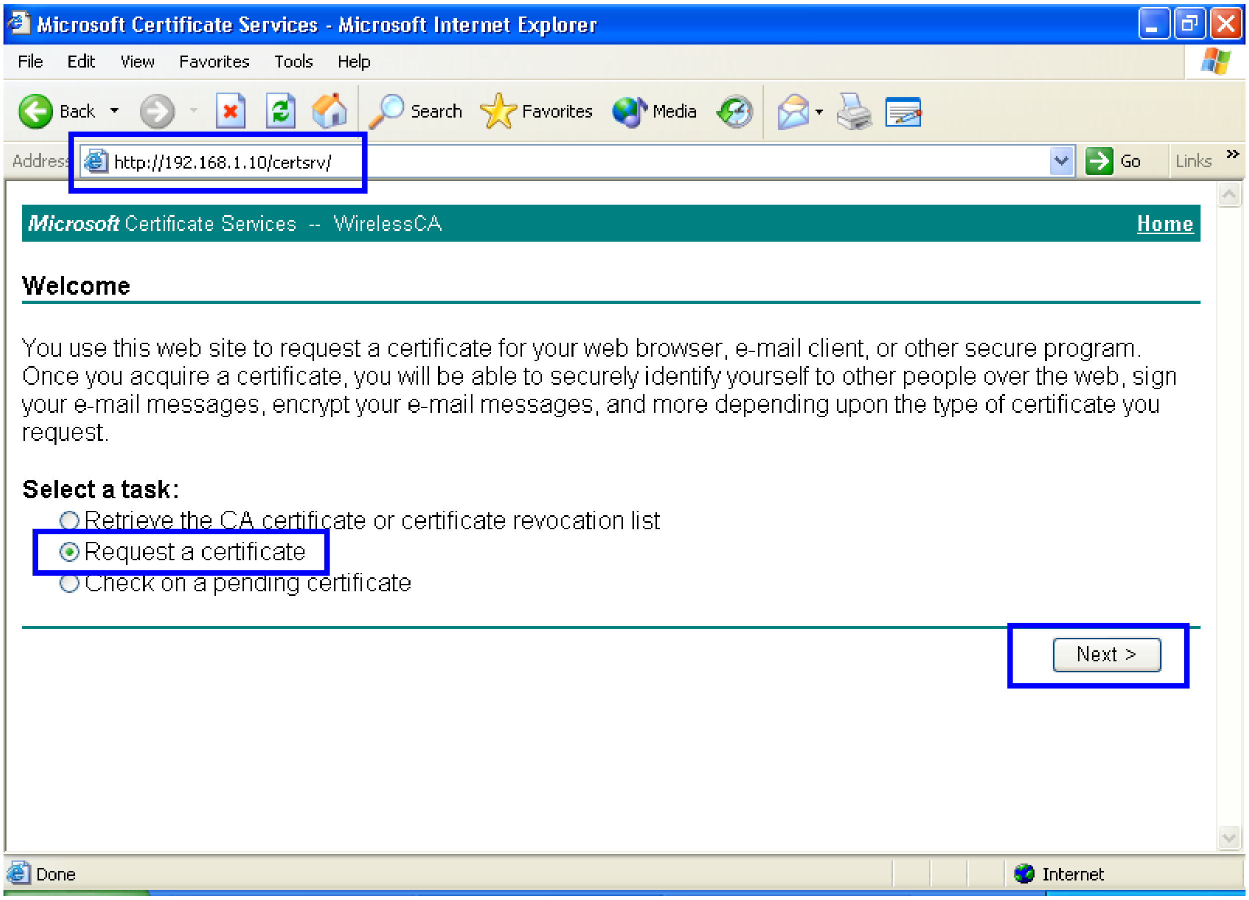
Please note that we use IP addresses for connection with the server for our illustration, and the IP of the server is 192.168.1.10.

15. After successful login, open up your Internet Browser, and type the following in the address field.

http://192.168.1.10/certsrv

This is how we connect to the Certificate Service installed in Windows 2000 server.

16. Now we are connected to the Certificate Service. Select "**Request a certificate**", and click "**Next**" to continue.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/
Go Links
Done
Internet

Microsoft Certificate Services -- WirelessCA **Home**

Welcome

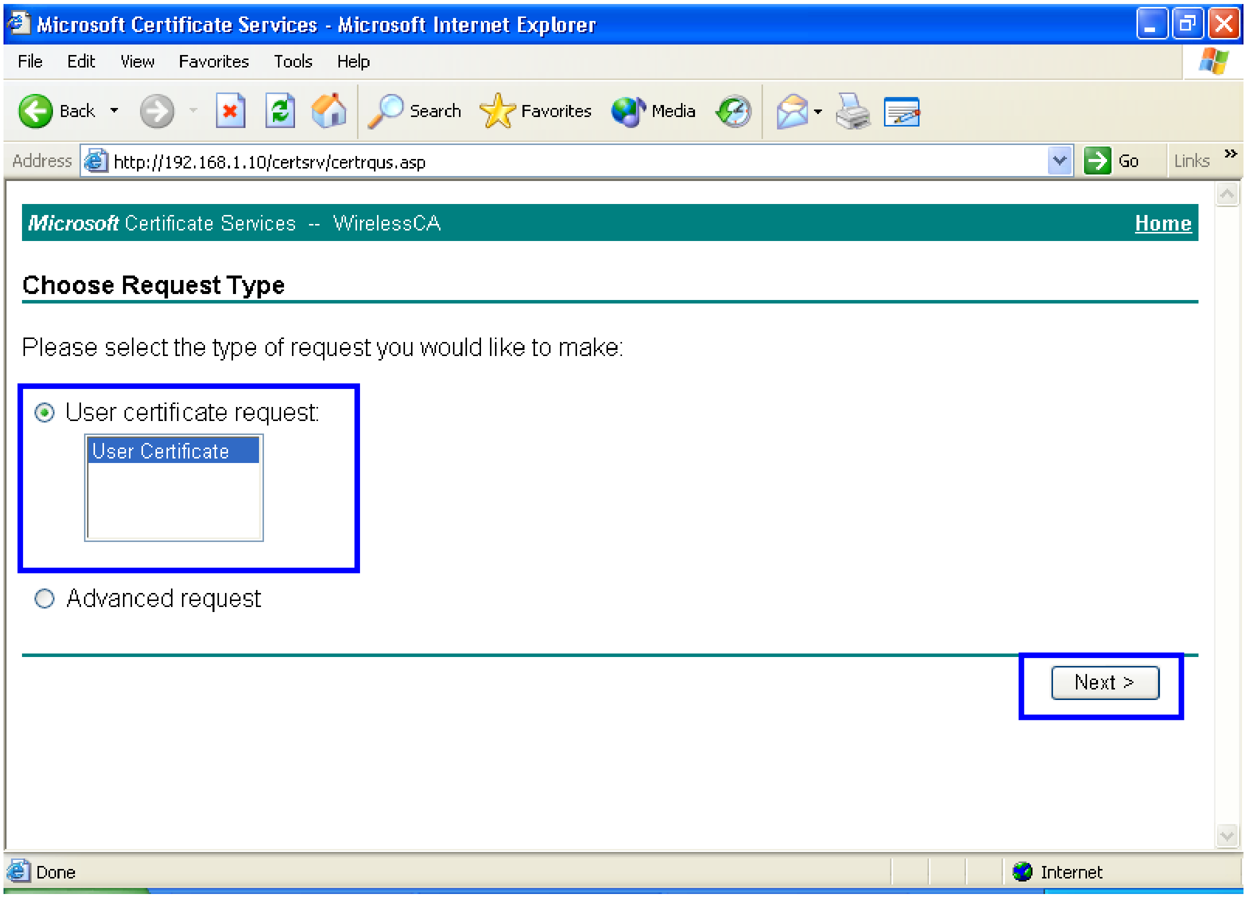
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Next >

17. Select "**User Certificate request**", and click "**Next**" to continue.



Microsoft Certificate Services -- WirelessCA

Home

Choose Request Type

Please select the type of request you would like to make:

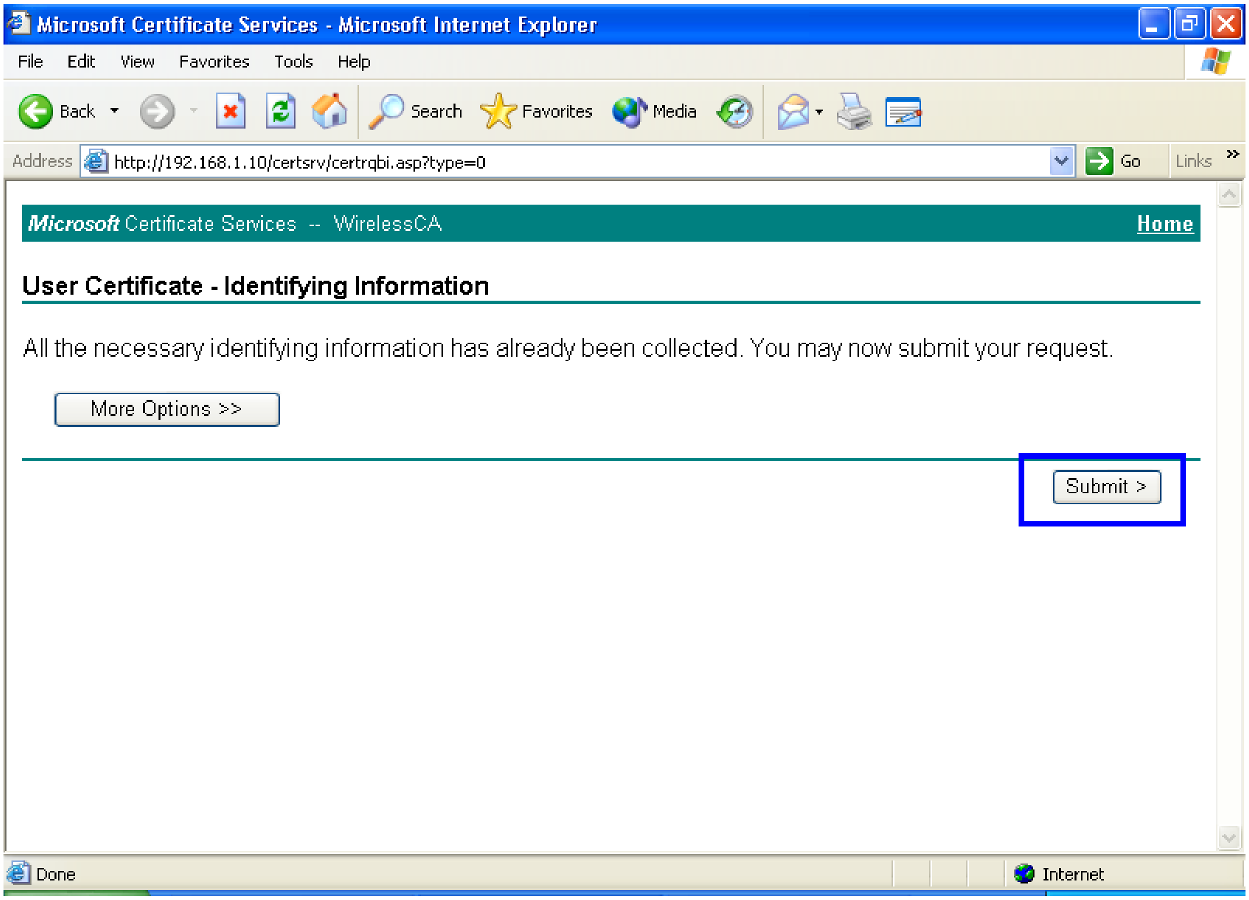
● User certificate request:

User Certificate

○ Advanced request

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://192.168.1.10/certsrv/certrqus.asp
Go
Links
Next >
Done
Internet

18. Click "**Submit >**" to continue.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrqbi.asp?type=0
Go Links
Done
Internet

Microsoft Certificate Services -- WirelessCA **Home**

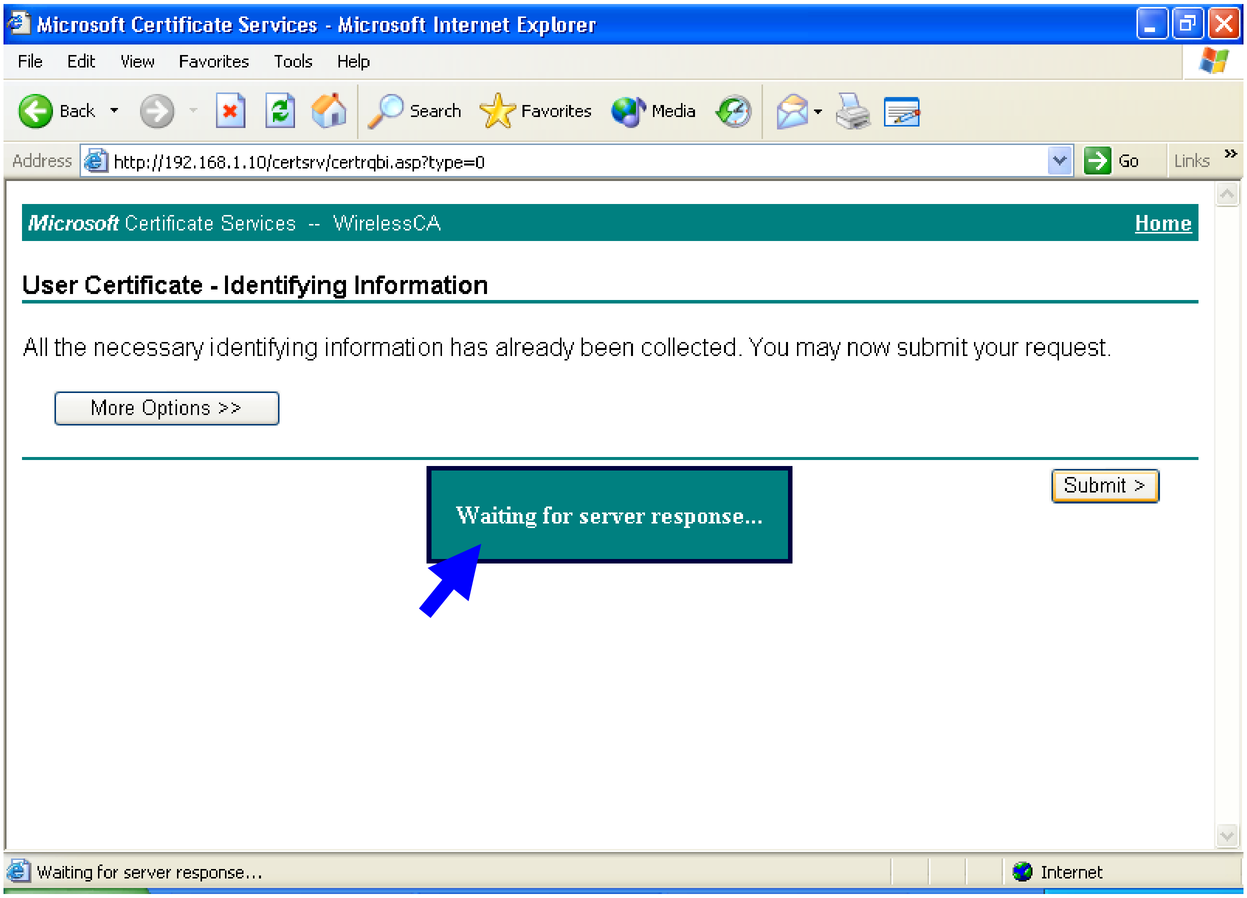
User Certificate - Identifying Information

All the necessary identifying information has already been collected. You may now submit your request.

More Options >>

Submit >

19. The Certificate Service is now processing the certificate request.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrqbi.asp?type=0
Go Links

Microsoft Certificate Services -- WirelessCA

Home

User Certificate - Identifying Information

All the necessary identifying information has already been collected. You may now submit your request.

