22Mbps Wireless Network PCI Adapter User Manual

version 3.0

Manufacturer's Disclaimer Statement

The information in this document is subject to change without notice and does not represent a commitment on the part of the vendor. No warranty or representation, either expressed or implied, is made with respect to the quality, accuracy or fitness for any particular purpose of this document. The manufacturer reserves the right to make changes to the content of this document and/or the products associated with it at any time without obligation to notify any person or organization of such changes. In no event will the manufacturer be liable for direct, indirect, special, incidental or consequential damages arising out of the use or inability to use this product or documentation, even if advised of the possibility of such damages. This document contains materials protected by copyright. All rights are reserved. No part of this manual may be reproduced or transmitted in any form, by any means or for any purpose without expressed written consent of its authors. Product names appearing in this document are mentioned for identification purchases only. All trademarks, product names or brand names appearing in this document are registered property of their respective owners.

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.

Table of Contents:

TABLE OF CONTENTS: **3**

INTRODUCTION **4**

PRODUCT FEATURES 4

SYSTEM REQUIREMENTS 5

GETTING TO KNOW THE 22MBPS WIRELESS NETWORK PCI ADAPTER 6

WIRELESS NETWORK PCI Adapter's LEDs *6*

SETTING UP THE WIRELESS NETWORK 6

INSTALLING YOUR 22MBPS WIRELESS NETWORK PCI ADAPTER 8

CONFIGURING YOUR WIRELESS PCI ADAPTER **13**

Link Info. Page *13*

Configuration Page *14*

Security Page *16*

SiteSurvey Page *17*

About Page *19*

APPENDIX A: TROUBLESHOOTING **20**

APPENDIX B: NETWORKING BASIS **25**

APPENDIX C: 802.1X AUTHENTICATION SETUP **39**

802.1X AUTHENTICATION INFRASTRUCTURE 39

SUPPLICANT: WIRELESS NETWORK PC CARD 40

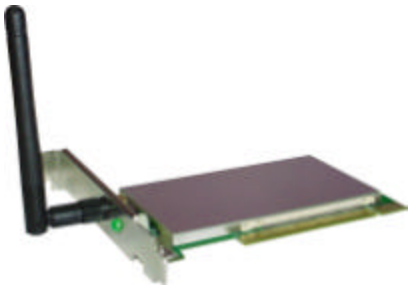
AUTHENTICATOR: WIRELESS NETWORK ACCESS POINT 59

RADIUS SERVER: WINDOW2000 SERVER 61

APPENDIX D: GLOSSARY **83**

APPENDIX E: TECHNICAL SPECIFICATION **88**

INTRODUCTION



The 22Mbps Wireless Network PCI Adapter delivers enhanced IEEE 802.11b high performance for up to 22Mbps, which is double of that offered by most of the current wireless products in the market.

The 22Mbps high data rate is made possible by the latest advanced TI wireless technology, which incorporates the new PBCC modulation method. Unlike the ordinary CCK modulation, not only the new PBCC modulation method offers double data rate for up to 22Mbps, but also it gives 20% more distance coverage.

The 22Mbps Wireless Network PCI Adapter is fully compatible with other 11Mbps wireless devices. The simple step-by-step installation allows you to have the wireless network setup in no time. The comprehensive configuration utility makes the setting control for the PCI Adapter easier than ever.

The 22Mbps Wireless Network PCI Adapter is an ideal wireless device that truly makes the idea of "wireless" come true. Please take a moment to read through this manual and get acquainted with this cutting-edge product.

Product Features

- Fully compatible with IEEE 802.11b standard for wireless.
- Interoperatable with existing IEEE 802.11b standard devices.
- Supports new data modulation PBCC technology from Text Instrument, which enables high data with double speed of up to 22Mbps.
- 20% more transmitting and receiving coverage supported by PBCC modulation.
- 4X mode enhancing the transmission speed to over 12Mbps throughput.
- Supports auto data rate fallback under noisy environment or longer distance.
- Enhanced security on WEP encryption from 64, 128 to the maximum of 256 bits.
- Supports SiteSurvey function with profile.
- Easy setup and installation with Install Wizard..

System Requirements

- Windows 98, 98SE, Millennium Edition (ME), 2000 and XP computers
- PC with Pentium III 600MHz system or above is recommended
- Equipped with at least one empty PCI standard v2.1 socket.
- One CD-ROM drive

GETTING STARTED

Getting To Know The 22Mbps Wireless Network PCI Adapter

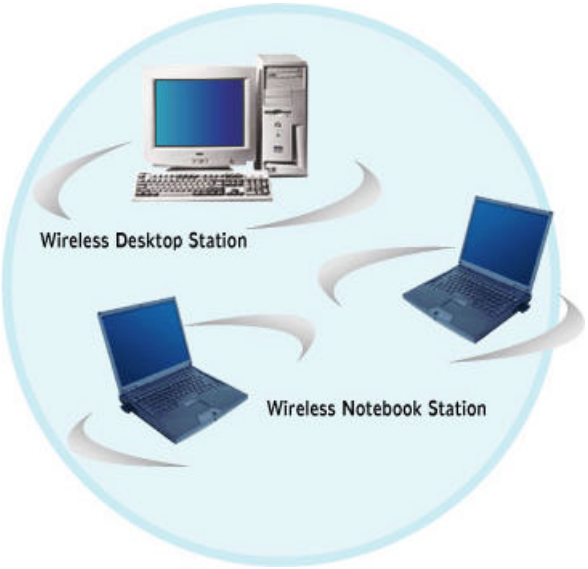
WIRELESS NETWORK PCI Adapter's LEDs

- Power LED
  ON when the unit is powered up
  Blink indicates wireless activity

Setting Up The Wireless Network

There two wireless network topologies that you can setup your wireless card with. One is called "**Ad-Hoc**", and the other is "**Infrastructure**". On an Ad-Hoc network, two or more computers each has at least one wireless network client device such as wireless PCI Adapter installed, establish point-to-point data communication with each other. While on an Infrastructure network, every wireless station communicates through Access Points.

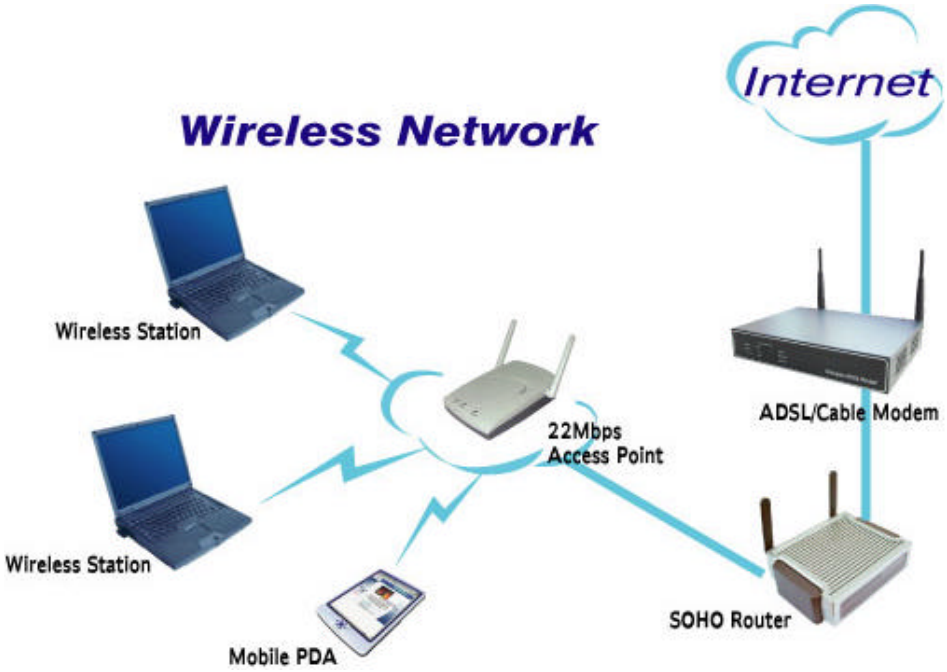
Setting Up Ad-Hoc Network



The idea of Ad-Hoc Network is rather simple. All the wireless station are set to use the

same BSS ID and channel to establish communication linkage with each other to form a point-to-point network for data transmission and reception.