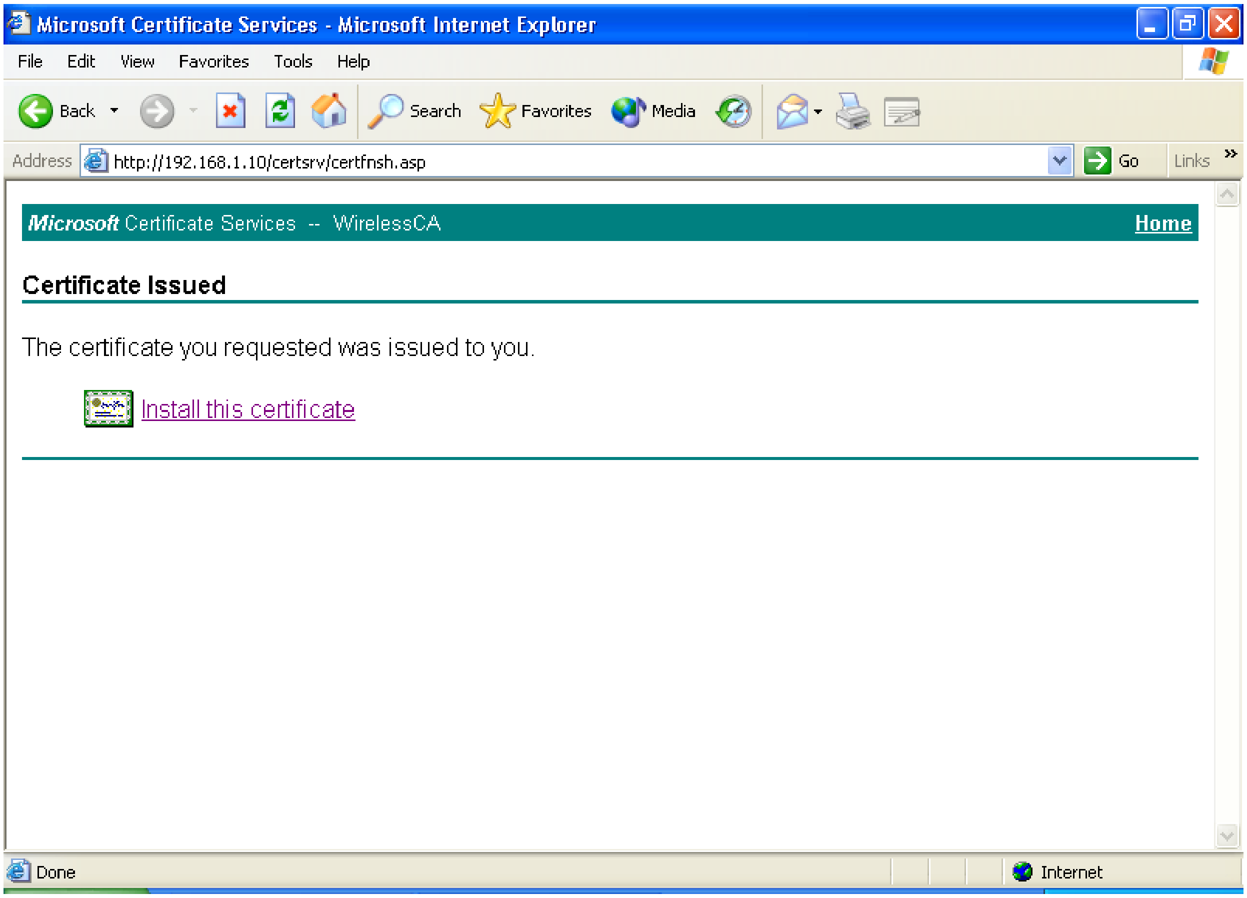
More Options >>

Submit >

Waiting for server response...

Waiting for server response...
Internet

20. The certificate is issued by the server, click "Install this certificate" to download and store the certificate to your local computer.

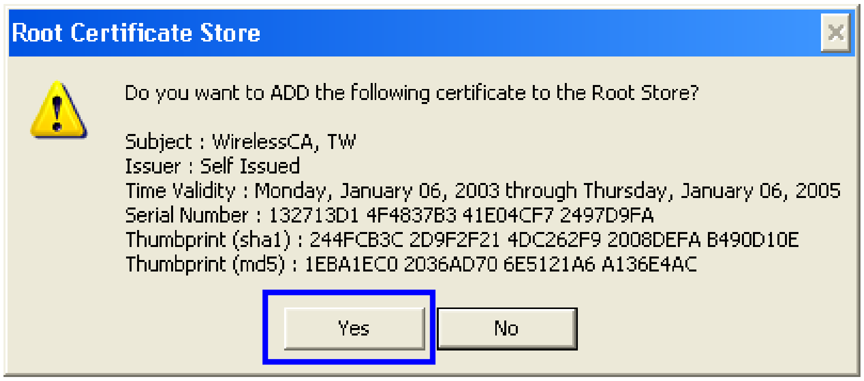

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certfnsh.asp
Go Links
Microsoft Certificate Services -- WirelessCA
Home
Done
Internet

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

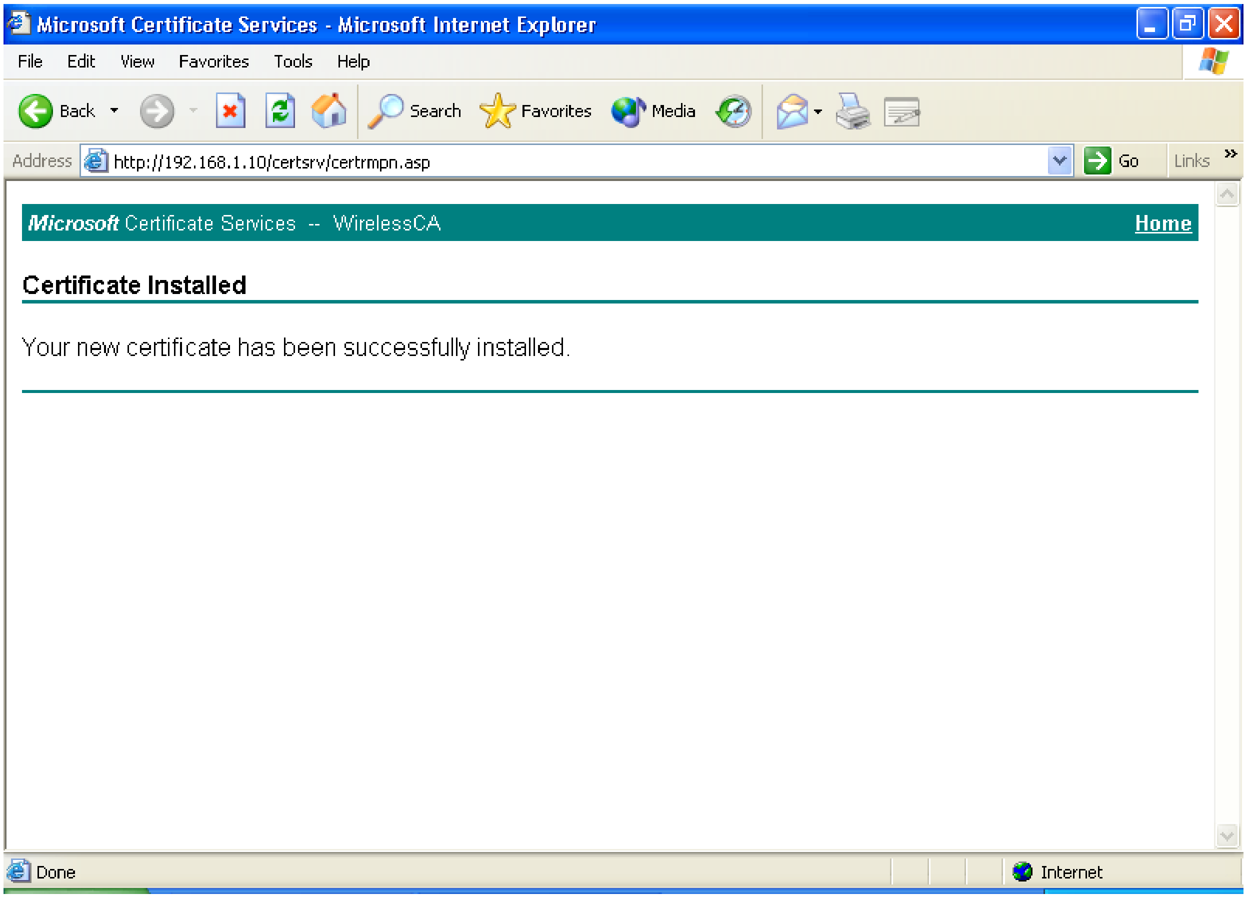
21. Click "**Yes**" to store the certificate to your local computer.



Do you want to ADD the following certificate to the Root Store?

Subject : WirelessCA, TW
Issuer : Self Issued
Time Validity : Monday, January 06, 2003 through Thursday, January 06, 2005
Serial Number : 132713D1 4F4837B3 41E04CF7 2497D9FA
Thumbprint (sha1) : 244FCB3C 2D9F2F21 4DC262F9 2008DEFA B490D10E
Thumbprint (md5) : 1EBA1EC0 2036AD70 6E5121A6 A136E4AC

22. Certificate is now installed.



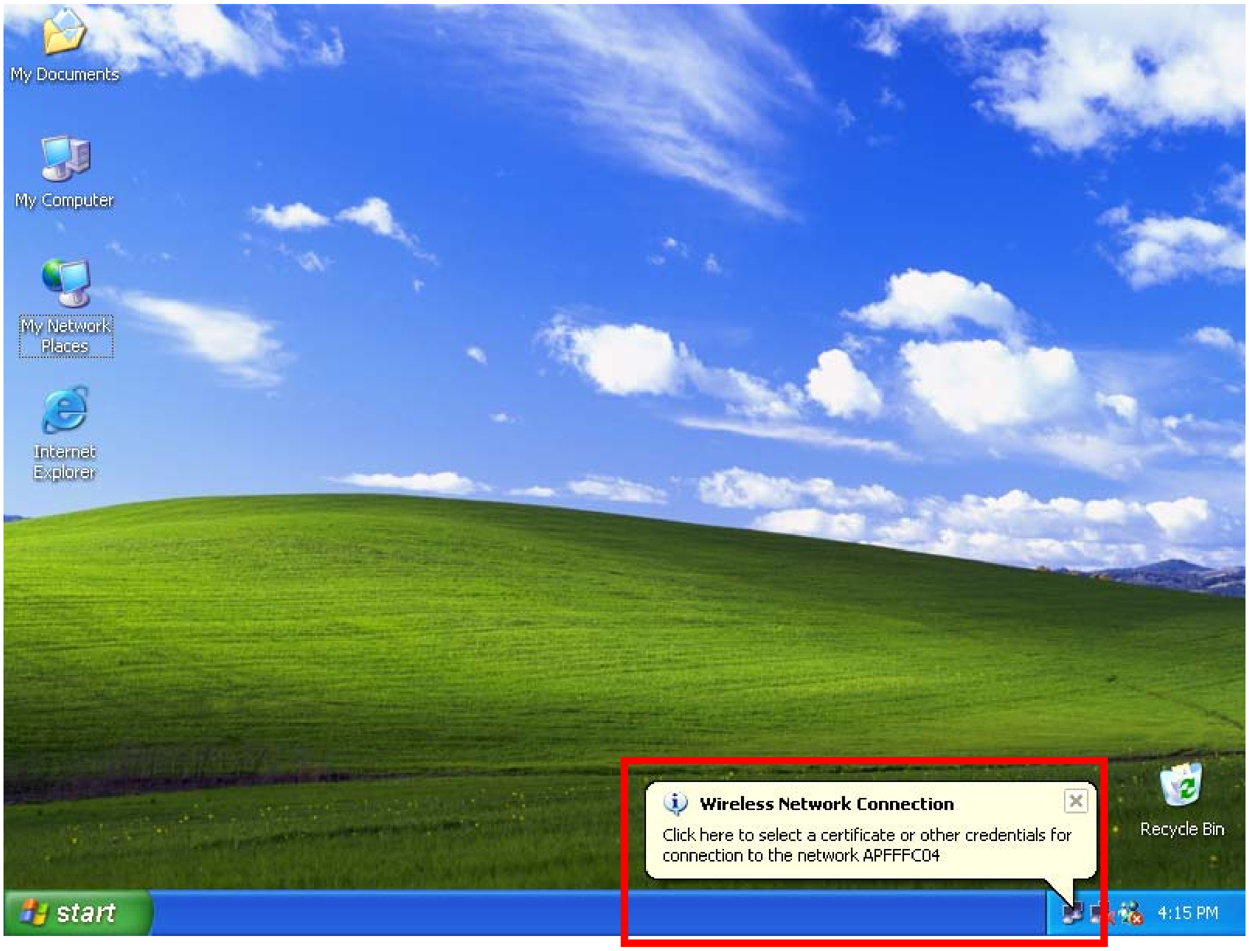
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrmpn.asp Go Links
Microsoft Certificate Services -- WirelessCA Home
Done Internet

Certificate Installed

Your new certificate has been successfully installed.

All the configuration and certificate download are now complete. Let's try to connect to the Access Point using 802.1x TLS Authentication.

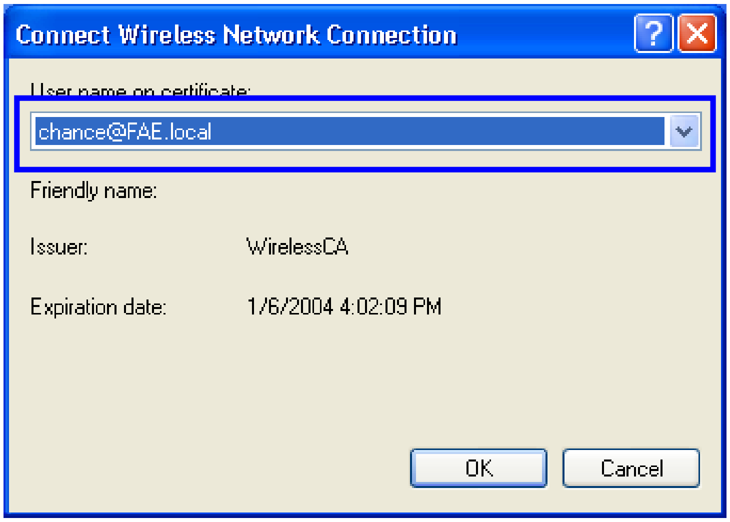
23. Windows XP will prompt you to select a certificate for wireless network connection. Click on the network connection icon in the system tray to continue.



Wireless Network Connection

Click here to select a certificate or other credentials for connection to the network APFFFC04

24. Select the certificate that was issued by the server (WirelessCA), and click “**OK**” to continue.



Connect Wireless Network Connection

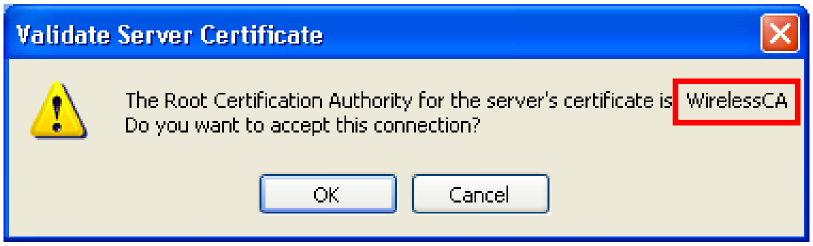
User name on certificate: chance@FAE.local

Friendly name:

Issuer: WirelessCA

Expiration date: 1/6/2004 4:02:09 PM

25. Check the server to make sure that it’s the server that issues certificate, and click “**OK**” to complete the authentication process.



Validate Server Certificate

The Root Certification Authority for the server's certificate is WirelessCA
Do you want to accept this connection?