Setting Up Infrastructure Network



In order to setup an Infrastructure of a wireless network such as the example shown above, you will need the following:

1. A broadband Internet connection.
2. ADSL or Cable modem provided by your ISP as part of the broadband connection installation.
3. A Router that connects to the ADSL/Cable modem for internet connection sharing.
4. An Access Point to connect with the Router to form a wireless infrastructure network.
5. Wireless clients equipped with wireless networking devices such as wireless PC Card for wireless connection.

In this case, all the wireless clients and Access Point operate under the same channel with the same ESSID. The wireless clients are all connected to the Access Point for data transmission.

Installing Your 22Mbps Wireless Network PCI Adapter

Make sure that the 22Mbps Wireless Network PCI Adapter is **NOT** inserted into your computer.

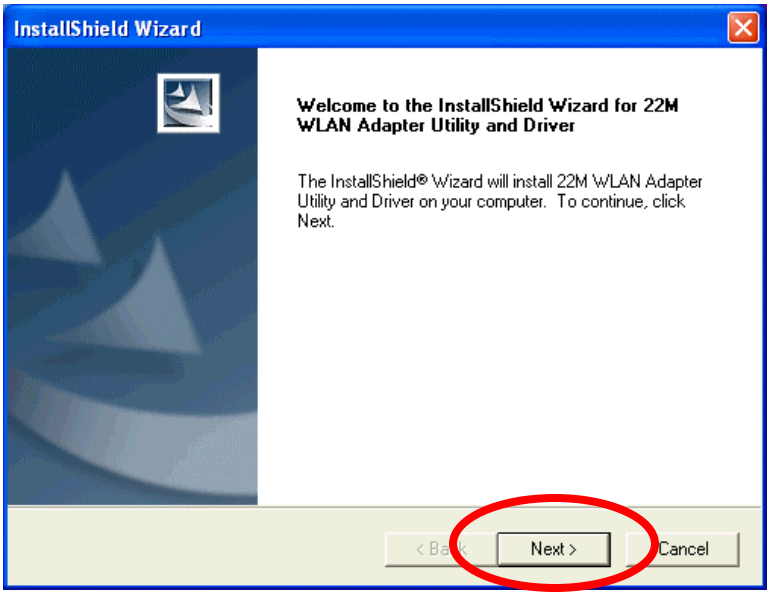
Turn on the computer. Insert the software CD into the CD-ROM Drive.

Please note that the installation screens in this quick guide are captured from WindowsXP. The other Windows systems will have similar screen for the installation procedure.

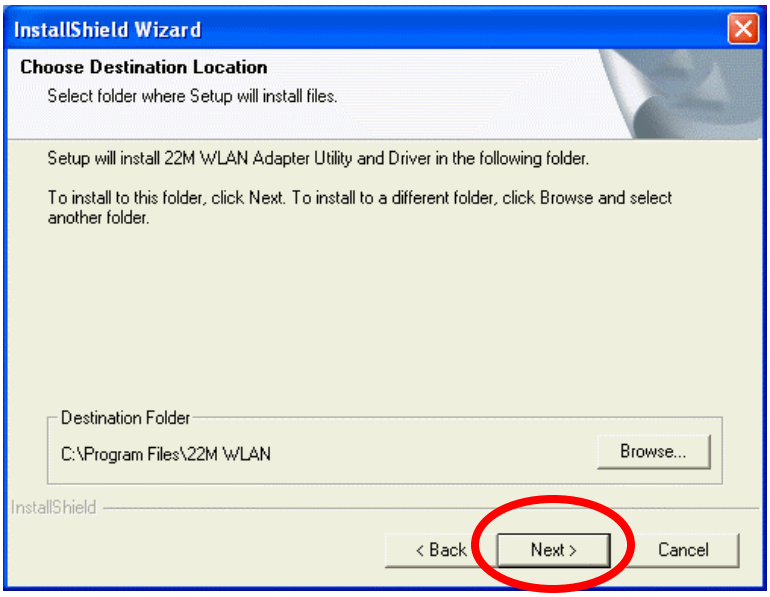
Click on the "**PC Card/PCI Card**" option on the left selection menu.

Click on "**Install**" button to start Utility installation.

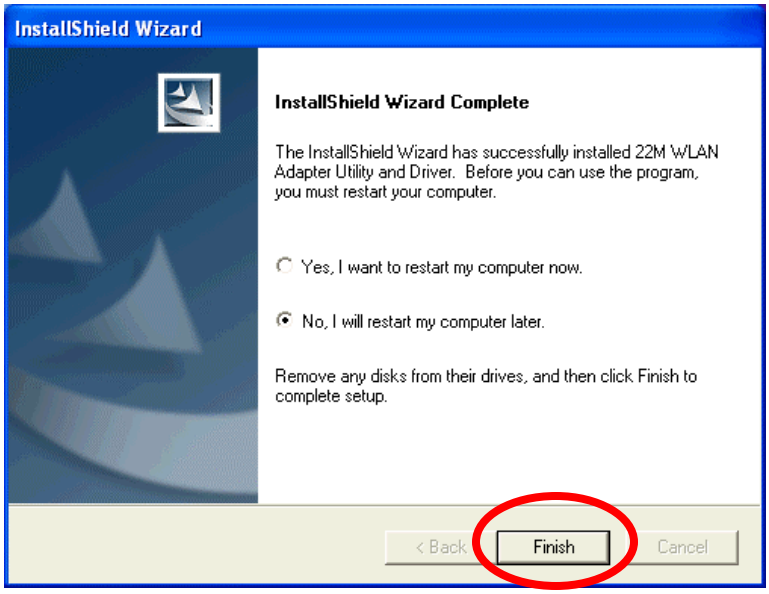
InstallShield Wizard starts. Click "**Next**" to continue.



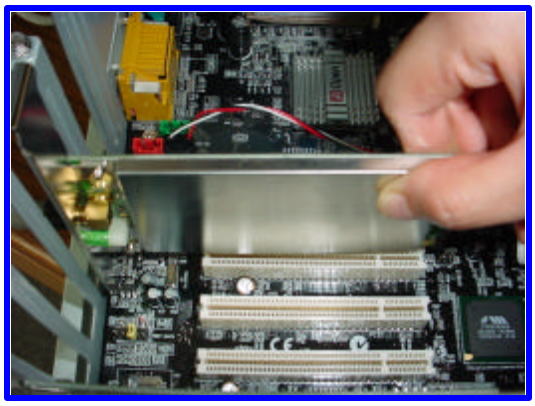
Click "**Next**" to install the program files in the default folder.



Select the second option, and click "**Finish**" to complete the installation.

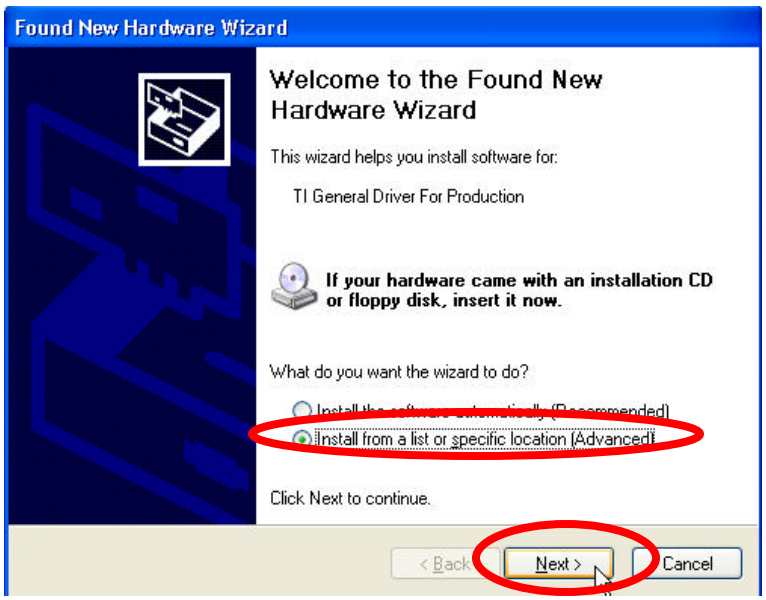


- Turn off your computer, and make sure the power core is unplugged.
- Open the computer case.
- Insert the 22Mbps Wireless Network PCI Adapter into the PCI socket on the mainboard of your computer.
- Seal the computer case and plug the power back on.
- Turn on your computer
- Continue with **Driver Installation.**

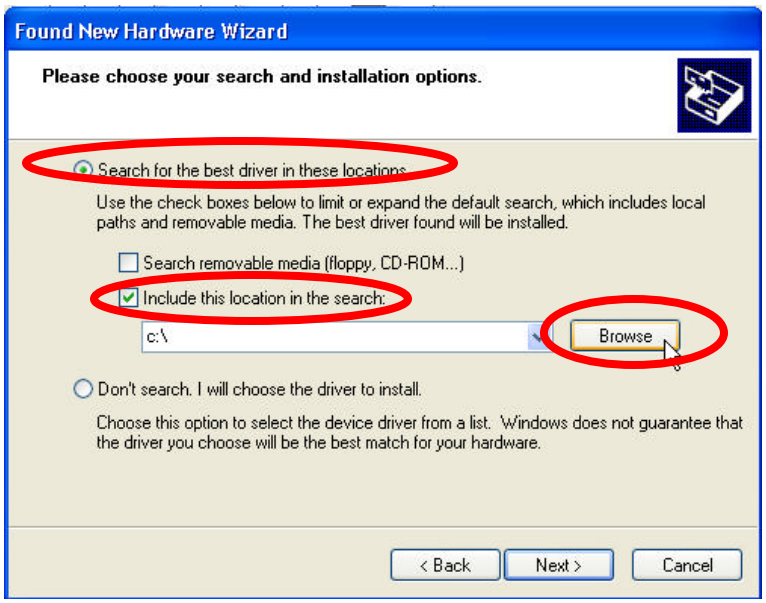


2 *Installation of Driver Files*

Select the second option and click "**Next**" to continue.

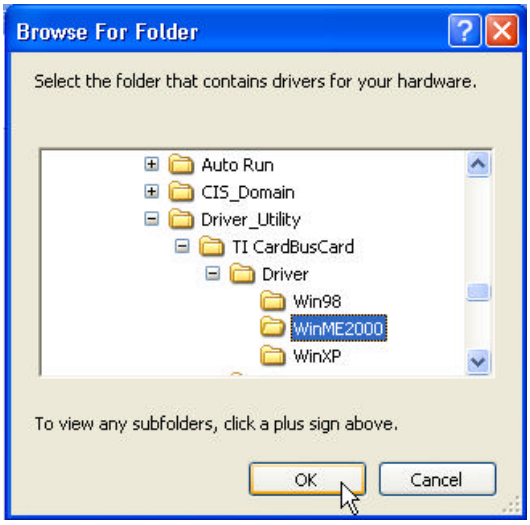


Select first option then click on the checkbox click "**Browse**" button to specify the driver file folder.

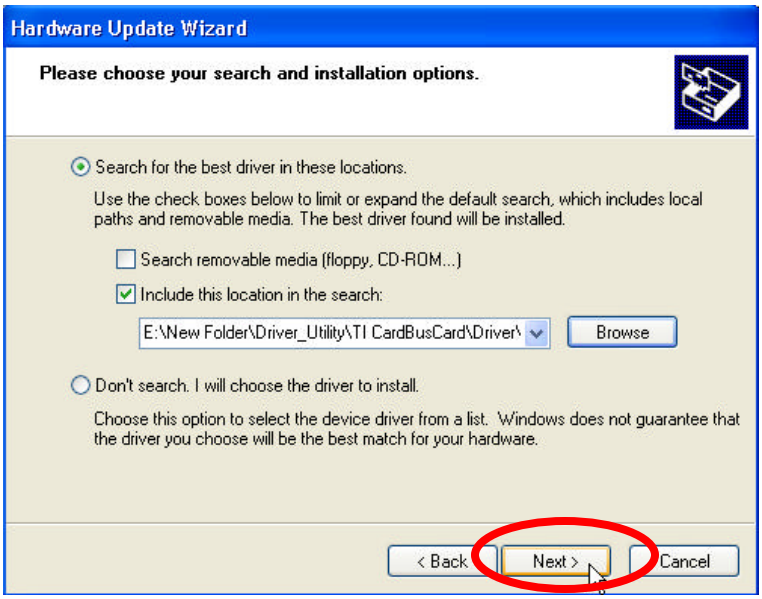


Go to D:\Driver\WinXP
Click "**OK**"

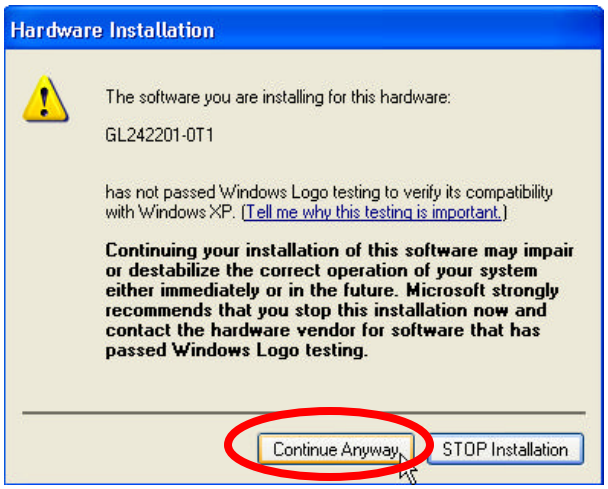
Please note that letter "**D:**\" represents the CD-ROM driver letter, and select folder "Win98" when installing under Windows 98 O/S or WinME2000 for Windows ME or 2000 O/S.



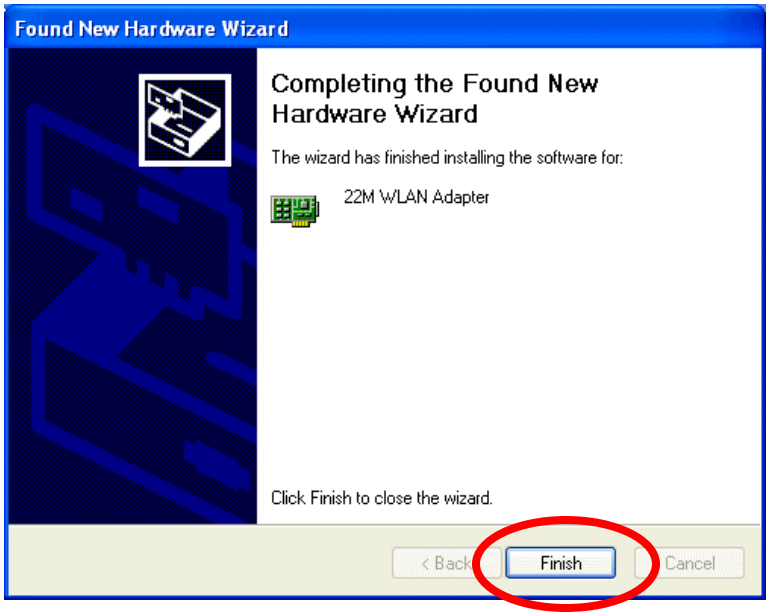
Click "**Next**" to continue



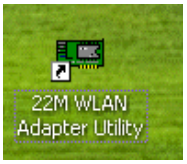
Click "**Continue Anyway**" to continue

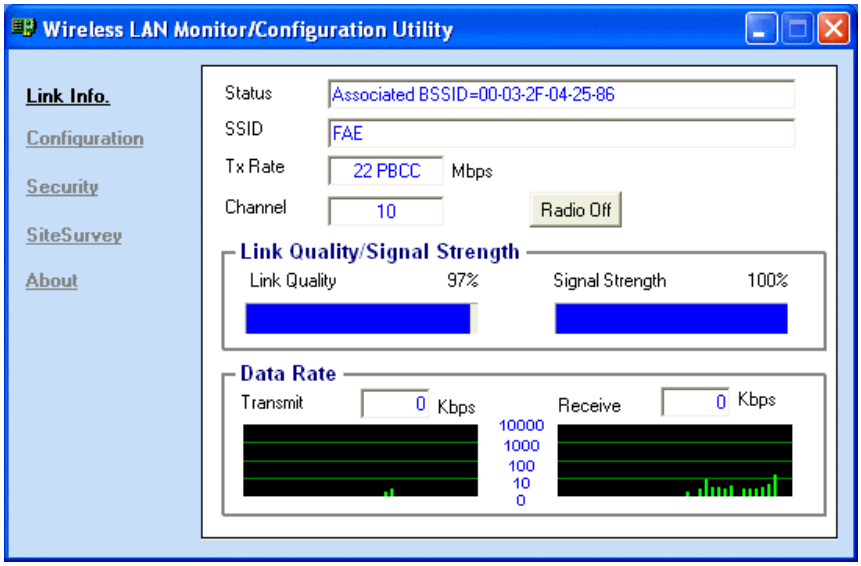


Click "**Finish**" to complete new hardware installation.