MD5 Authentication

26. Select "**Data encryption (WEP enabled)**" option, but leave other option unselected.

27. Select the **key format** that you want to use to key in your Network key.

ASCII characters: 0~9, a~z and A~Z

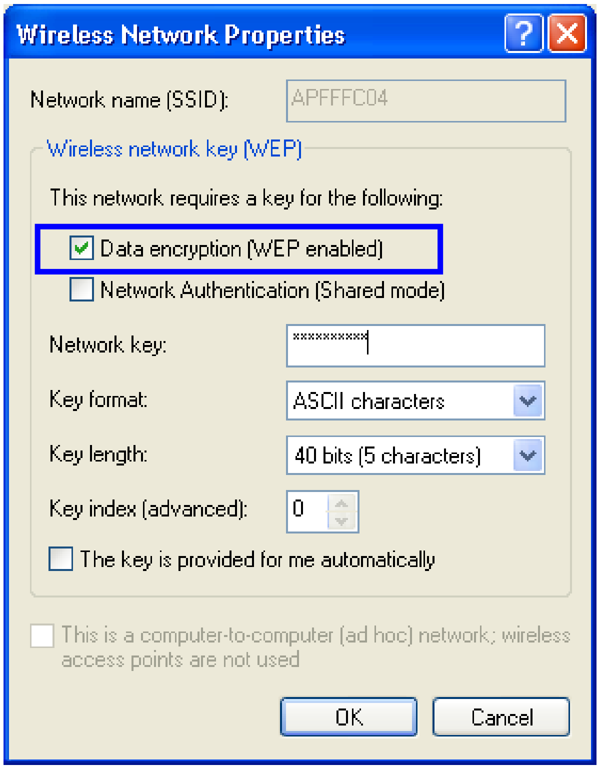
HEX characters: 0~9, a~f

28. Select the **key length** that you wish to use

40 bits (5 characters for ASCII, 10 characters for HEX)

104 bits (13 characters for ASCII, 26 characters for HEX)

29. After deciding the key format and key length that you wish to use for network key. Enter the network key in "**Network key**" text box.



Wireless Network Properties

Network name (SSID): APFFFC04

Wireless network key (WEP)

This network requires a key for the following:

☑ Data encryption (WEP enabled)

□ Network Authentication (Shared mode)

Network key: **********

Key format: ASCII characters

Key length: 40 bits (5 characters)

Key index (advanced): 0

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

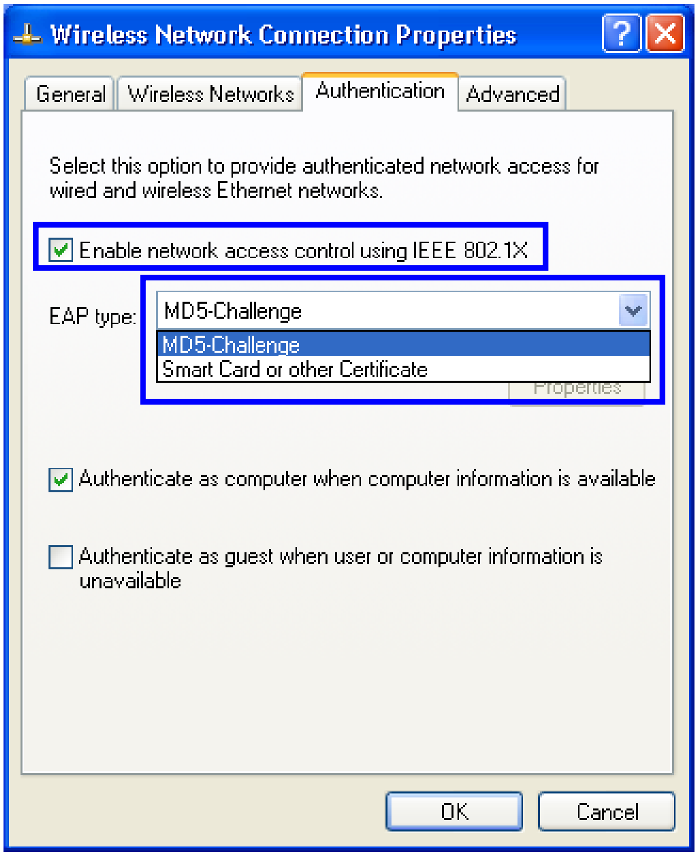
Please note that that value of Network key entered, and key format/length used, must be the same as that used in the Access Point. Although there are 4 set of keys can be set in the Access Point WEP configuration, it's the ***first set*** of key that must be the same as that we used by the supplicant wireless client.

30. Click "**OK**" to close the Wireless Network Properties window, thus make the changes effective.

31. Select “**Authentication**” tab.

32. Select “**Enable network access control using IEEE 802.1X**” to enable 802.1x authentication.

33. Select “**MD-5 Challenge**” from the drop-down list box for EAP type.



Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: MD5-Challenge

MD5-Challenge
Smart Card or other Certificate

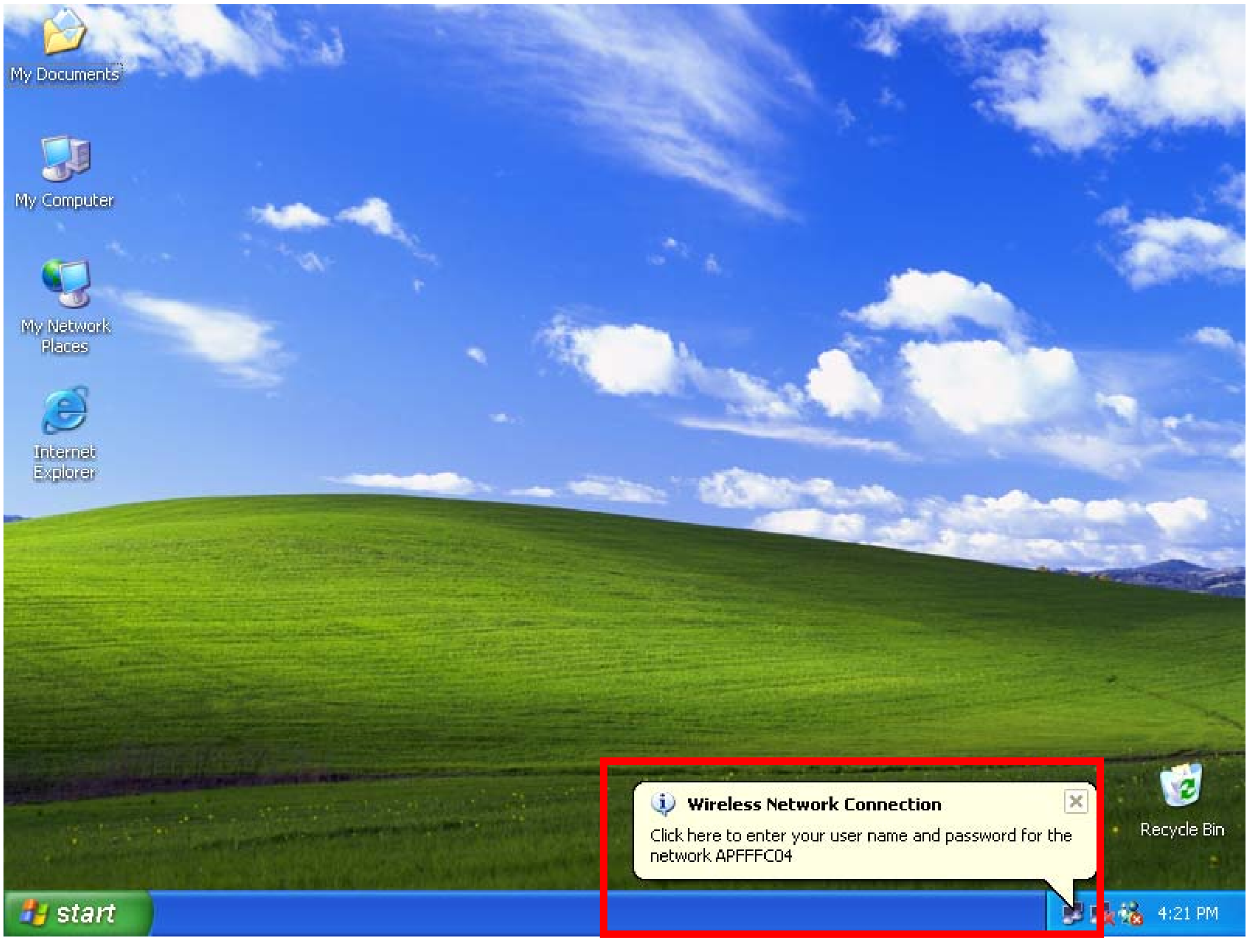
☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

34. Click “**OK**” to close Wireless Network Connection Properties window, thus make all the changes effective.

Unlike TLS, which uses digital certificate for validation, the MD-5 Authentication is based on the user account/password. Therefore, you must have a valid account used by the server for validation.

35. WindowsXP will prompt you to enter your user name and password. Click on the network connection icon in the system tray to continue.

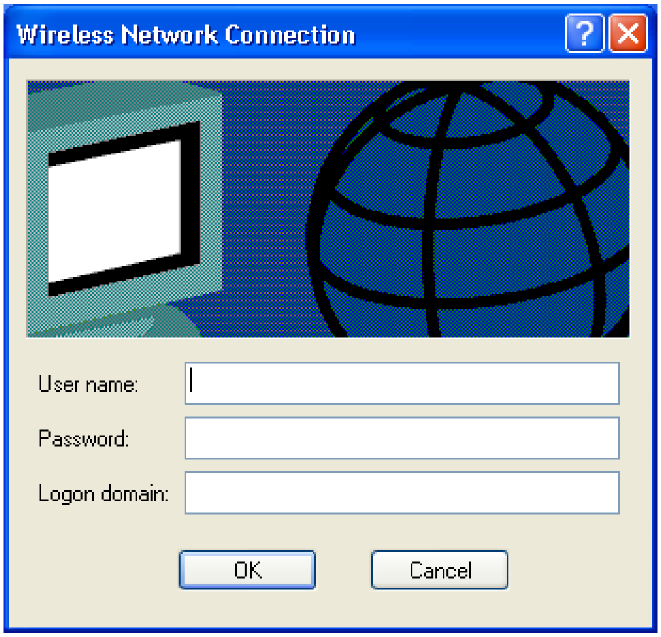


Wireless Network Connection

Click here to enter your user name and password for the network APFFFC04

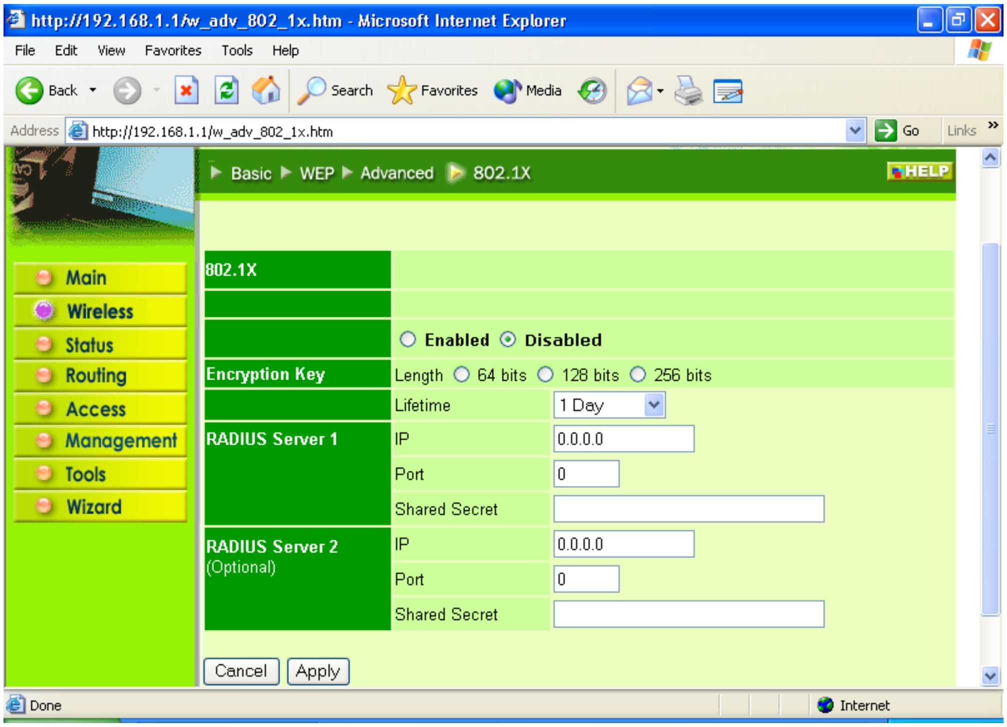
36. Enter the user name, password and the logon domain that your account belongs if you have one or more network domain exist in your network.

37. Click "**OK**" to complete the validation process.



Authenticator: Wireless Network Router

This is the web page configuration in the Router that we use.


http://192.168.1.1/w_adv_802_1x.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/w_adv_802_1x.htm
Go Links
Basic WEP Advanced 802.1X
HELP
Main
Wireless
Status
Routing
Access
Management
Tools
Wizard
Cancel
Apply
Done
Internet

802.1X		
	○ Enabled ● Disabled	
Encryption Key	Length ○ 64 bits ○ 128 bits ○ 256 bits	
	Lifetime	1 Day
RADIUS Server 1	IP	0.0.0.0
	Port	0
	Shared Secret	
RADIUS Server 2 (Optional)	IP	0.0.0.0
	Port	0
	Shared Secret	

1. Enable 802.1x security by selecting "**Enable**".

2. Select the **Encryption Key Length Size** ranging from 64 to 256 Bits that you would like to use.Select the **Life-time of the Encryption Key** from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.

1. Enter the **IP address** of and the **Port** used by the **Primary** Radius Server

Enter the **Shared Secret**, which is used by the Radius Server.

6. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.

Click "**Help**" to get interpretation for Encryption Key and Radius Server

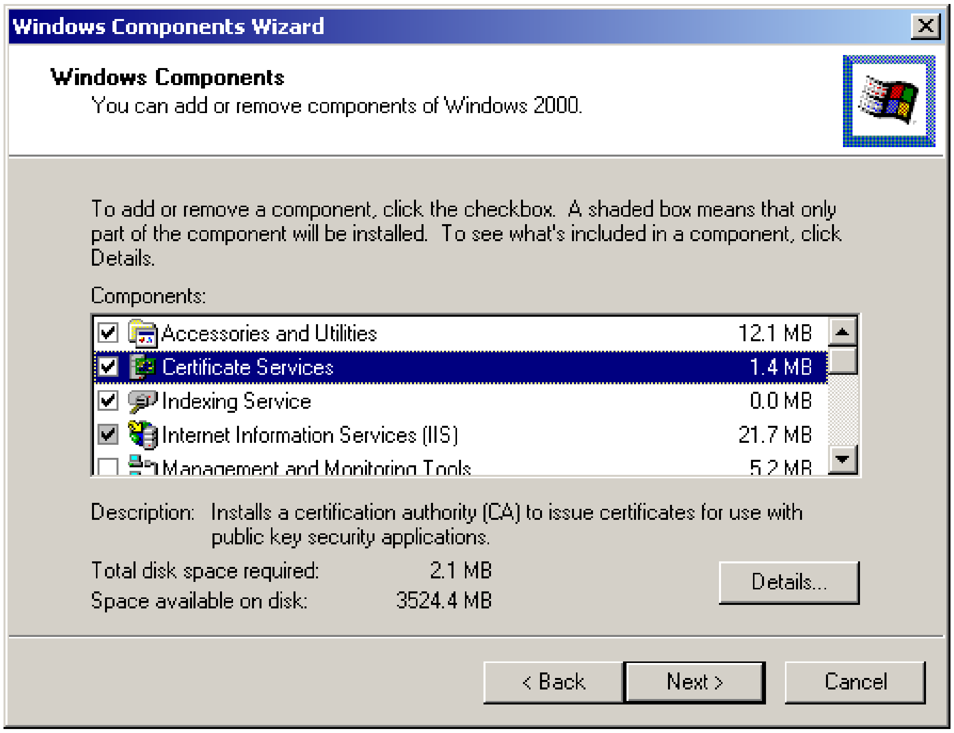
7. Click "**Apply**" button for the 802.1x settings to take effect after Access Point reboots itself.