After successful installation, an utility program icon will appear on your desktop screen.
Simply, double-click the icon to launch the utility.



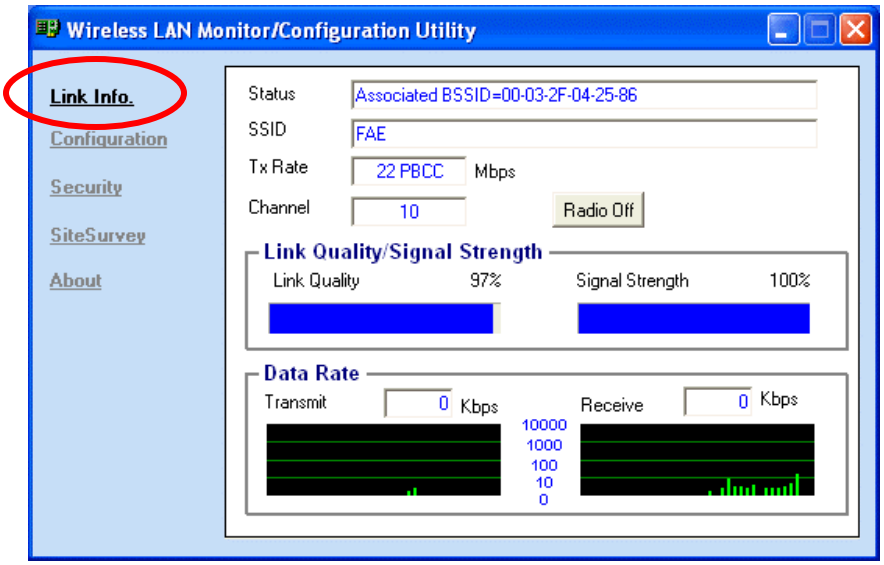


CONFIGURING YOUR WIRELESS PCI Adapter

Link Info. Page

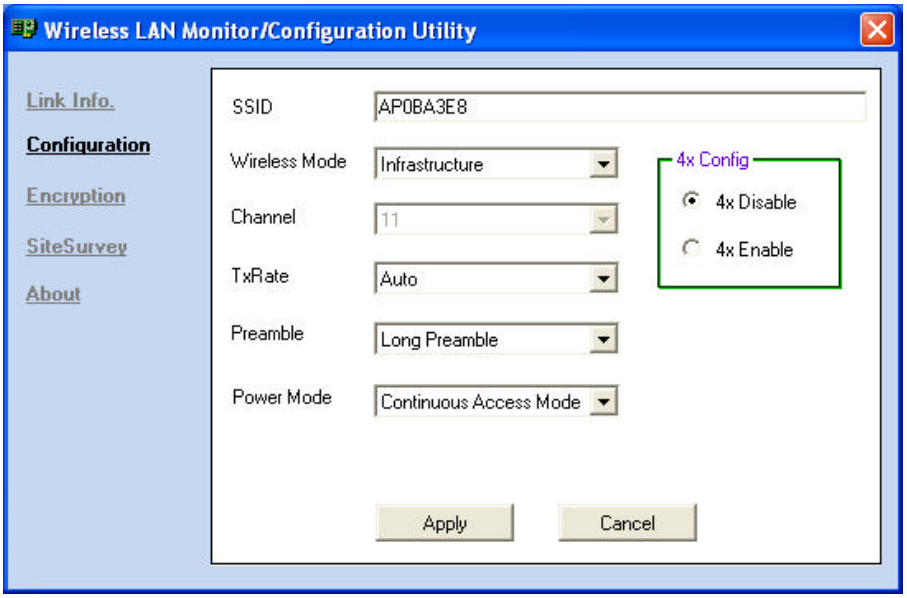
This is the default page when the utility starts up.

Status: Shows the BSSID associated, which can be used to identify the wireless network.
SSID: Shows current SSID, which must be the same for the wireless client and AP in order for communication to be established.
TxRate: Shows the current data rate used for transmitting.
Channel: Shows the current channel for communication.
Radio Off button: When clicked, you disable the radio signal, and cut-off the wireless connection.
Link Quality: Shows the link quality of the 22Mbps wireless Network PCI Adapter with the Access Point when operating under Infrastructure mode.
Signal Strength: Shows the wireless signal strength of the connection between the 22mpbs wireless Network PCI Adapter with the Access Point.
Data Rate: Shows the statistics of data transfer, and the calculation is based on the number of packets transmitted and received.



Configuration Page

This is the page where you can change the basic settings of the Access Point with the minimum amount of effort to adjust a secure wireless network.



SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

BSS Type: There are two types available for selection

- Infrastructure – to establish wireless communication with LAN and other wireless clients through the use the Access Points.
- Ad-Hoc – to establish point-to-point wireless communication directly with other wireless client devices such as wireless network PCI Adapter.

Channel: The value of channel that AP will operate in. You can select the channel range of 1 to 11 for North America (FCC) domain, 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain.

Tx Rate: Select the data rate for data transmission.

Preamble: Select **Long** or **Short** Preamble type. Preamble is a sequence of bits transmitted at 1Mbps that allows the PHY circuitry to reach steady-state demodulation and synchronization of bit clock and frame start. Two different preambles and headers are defined: the mandatory supported Long Preamble and header, which interoperates with the 1 Mbit/s and 2 Mbit/s DSSS specification (as described in IEEE Std 802.11), and an optional Short Preamble and header (as described in IEEE Std 802.11b). At the receiver, the Preamble and header are processed to aid in demodulation and delivery of

the PSDU. The Short Preamble and header may be used to minimize overhead and, thus, maximize the network data throughput. However, the Short Preamble is supported only from the IEEE 802.11b (High-Rate) standard and not from the original IEEE 802.11. That means that stations using Short-Preamble cannot communicate with stations implementing the original version of the protocol.

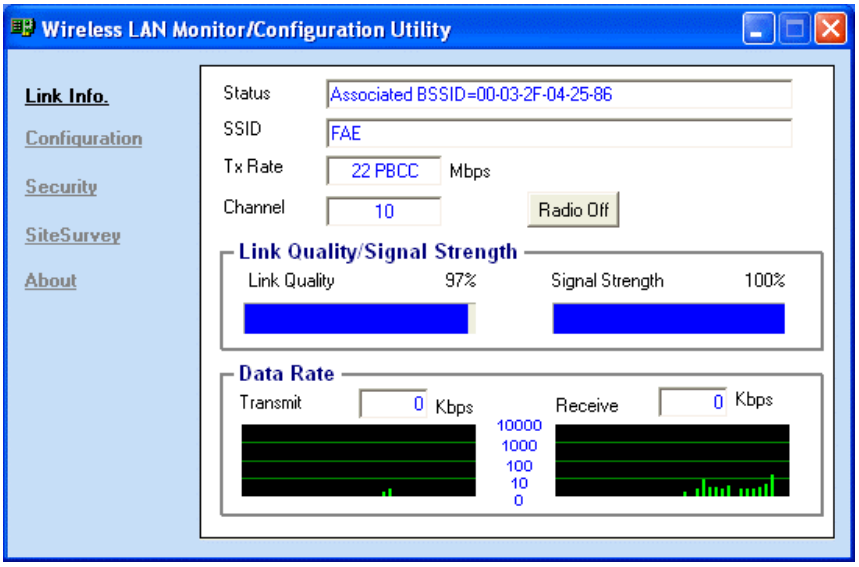
Power Mode: There are 3 modes to choose from

- Continuous Access Mode (default) – the PCI Adapter is constantly operating with full power and it consumes the most power
- Maximum Power Save – the PCI Adapter consumes the least power and only operates when there is wireless network activity.
- Power Save – the PCI Adapter consumes the moderate level of power.

4X Config.: When "4X enable" is selected, you will be running 22Mbps PBCC+4X mode, the wireless transmission speed can achieve over 12Mbps real throughput assuming that the other wireless LAN devices are also running 22Mbps PBCC+4X.

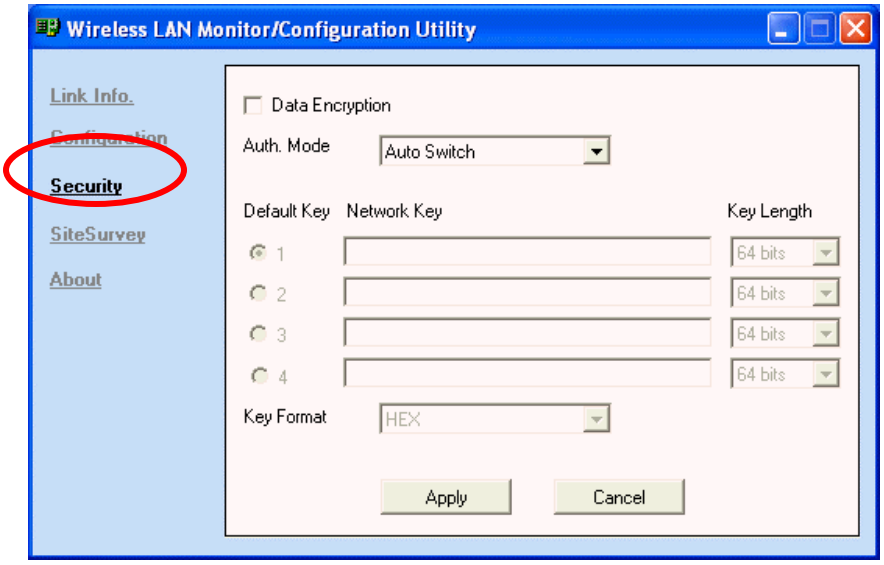
Note !: 4X mode is proprietary transmission mode available only with our solution chipset. In order to achieve superb speed by 4X or 22Mbps PBCC mode, both the transmitting and receiving parties must be using our WLAN solution products.

For the changes made to any of the items above to be effective, click "**Apply**". The screen will be changed back to **Link Info.** Page



Security Page

This is the page where you configure Security settings of your 22Mbps wireless PCI Adapter.



Data Encryption: Click the box to enable Data Encryption feature.

Aut. Mode: There are three modes available to choose from.

- **Open Authentication** – the sender and receiver do not share secret Key for communication. Instead, each party generates its own key-pairs and ask the other party to accept it. The key is regenerated when the connection is established every time.
- **Shared Authentication** – the sender and receiver shares the common key for data communication, and the key is used for extended length of time.
- **Auto** – depend on the communication to establish, and automatically use the proper authentication mode.

The following will only be activated to allow for configuration when **Data Encryption** is enabled.

Default Key: select one of the 4 keys to use.

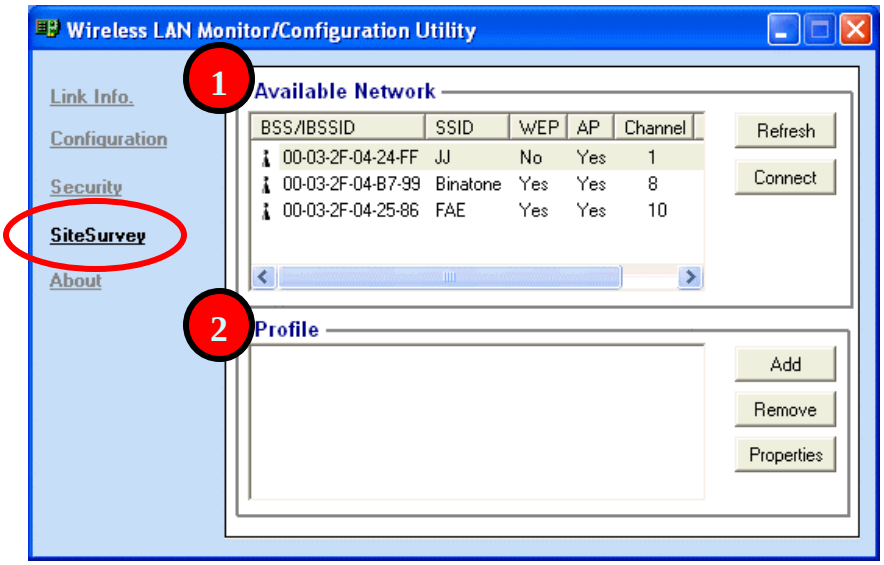
Network Key: enter values to these fields, either in HEX or ASCII formats. You only have to enter the key that you will use

Key Length : select 64, 128 or 256 bits as the length of the keys

Key Format: ASCII or **HEX** (Please refer to Appendix G: Glossary for details about these two formats).

SiteSurvey Page

This page allows to utilize the SiteSurvey function to scan for the available wireless network (wireless clients and Access Points) and select one to establish wireless communication.



1 **Available Network** – displays the wireless networks (wireless clients and Access Points) that are in your signal range. Select any one of them and establish communication by simply mouse **double-click** or a single click on the "**Connect**" button.

Click "**Refresh**" button to start scanning for available network again.

2 **Profile** – You can create and manage the created profiles for Home, offices or public areas.

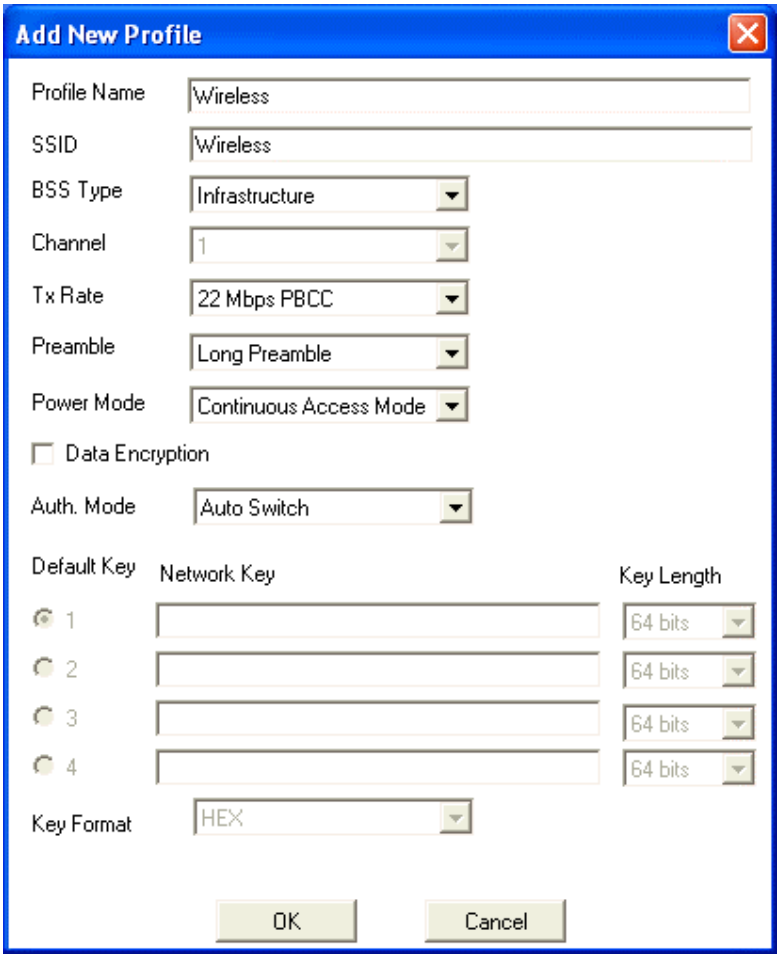
By double-clicking on one of the created profile, the setting will adapt to the configuration such as SSID, channel, and WEP settings saved by that particular profile.