Note! As soon as 802.1x security is enabled, all the wireless client stations that are connected to the Router currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.

Radius Server: Window2000 Server

This section to help those who has Windows 2000 Server installed and wants to setup Windows2000 Server for 802.1x authentication, which includes setting up Certificate Service for TLS Authentication, and enable EAP-methods.

1. Login into your Windows 2000 Server as Administrator, or account that has Administrator authority.
2. Go to **Start** > **Control Panel**, and double-click "Add or Remove Programs"
3. Click on "**Add/Remove Windows components**"
4. Check "**Certificate Services**", and click "Next" to continue.



Windows Components Wizard

Windows Components

You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

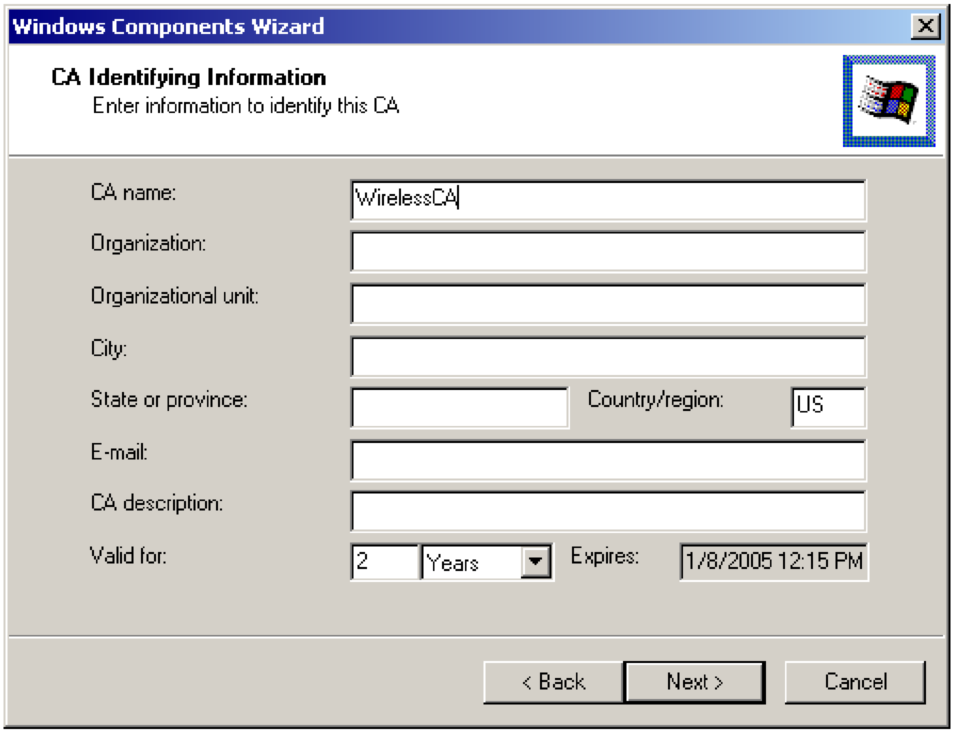
☑ Accessories and Utilities	12.1 MB
☑ Certificate Services	1.4 MB
☑ Indexing Service	0.0 MB
☑ Internet Information Services (IIS)	21.7 MB
☐ Management and Monitoring Tools	5.2 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security applications.

Total disk space required: 2.1 MB

Space available on disk: 3524.4 MB

5. Select "**Enterprise root CA**", and click "**Next**" to continue.



CA Identifying Information

Enter information to identify this CA

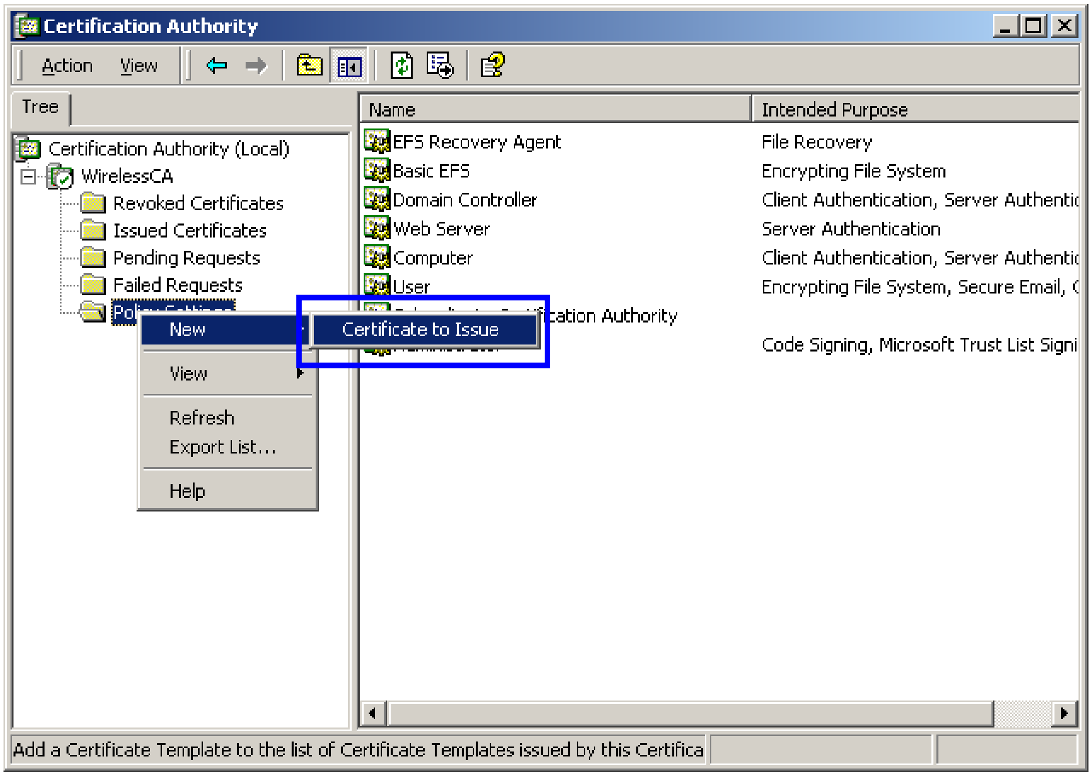
CA name:	WirelessCA
Organization:	
Organizational unit:	
City:	
State or province:	
Country/region:	US
E-mail:	
CA description:	
Valid for:	2 Years
Expires:	1/8/2005 12:15 PM

6. Enter the information that you want for your Certificate Service, and click "**Next**" to continue.

7. Go to Start > Program > Administrative Tools > **Certificate Authority**

8. Right-click on the "**Policy Setting**", select "**new**"

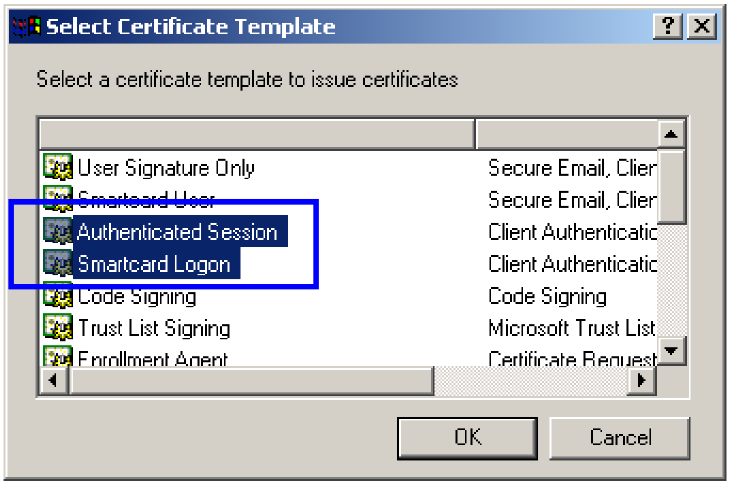
9. Select "**Certificate to Issue**"



Name	Intended Purpose
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic
User	Encrypting File System, Secure Email, C
...ation Authority	
	Code Signing, Microsoft Trust List Signi

Add a Certificate Template to the list of Certificate Templates issued by this Certifica

10. Select "**Authenticated Session**" and "**Smartcard Logon**" by holding down to the Ctrl key, and click "**OK**" to continue.

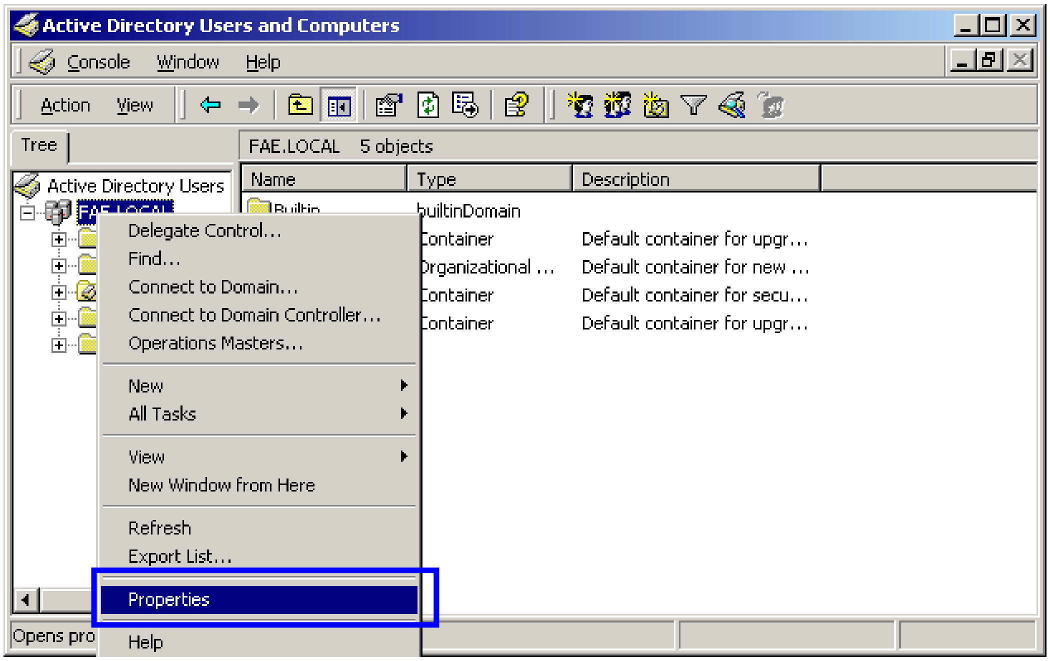


Select a certificate template to issue certificates

User Signature Only	Secure Email, Clier
Smartcard User	Secure Email, Clier
Authenticated Session	Client Authenticatic
Smartcard Logon	Client Authenticatic
Code Signing	Code Signing
Trust List Signing	Microsoft Trust List
Enrollment Agent	Certificate Request

11. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.

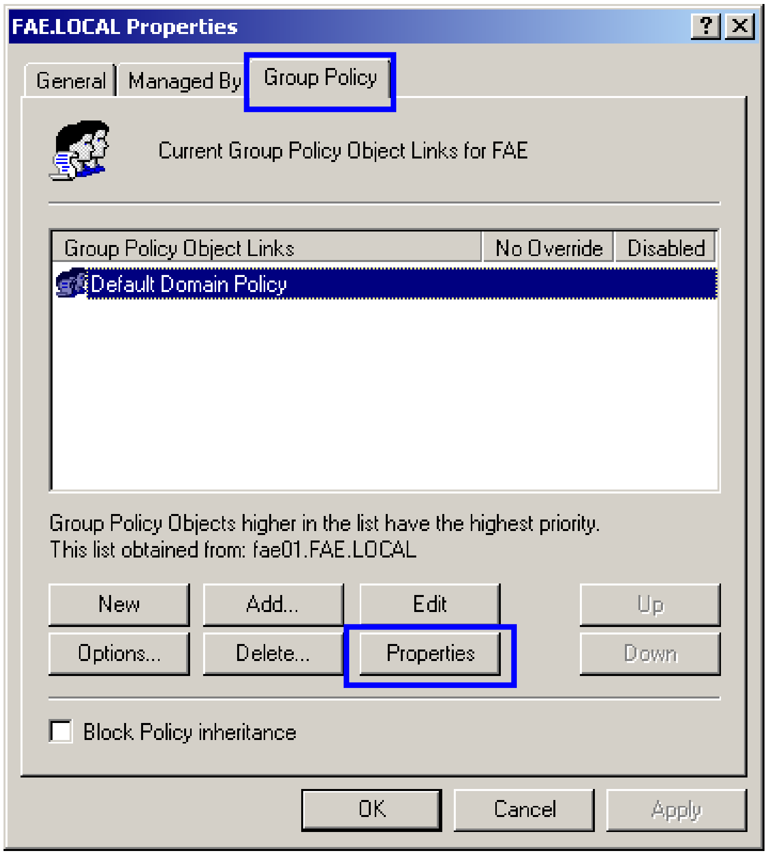
12. Right-click on domain, and select "**Properties**" to continue.



FAE.LOCAL 5 objects

Name	Type	Description
Builtin	builtinDomain	
	Container	Default container for upgr...
	Organizational ...	Default container for new ...
	Container	Default container for secu...
	Container	Default container for upgr...

13. Select "**Group Policy**" tab and click "**Properties**" to continue.



Current Group Policy Object Links for FAE

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

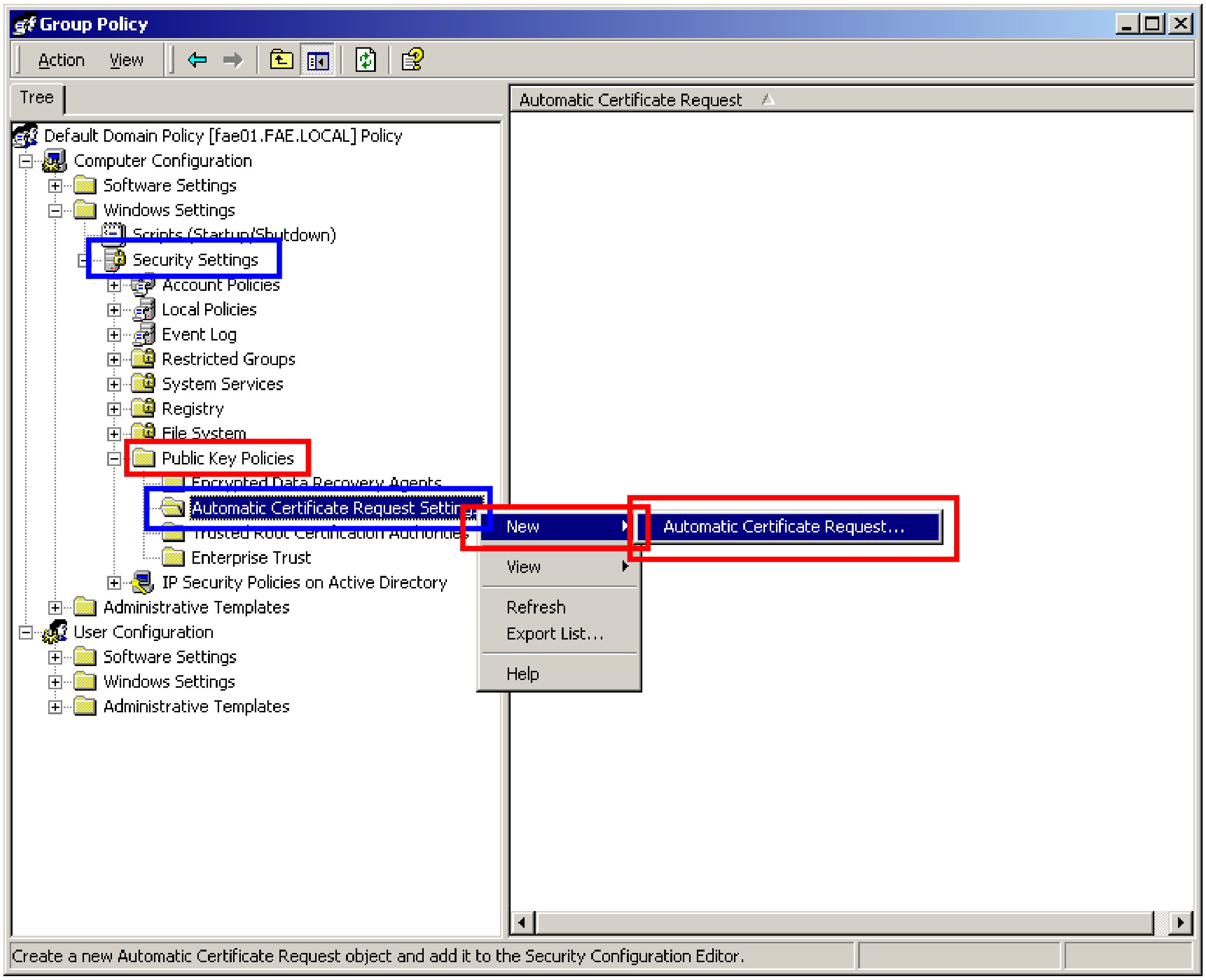
Group Policy Objects higher in the list have the highest priority.
This list obtained from: fae01.FAE.LOCAL

□ Block Policy inheritance

14. Go to “Computer Configuration” > “Security Settings” > “**Public Key Policies**”

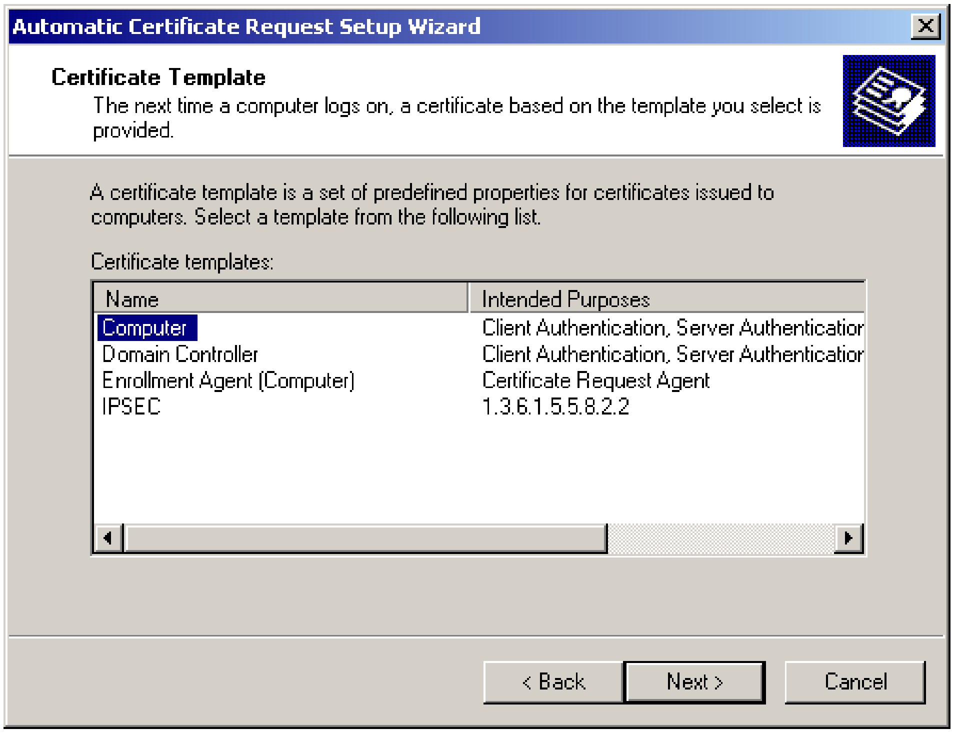
15. Right-click “**Automatic Certificate Request Setting**”, and select “**New**”

16. Click “**Automatic Certificate Request ...**”



Create a new Automatic Certificate Request object and add it to the Security Configuration Editor.

17. The Automatic Certificate Request Setup Wizard will guide you through the Automatic Certificate Request setup, simply click "**Next**" through to the last step.



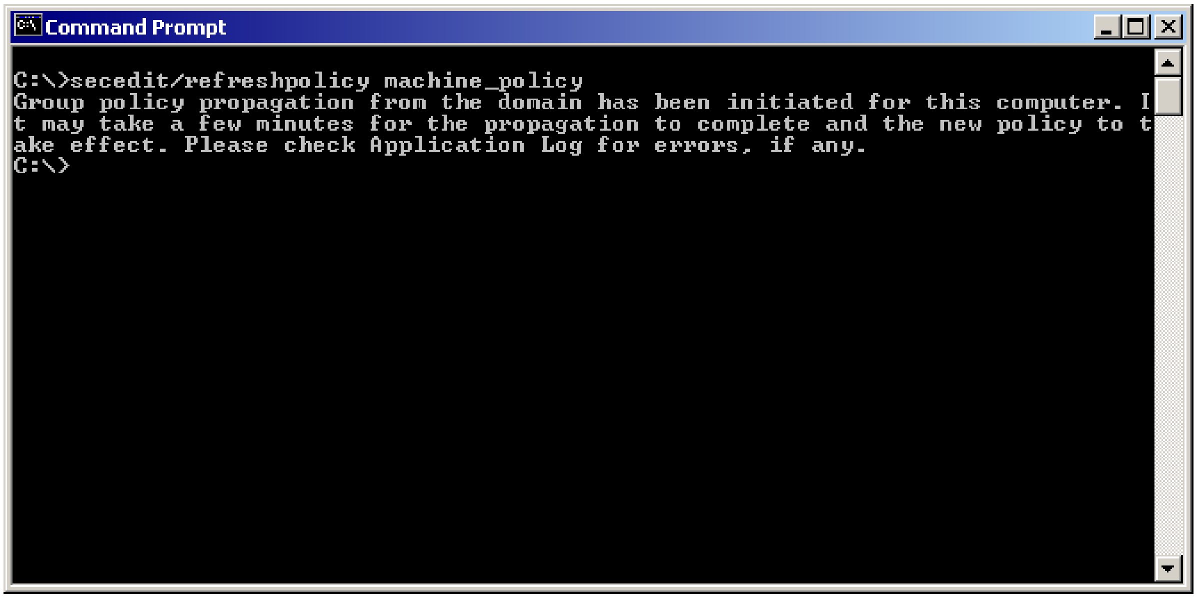
The next time a computer logs on, a certificate based on the template you select is provided.

A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

Certificate templates:

Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSEC	1.3.6.1.5.5.8.2.2

18. Click "**Finish**" to complete the Automatic Certificate Request Setup



```
C:\>secedit/refreshpolicy machine_policy
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>
```

19. Go to Start > **Run**, and type "**command**" and click "**Enter**" to open Command Prompt.

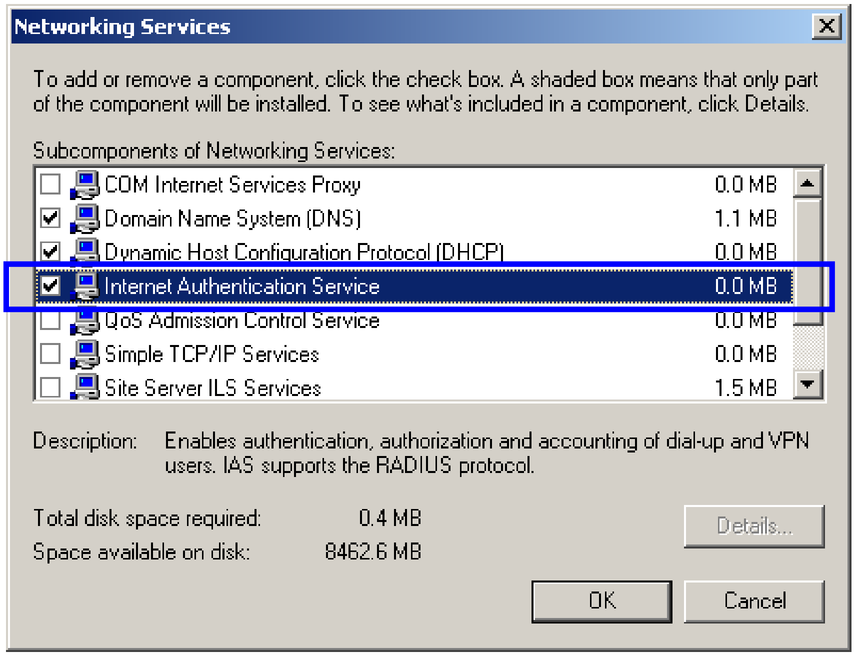
20. Type "secedit/refreshpolicy machine_policy" to refresh policy.

Adding Internet Authentication Service

21. Go to Start > Control Panel > **Add or Remove Programs**

22. Select “**Add/Remove Windows Components**” from the panel on the left.

23. Select “**Internet Authentication Service**”, and click “**OK**” to install.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	COM Internet Services Proxy	0.0 MB
☑	Domain Name System (DNS)	1.1 MB
☑	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑	Internet Authentication Service	0.0 MB
□	QoS Admission Control Service	0.0 MB
□	Simple TCP/IP Services	0.0 MB
□	Site Server ILS Services	1.5 MB

Description: Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.

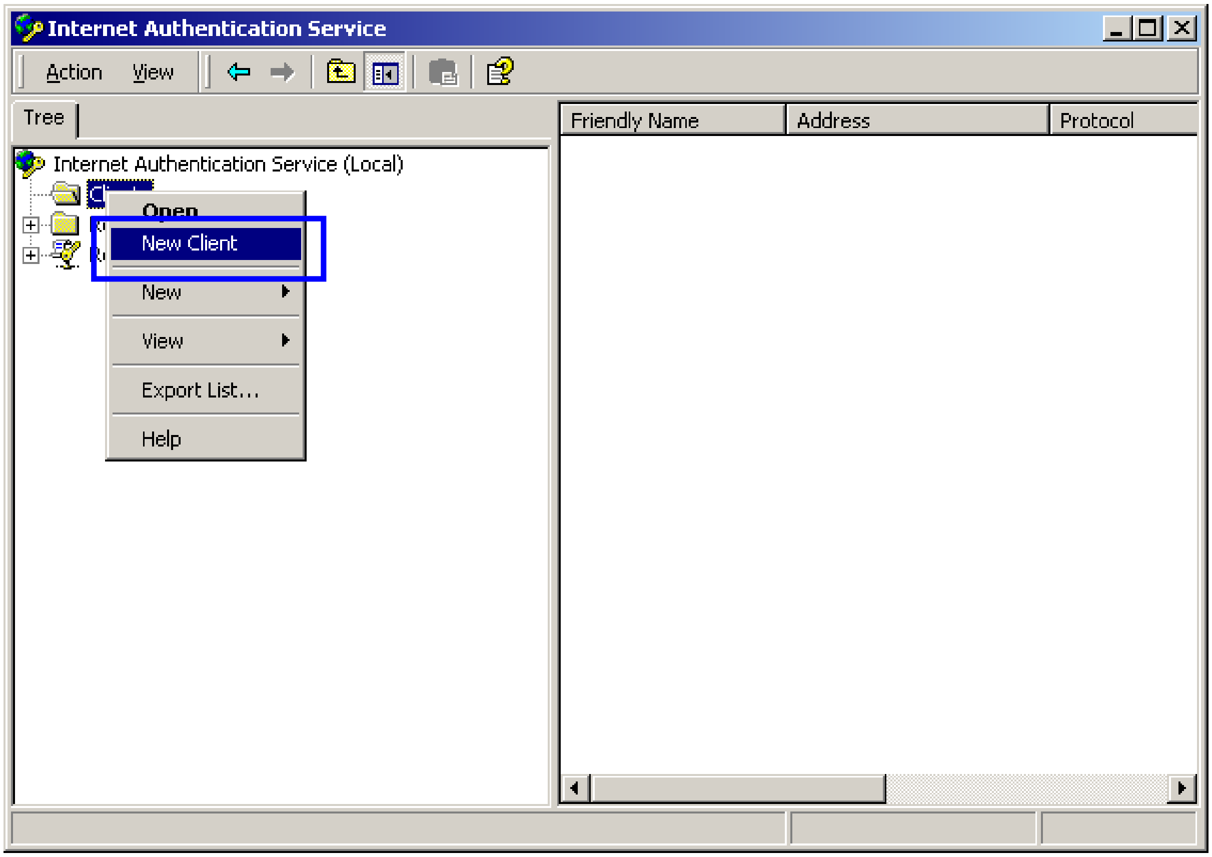
Total disk space required: 0.4 MB

Space available on disk: 8462.6 MB

Setting Internet Authentication Service

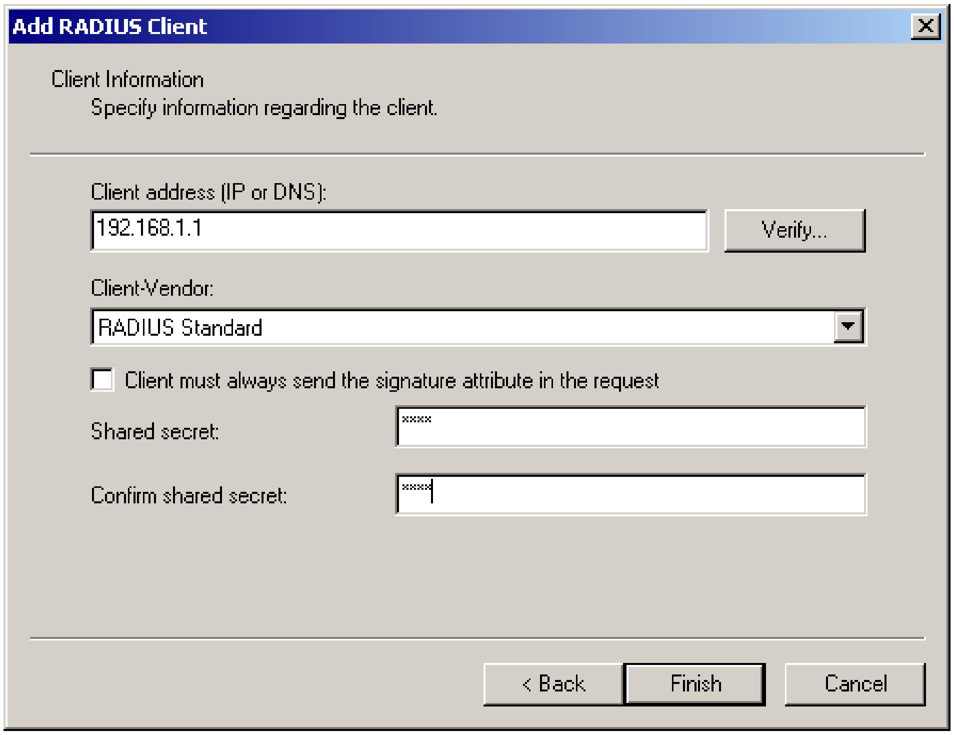
24. Go to Start > Program > Administrative Tools > **Internet Authentication Service**

25. Right-click "**Client**", and select "**New Client**"



26. Enter the IP address of the Access Point in the **Client address** text field, a memorable name for the Access Point in the **Client-Vendor** text field, the access password used by the Access Point in the **Shared secret** text field. Re-type the password in the **Confirmed shared secret** text field.

27. Click "Finish" to complete adding of the Access Point.



Add RADIUS Client

Client Information

Specify information regarding the client.