Click to select any one of the profiles, and you can

Click on "**Remove**" button to remove the profile, or

Click on "**Properties**" button to view and change its settings. The Properties is very similar to that of adding profile.

Click "**Add**" to add a profile, and the following screen would appear.



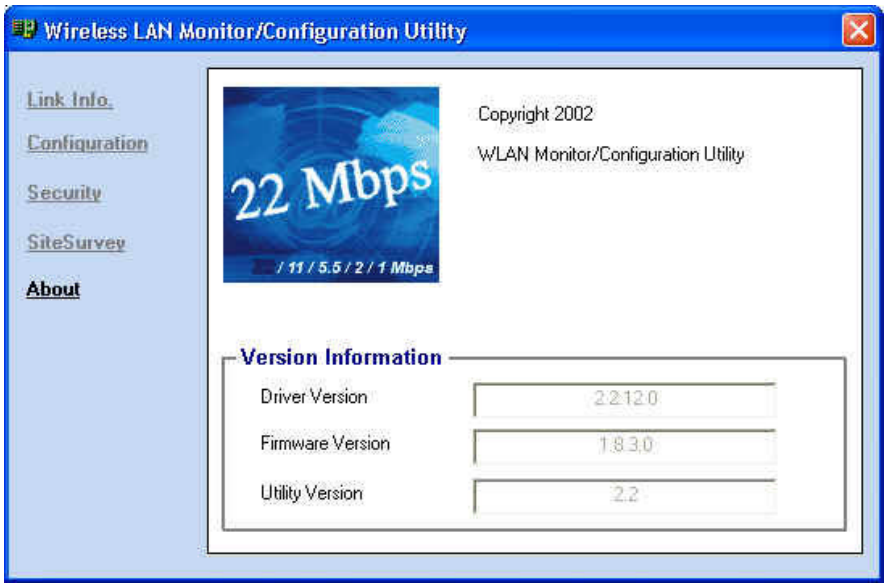
All the detail information about each settings and configuration item are described in previous Configuration and Security Page sessions. Please refer to those two sessions for more information.

When you finish enter the setting for this profile, click "**OK**" to add a new profile.

About Page

This page displays some information about the 22mpbs PCI Adapter utility, which includes the version numbers for Driver, Firmware and Utility.

When there is new version of software available for upgrade, you will be able to identify by version numbers.



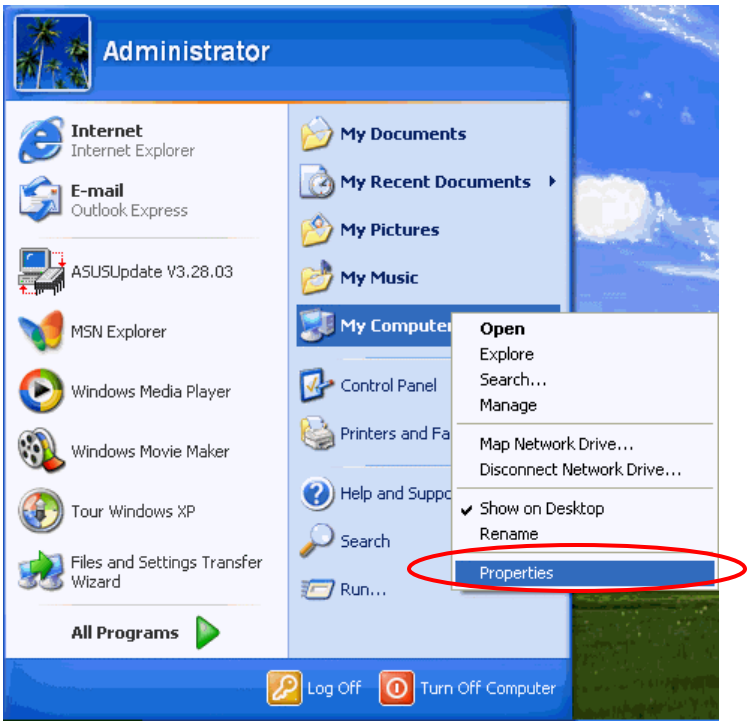
APPENDIX A: TROUBLESHOOTING

This chapter provides solutions to frequently encountered problems that can occur during the installation and operation of the 22Mbps Wireless Network PCI Adapter. Please read through the following to solve your problems.

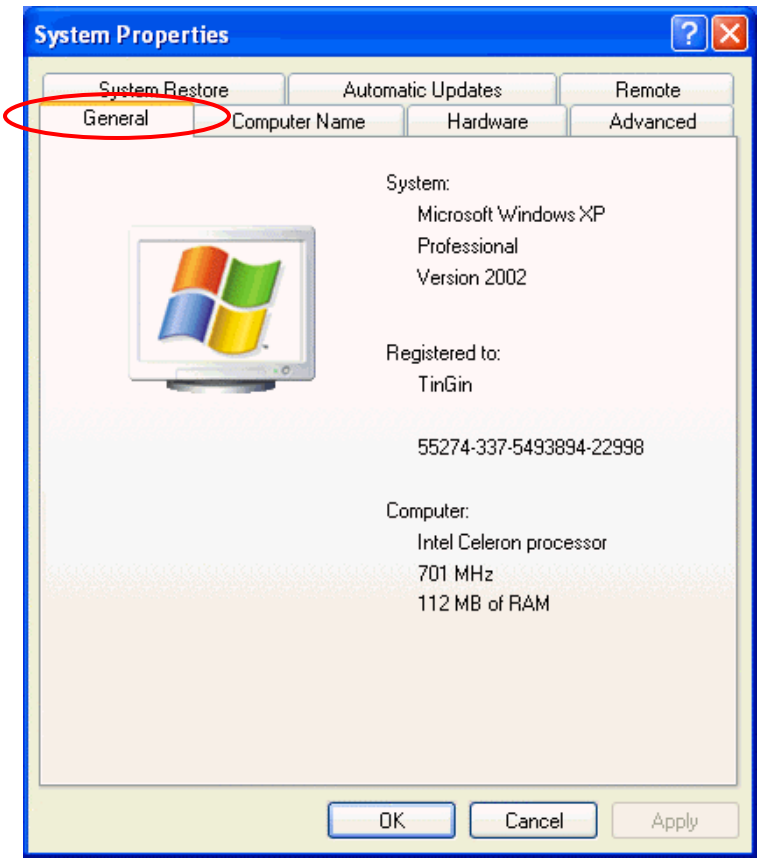
1. The wireless clients cannot access the network in the infrastructure mode.

- Check that the wireless network device is being installed and working properly.

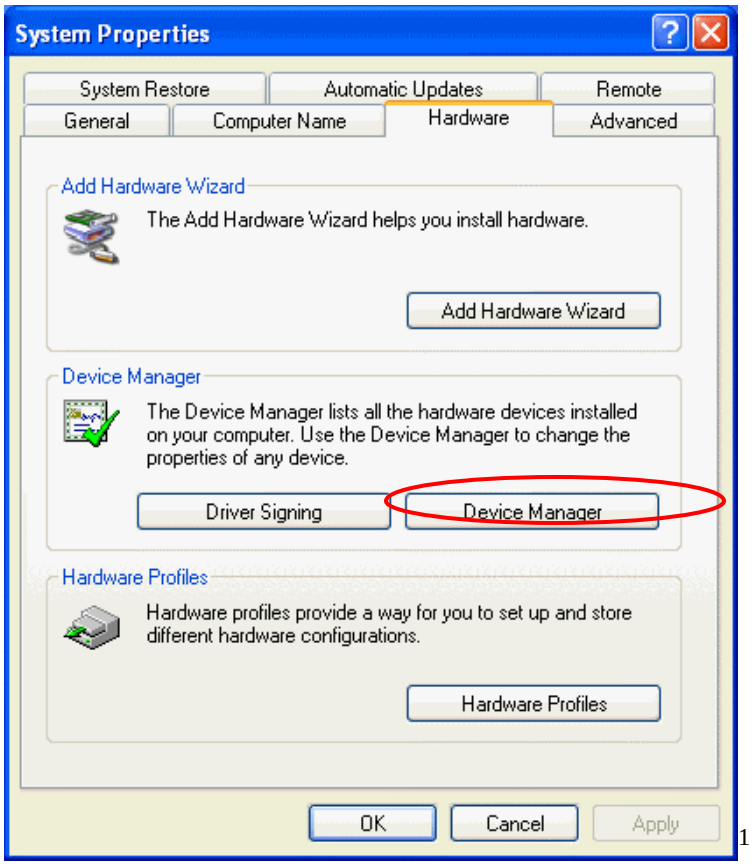
Go to "Start" > Right mouse click on "My Computer" > "Properties"