Client address (IP or DNS): 192.168.1.1

Client-Vendor: RADIUS Standard

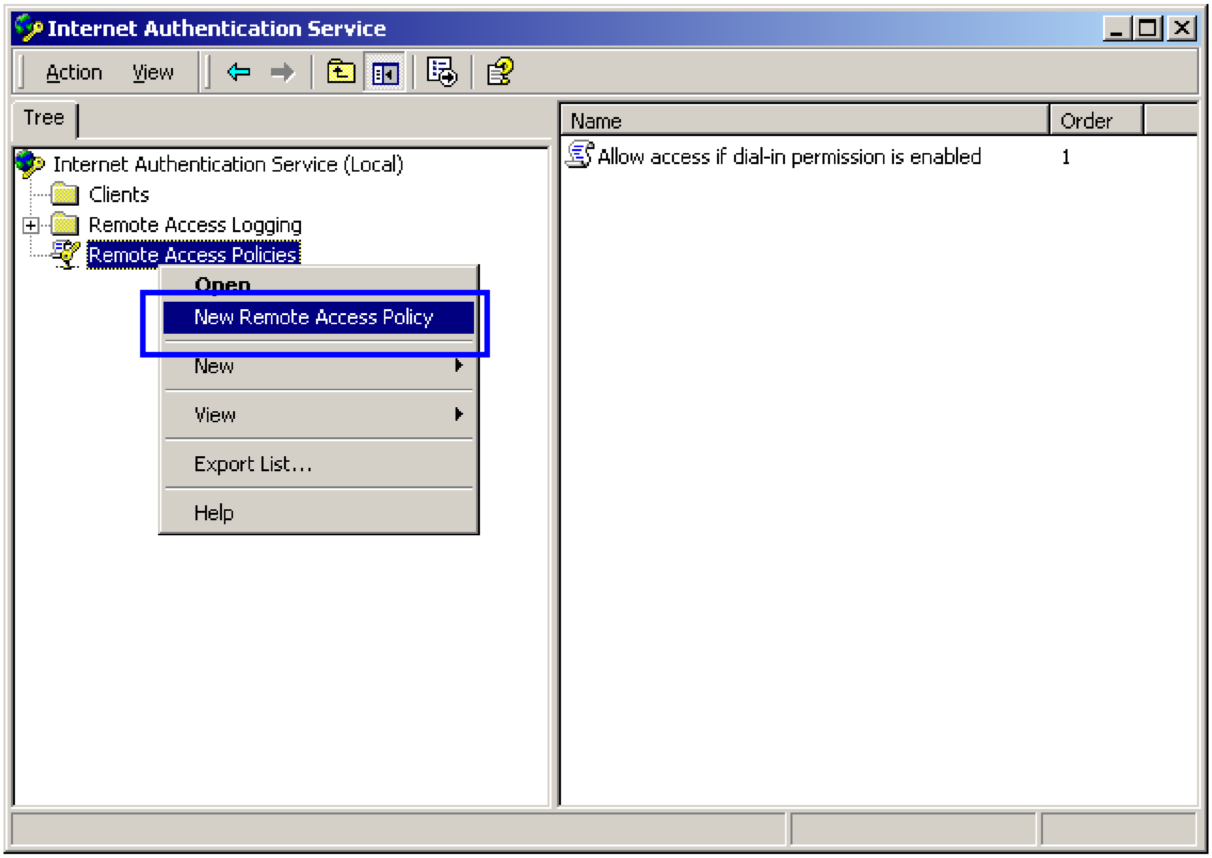
□ Client must always send the signature attribute in the request

Shared secret: ****

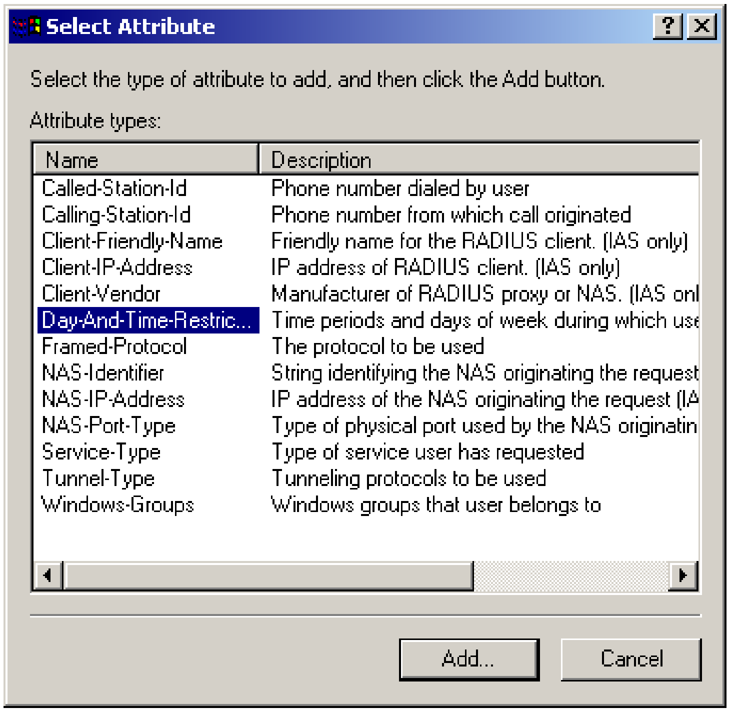
Confirm shared secret: ****

28. In the Internet Authentication Service, right-click "**Remote Access Policies**"

29. Select "New Remote Access Policy".



30. Select "**Day-And-Time-Restriction**", and click "**Add**" to continue.

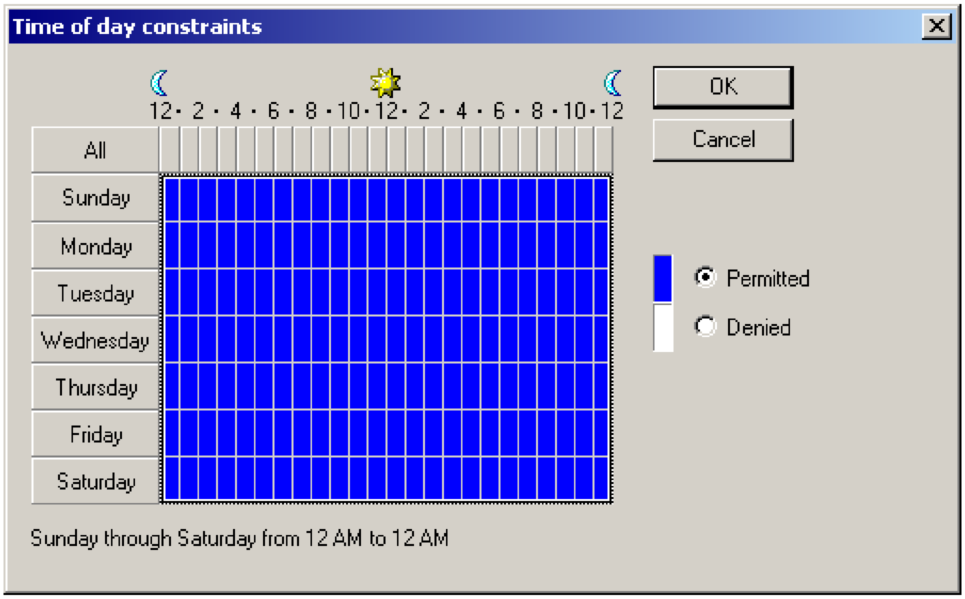


Select the type of attribute to add, and then click the Add button.

Attribute types:

Name	Description
Called-Station-Id	Phone number dialed by user
Calling-Station-Id	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (IAS only)
Client-IP-Address	IP address of RADIUS client. (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS. (IAS onl
Day-And-Time-Restric...	Time periods and days of week during which use
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originating the request
NAS-IP-Address	IP address of the NAS originating the request (IA
NAS-Port-Type	Type of physical port used by the NAS originatin
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used
Windows-Groups	Windows groups that user belongs to

31. Unless you want to specify the active duration for 802.1x authentication, click “**OK**” to accept to have 802.1x authentication enabled at all times.

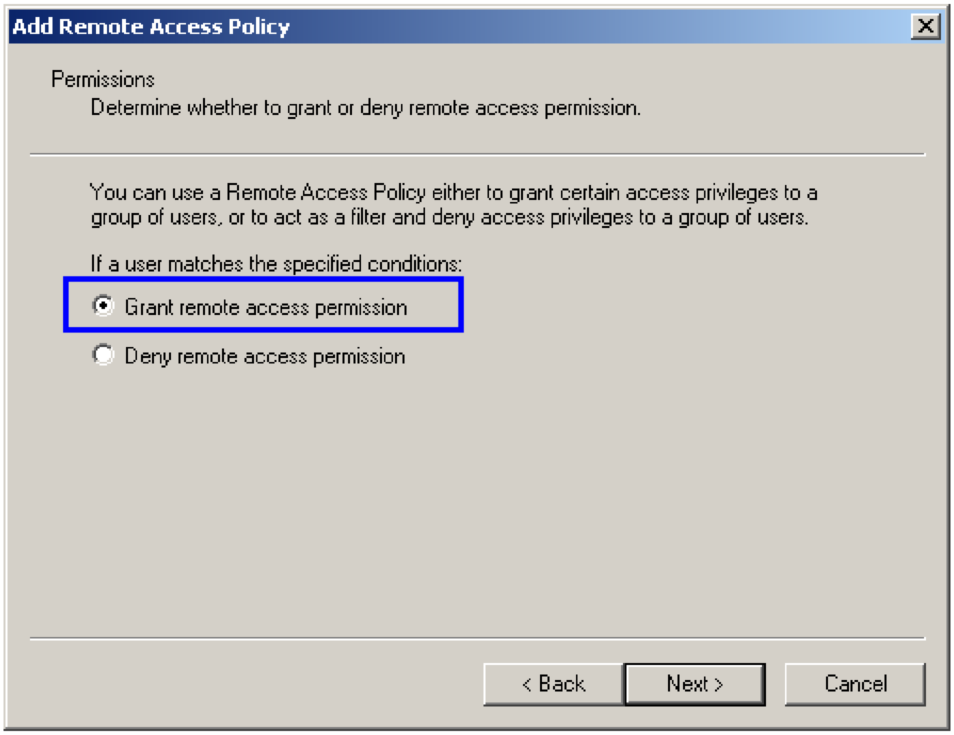


● Permitted

○ Denied

Sunday through Saturday from 12 AM to 12 AM

32. Select “**Grant remote access permission**”, and click “**Next**” to continue.



Permissions

Determine whether to grant or deny remote access permission.

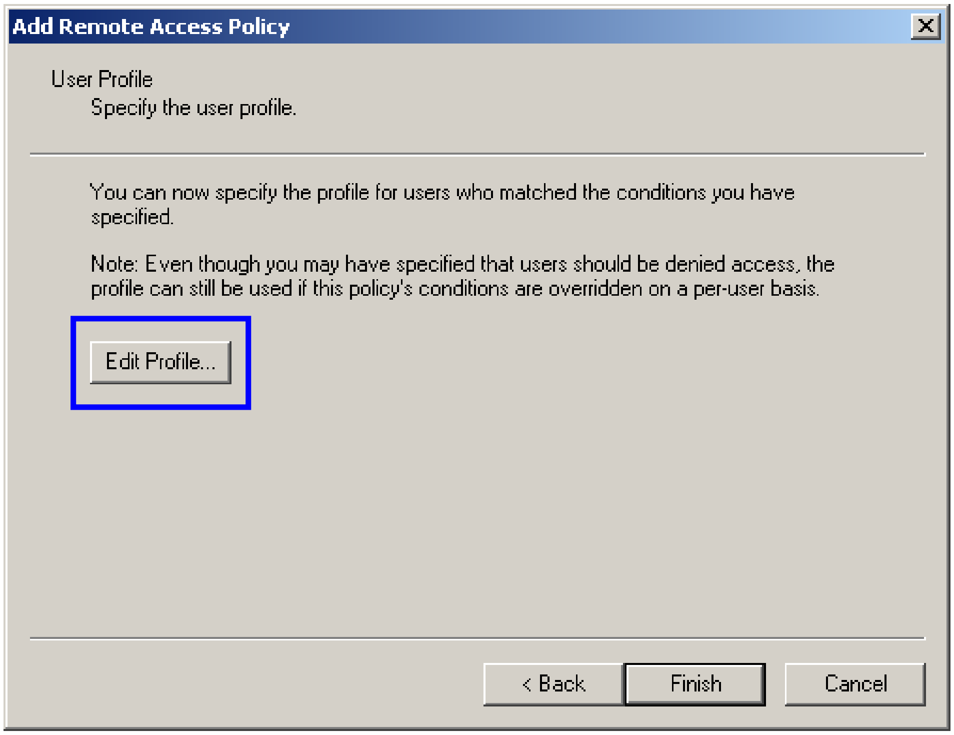
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.

If a user matches the specified conditions:

● Grant remote access permission

○ Deny remote access permission

33. Click "Edit Profile" to open up



Add Remote Access Policy

User Profile

Specify the user profile.

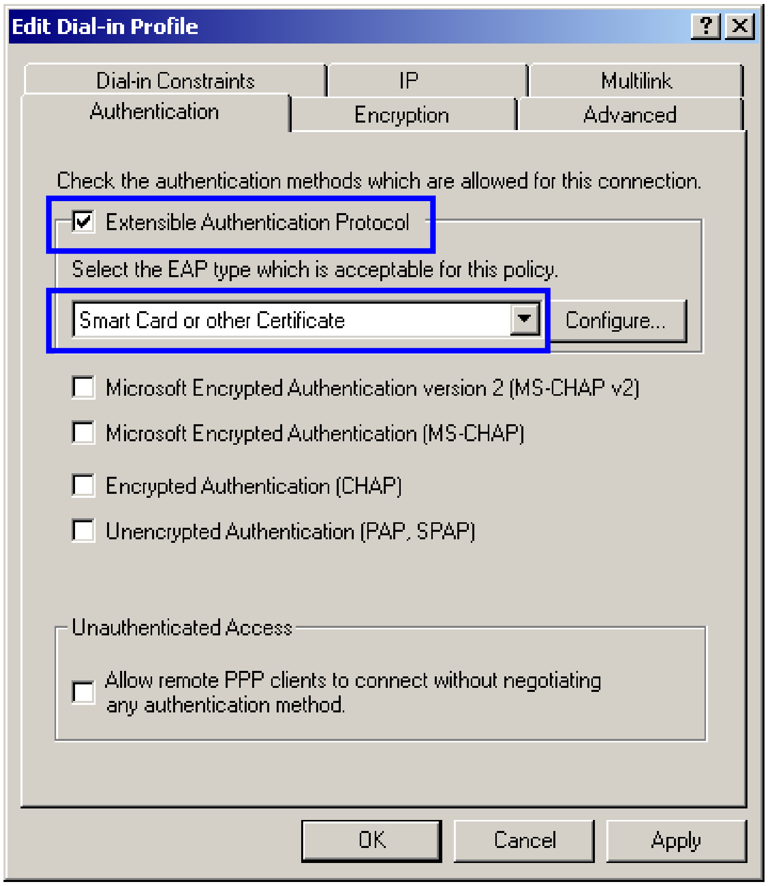
You can now specify the profile for users who matched the conditions you have specified.

Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.