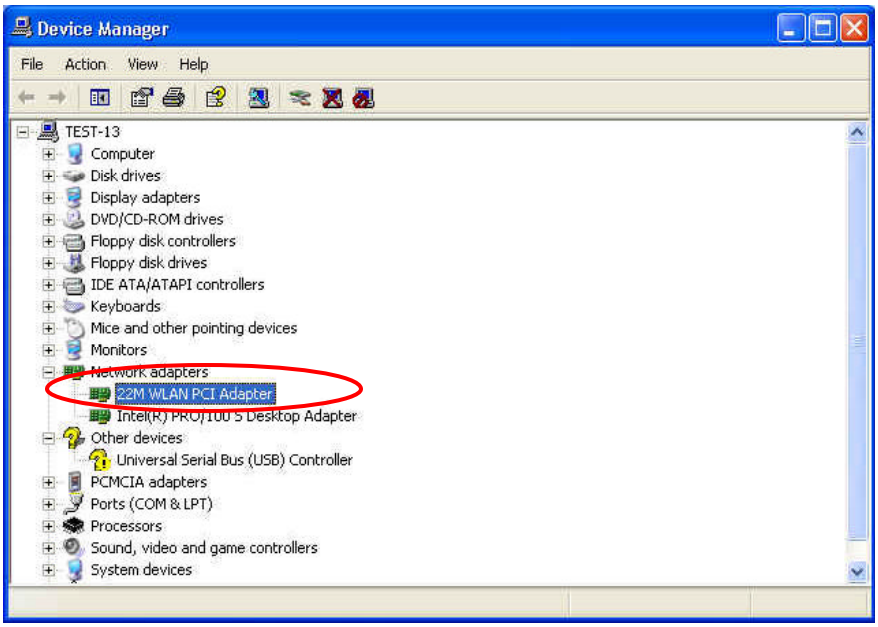
Go to “Hardware”



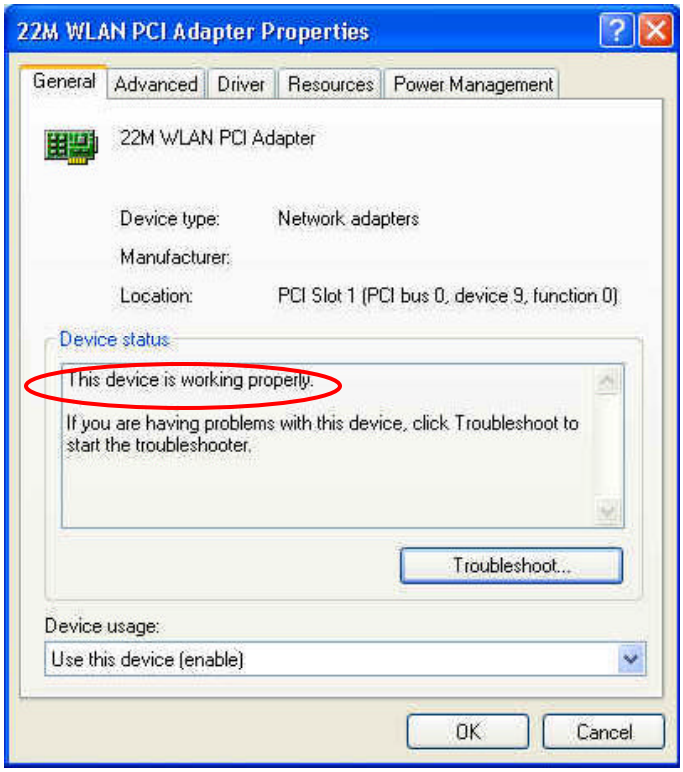
Go to “Device Manager”



Right mouse click on the 22 M WLAN PCI Adapter and go to “Properties”



Check and make sure that the network adapter is working properly



2. What is the difference between 22Mbps and 11Mbps wireless products? What's the benefit of 22Mbps Wireless Access Point?

The 22Mbps is made possible by the new modulation method called PBCC developed by TI, which is different from the current CCK modulation method for 11Mbps. The 22Mbps Wireless Access Point offers double data rate than that of 11Mbps with 20% more distance coverage. The 22Mbps wireless products also operate in the 2.4GHz ISM band and they are backward compatible with 11Mbps wireless products.

3. What is Roaming?

Roaming is the ability of portable computers, e.g., Packet PC and notebook, to have consistent and continuous data transmission/reception throughout an area covered by more than one Wireless Access Point. In order to achieve seamless connectivity, all the wireless clients and Access Points must be set to use the same SSID. When a user walked out of the coverage area of one AP into another, the wireless client network device will automatically reestablish connection with the new AP.

4. What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking devices, e.g. a network adapter, that

allows the network to identify it at the hardware level. Unlike IP addresses, which can be changed or dynamically assigned by the network, the MAC address of a networking device is permanent.

5. What is WEP?

Wired Equivalent Privacy (WEP) is a type of data encryption mechanism described in the IEEE 802.11 standard. The 22Mbps Wireless Access Point supports 64/128/256 bit shared key for WEP.

6. Would the information be transmitted securely in the air?

WLAN offers two layers of protection for security. First layer is on the hardware level. As with Direct Sequence Spread Spectrum (DSSS) technology, it has the inherent security feature of scrambling. Second of all, on the software level, the security control is made possible by Wired Equivalent Privacy (WEP) for access control.

7. What is ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. The 2.4GHz unlicensed ISM band is available worldwide, which presents the opportunity for the global market of 802.11b high speed wireless products.

8. What is 4X mode?

This is a proprietary wireless data transmission mode provided by TI, which enhances TI's 22Mbps PBCC speed to reach data throughput to over 12Mbps. Since it is not IEEE 802.11b standard wireless data mode, in order to allow 4X mode, both the receiving and transmitting parties must be using TI solution.