For TLS Authentication Setup (Steps 34 ~ 38)

34. Select "**Authentication**" Tab

35. Enable "**Extensible Authentication Protocol**", and select "**Smart Card or other Certificate**" for **TLS** authentication



Edit Dial-in Profile

Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

Smart Card or other Certificate ▾

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

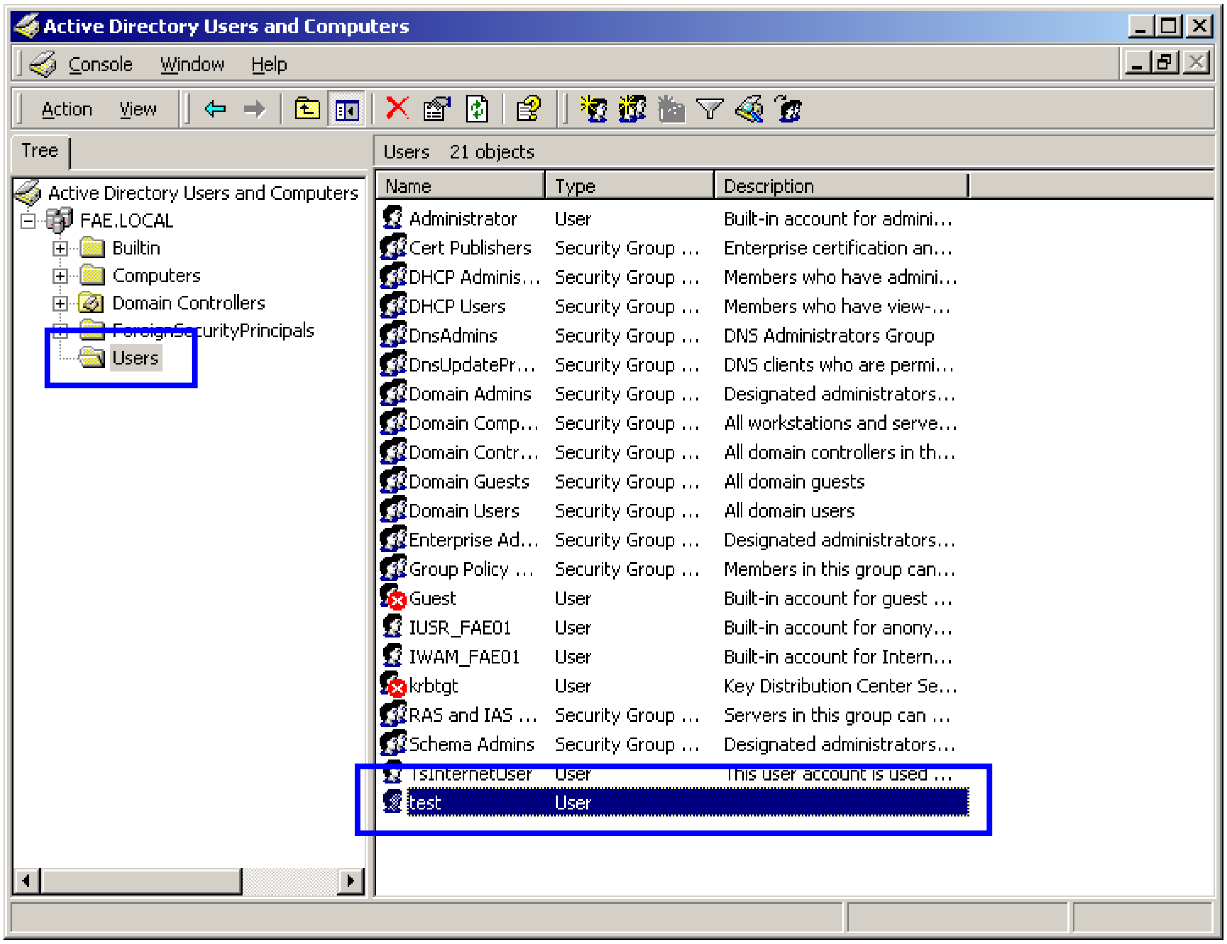
□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

36. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**

37. Select "**Users**", and double-click on the user that can be newly created or currently existing, who will be configured to have the right to obtain digital certificate remotely.



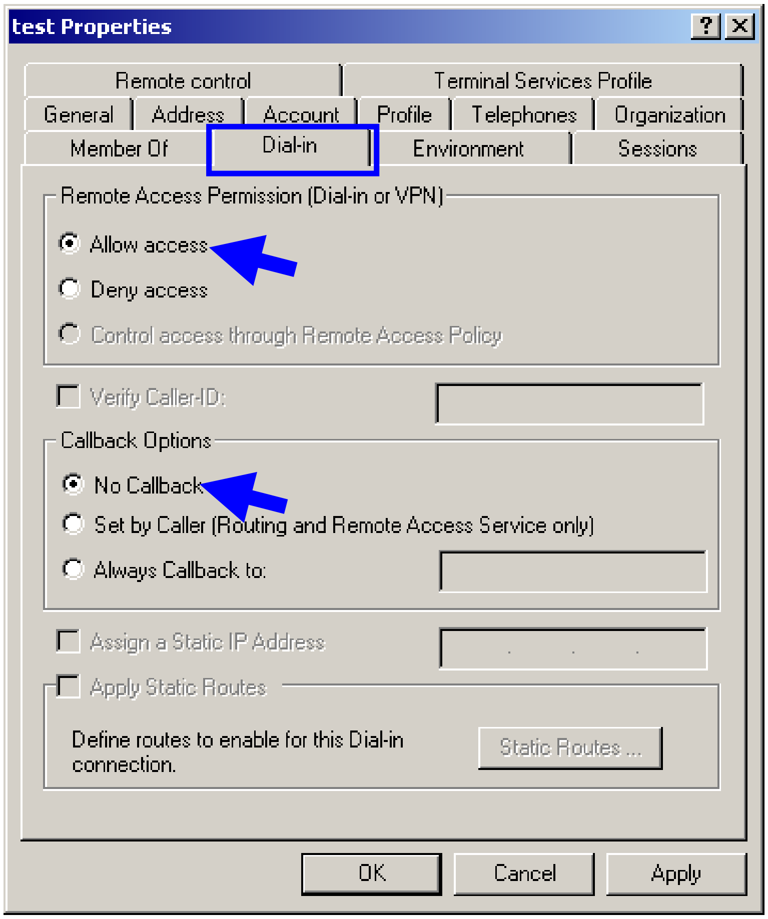
Active Directory Users and Computers
FAE.LOCAL
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Users 21 objects

Name	Type	Description
Administrator	User	Built-in account for admini…
Cert Publishers	Security Group …	Enterprise certification an…
DHCP Adminis…	Security Group …	Members who have admini…
DHCP Users	Security Group …	Members who have view-…
DnsAdmins	Security Group …	DNS Administrators Group
DnsUpdatePr…	Security Group …	DNS clients who are permi…
Domain Admins	Security Group …	Designated administrators…
Domain Comp…	Security Group …	All workstations and serve…
Domain Contr…	Security Group …	All domain controllers in th…
Domain Guests	Security Group …	All domain guests
Domain Users	Security Group …	All domain users
Enterprise Ad…	Security Group …	Designated administrators…
Group Policy …	Security Group …	Members in this group can…
Guest	User	Built-in account for guest …
IUSR_FAE01	User	Built-in account for anony…
IWAM_FAE01	User	Built-in account for Intern…
krbtgt	User	Key Distribution Center Se…
RAS and IAS …	Security Group …	Servers in this group can …
Schema Admins	Security Group …	Designated administrators…
TsInternetUser	User	This user account is used …
test	User	

Please note that in this case, we have a user called, **test**, whose account/password are used to obtain the digital certificate from server.

38. Go to the “**Dial-in**” tab, and check “**Allow access**” option for Remote Access Permission and “**No Call-back**” for Callback Options.



Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

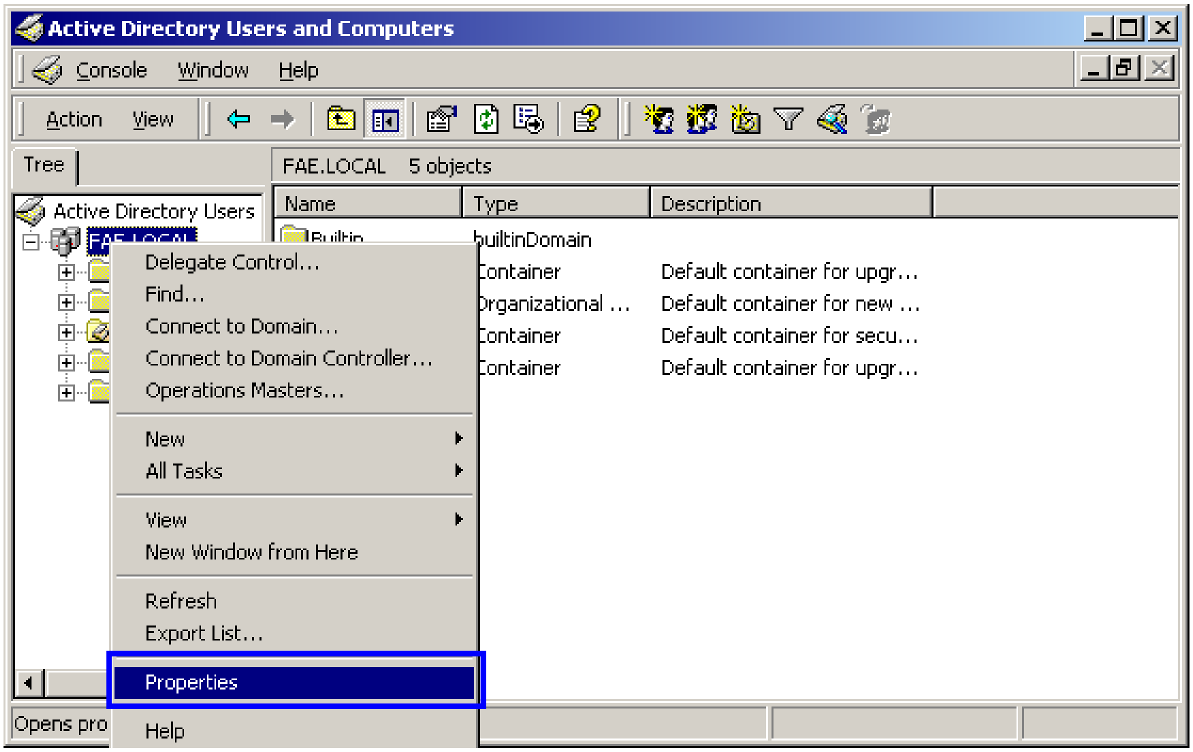
□ Apply Static Routes

Define routes to enable for this Dial-in connection.

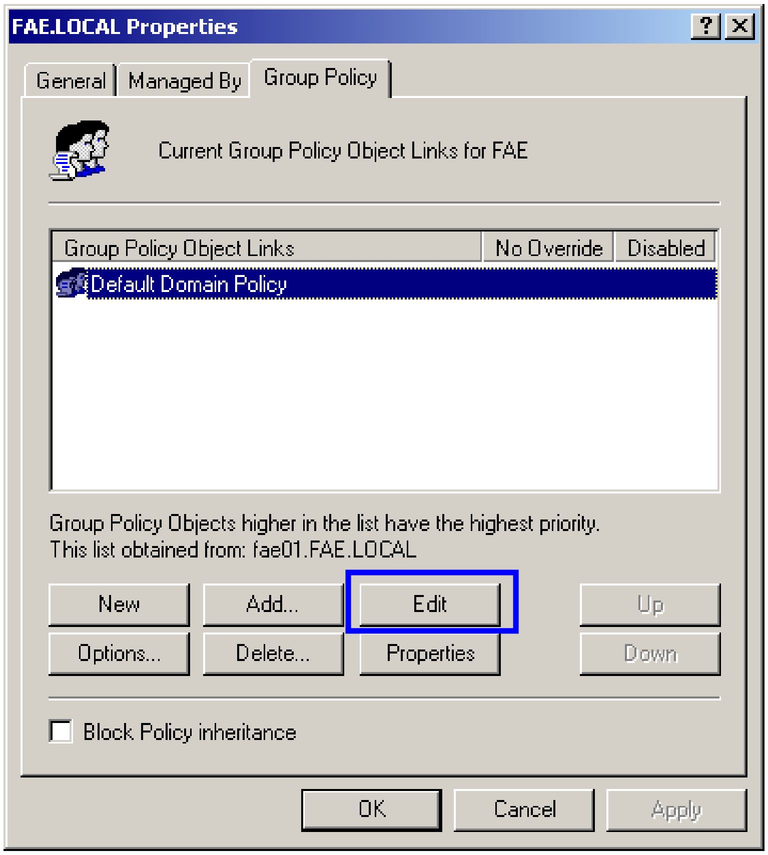
For MD5 Authentication (Steps 39 ~ 54)

39. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers.**

40. Right click on the domain, and select "**Properties**"



41. Select “**Group Policy**” tab, and click “**Edit**” to edit the Group Policy.



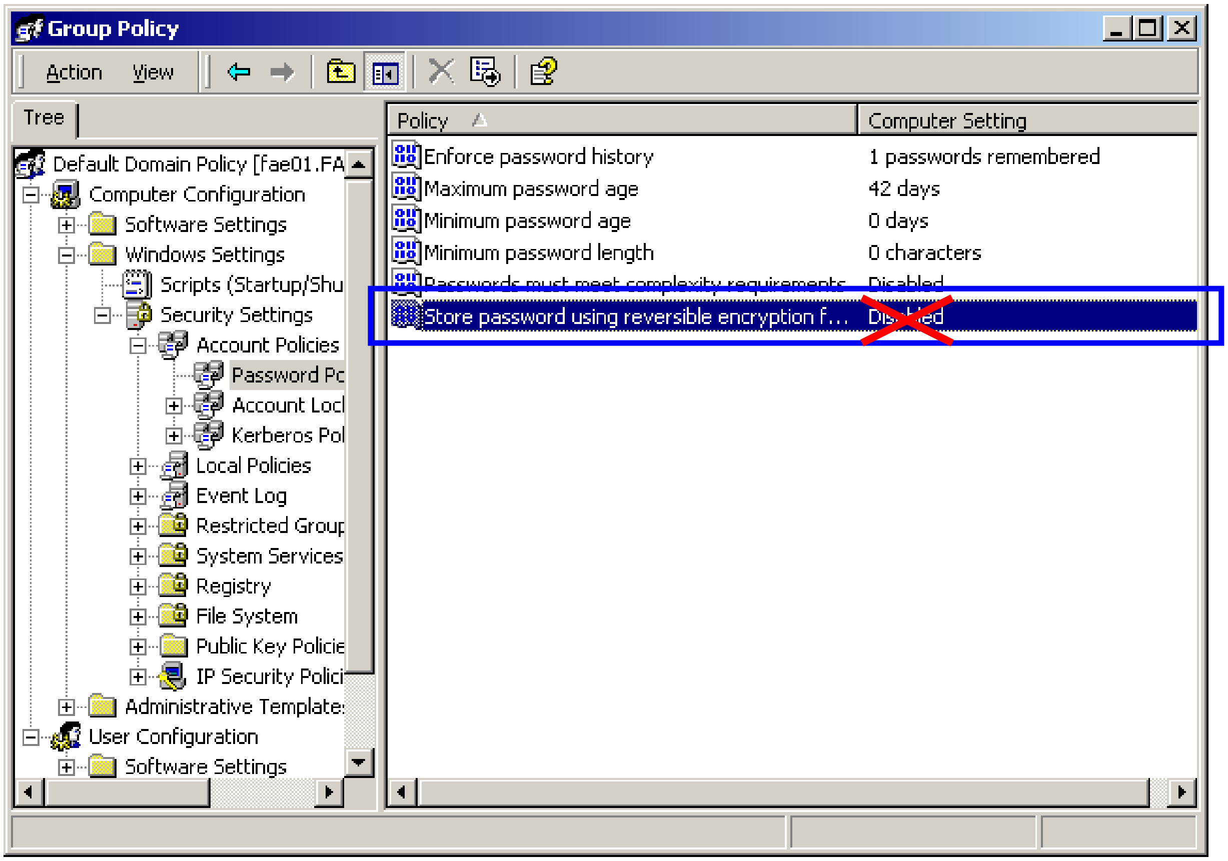
Current Group Policy Object Links for FAE

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: fae01.FAE.LOCAL

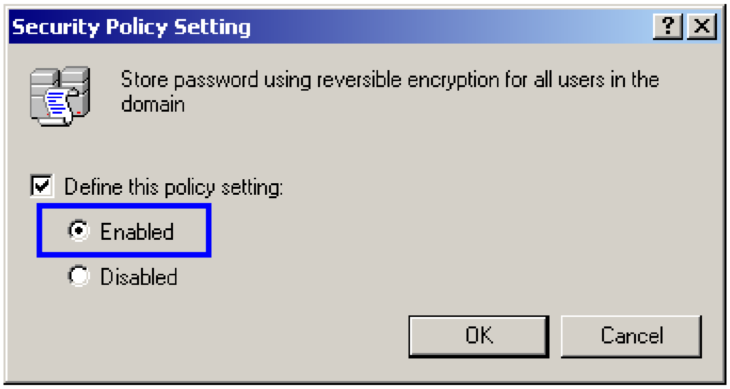
□ Block Policy inheritance

42. Go to “Computer Configuration” > “Windows Settings” > “Security Settings” > “Account Policies” > “**Password Policies**”



Policy	Computer Setting
Enforce password history	1 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Passwords must meet complexity requirements	Disabled
Store password using reversible encryption f...	Disabled

43. Click “**Define this policy setting**”, select “**Enabled**”, and click “**OK**” to continue.



Store password using reversible encryption for all users in the domain

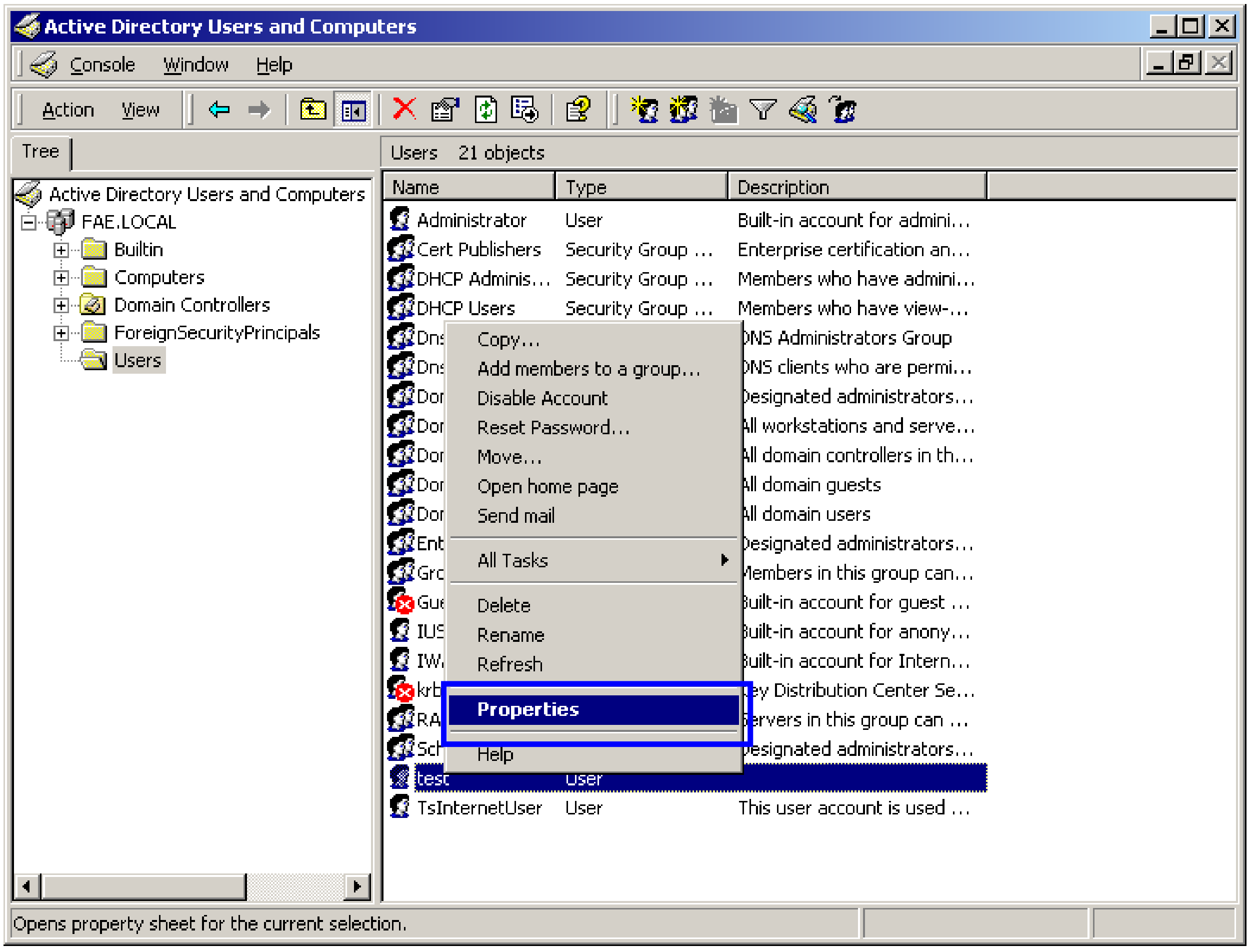
☑ Define this policy setting:

● Enabled

○ Disabled

44. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.

45. Go to **Users.** Right-click on the user that you are granting access, and select “**Properties**”



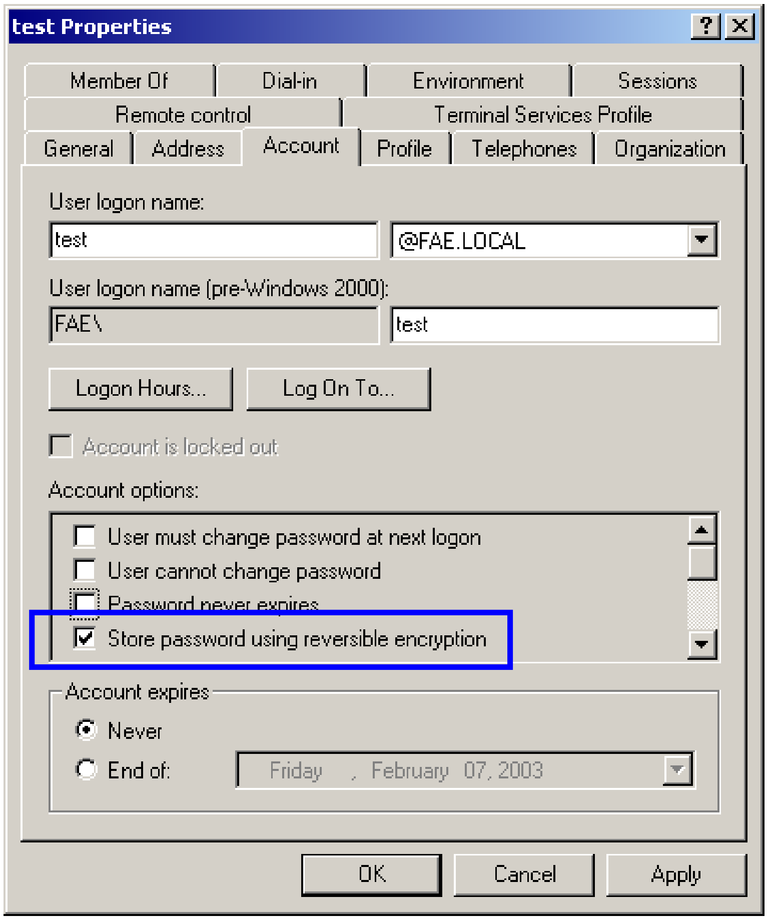
Users 21 objects

Name	Type	Description
Administrator	User	Built-in account for admini…
Cert Publishers	Security Group …	Enterprise certification an…
DHCP Adminis…	Security Group …	Members who have admini…
DHCP Users	Security Group …	Members who have view-…
Dns		NS Administrators Group
Dns		NS clients who are permi…
Dor		esignated administrators…
Dor		ll workstations and serve…
Dor		ll domain controllers in th…
Dor		ll domain guests
Dor		ll domain users
Ent		esignated administrators…
Grc		embers in this group can…
Gue		uilt-in account for guest …
IUS		uilt-in account for anony…
IW		uilt-in account for Intern…
krb		ey Distribution Center Se…
RA		ervers in this group can …
Sch		esignated administrators…
test	User	
TsInternetUser	User	This user account is used …

Opens property sheet for the current selection.

46. Go to "**Account**" tab, and enable "**Store password using reversible encryption**"

47. Click "**OK**" to continue.



User logon name:
test @FAE.LOCAL

User logon name (pre-Windows 2000):
FAE\ test

□ Account is locked out

Account options:

- □ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- ☑ Store password using reversible encryption

Account expires

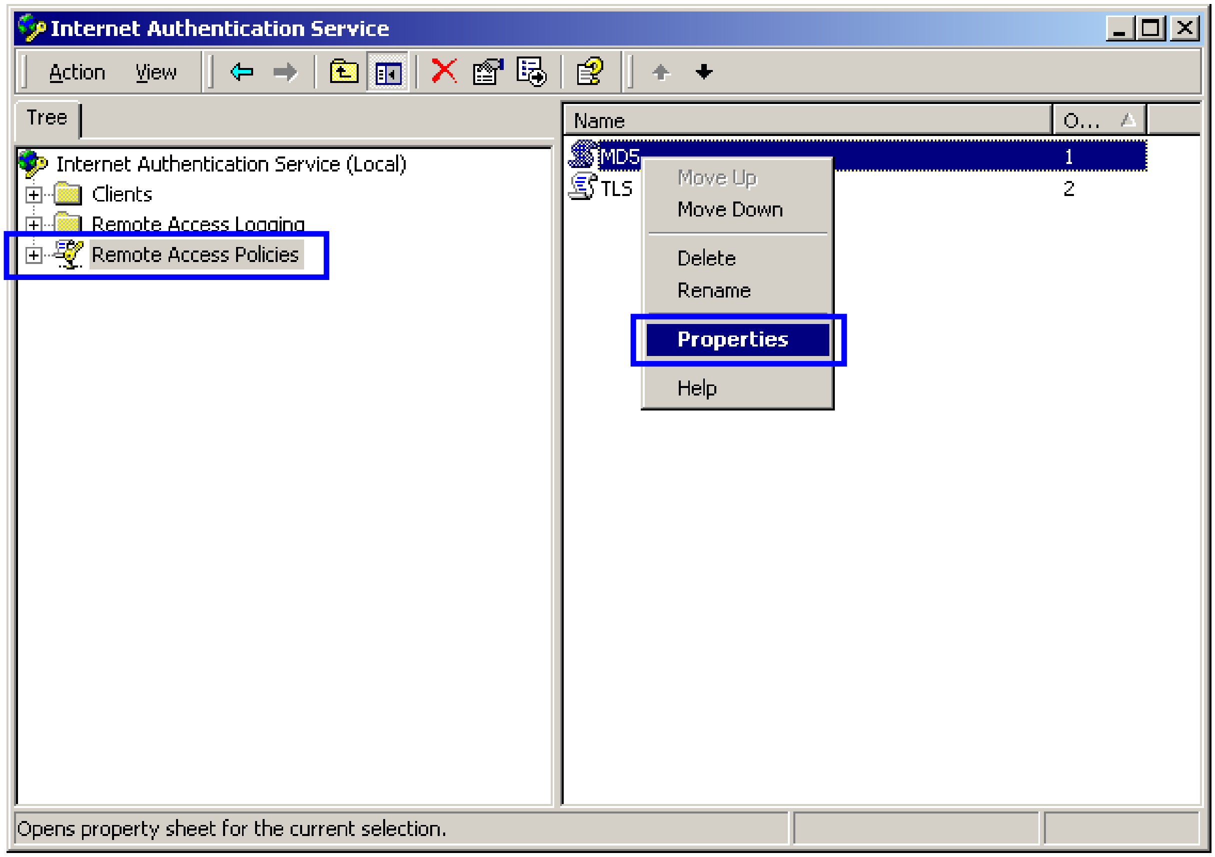
- ● Never
- ○ End of: Friday , February 07, 2003

48. Go to Start > Program > Administrative Tools > **Internet Authentication Service**.

49. Go **to Remote Access Policies**

50. Make sure that **MD5** is moved up to Order 1

51. Right-click "**MD5**", and select "**Properties**"

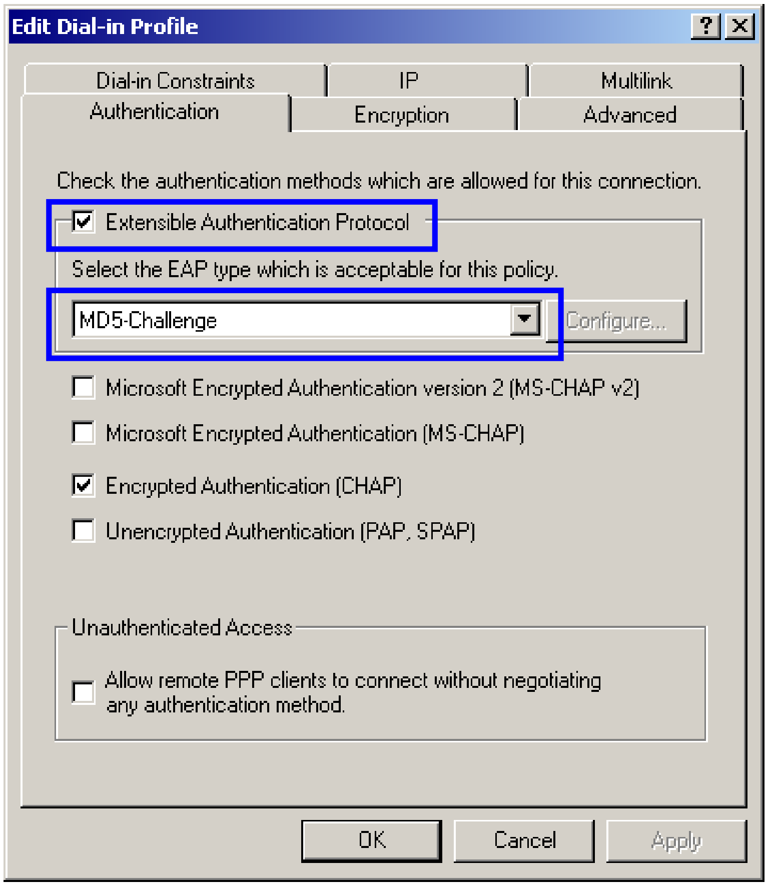


Opens property sheet for the current selection.

52. Go to "**Authentication**" tab

53. Enable "**Extensible Authentication Protocol**"

54. Select "**MD5-Challenge**" for EAP type.



Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

MD5-Challenge

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

☑ Encrypted Authentication (CHAP)

□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

APPENDIX E: TECHNICAL SPECIFICATIONS

General Specifications	
Standards compliance	IEEE802.11b
Regulations compliance	FCC Part 15 Class B, Sec. 15.247 and 15.109
	ETS 300 328, ETS 300 826, EN60950 and CE-Mark
	Telec (Japan)
	Wi-Fi Compliant
Data rate	1/2/5.5/11/22 Mbps
Security	Wired Equivalent Privacy (WEP) 64/128/256 Bit
Dimensions	200 x 150 x 60 mm
LED indicators	Power/Status Wireless activity LAN activity WAN activity
Network interface	Four RJ-45 x 10/100 Base-T LAN ports (MDI/MDIX auto detect) 1 x 10/100 Base-T Broadband WAN port
Antenna	2 ports
Power jack	2.5 mm
RF Specifications	
Emission type	Direct Sequence Spread Spectrum (DSSS)
RF frequency	2412 MHz – 2484 MHz – Japan Band
	2412 MHz – 2462 MHz – North America
	2412 MHz – 2472 MHz – General Europe
Operating channel	11 channels (US, Canada)
	13 channels (Europe, Spain)
	14 channels (Japan)
Radio chipset	RFMD
MAC with BBP	TI ACX100
Antenna type	Dual Dipole Antenna with Diversity