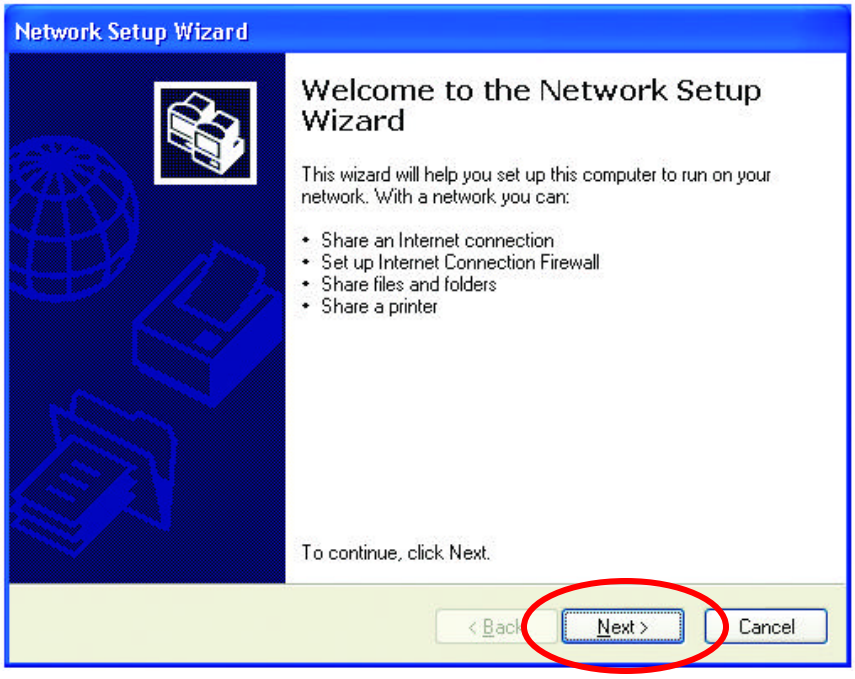
APPENDIX B: NETWORKING BASIS

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

Using the Windows XP Network Setup Wizard

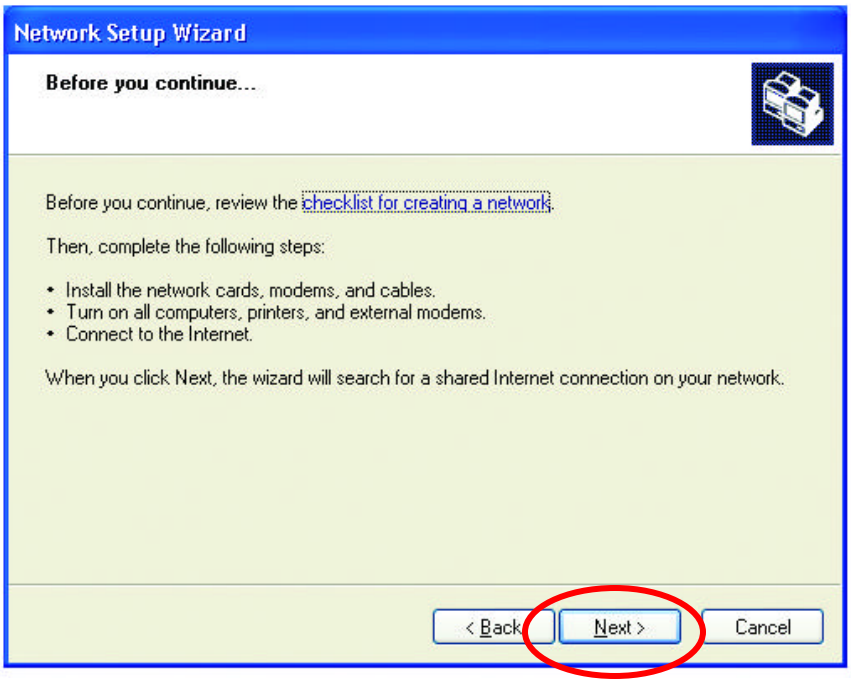
Go to **Start menu** > **Control Panel**> **Network Connections**

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



Click "**Next**" to procced

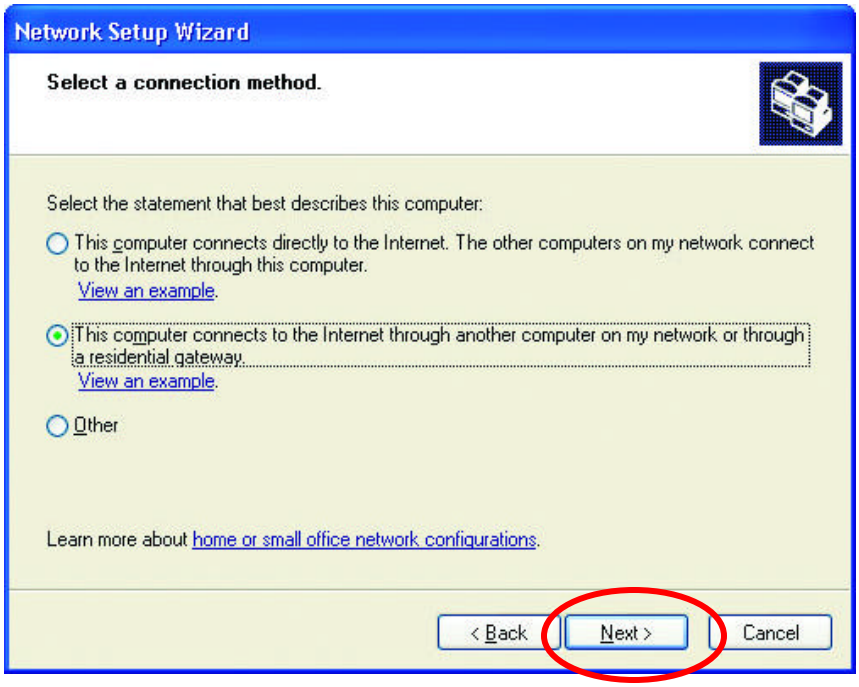
Click "**Next**" to continue



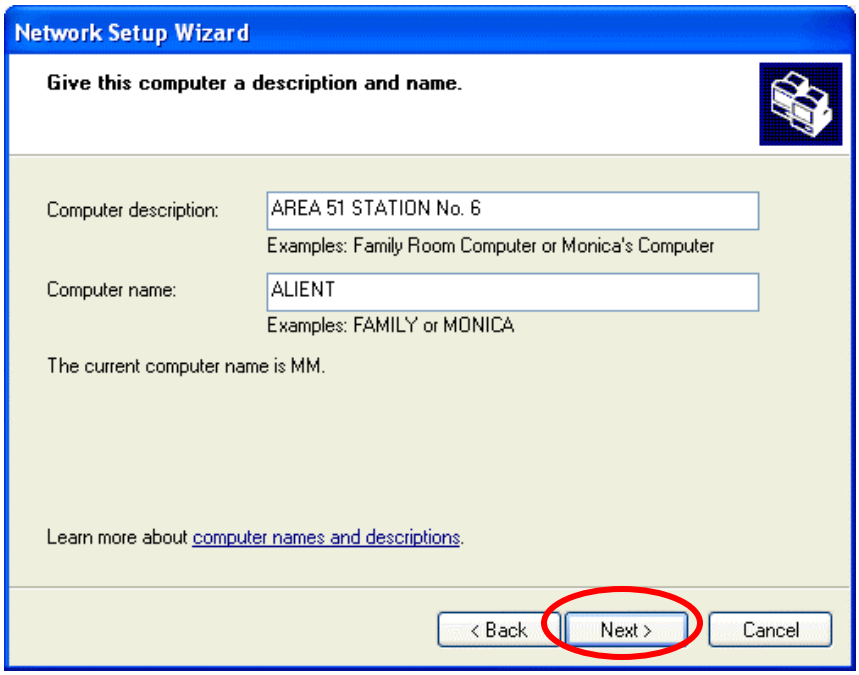
Select the option that best describes how you connect your computer to the Internet.

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

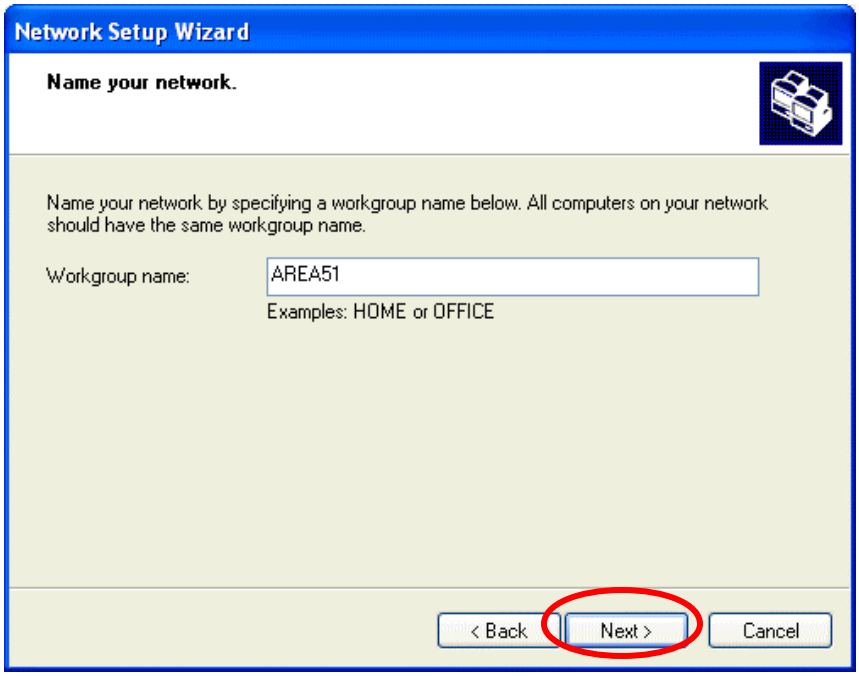
Click "**Next**" to continue.



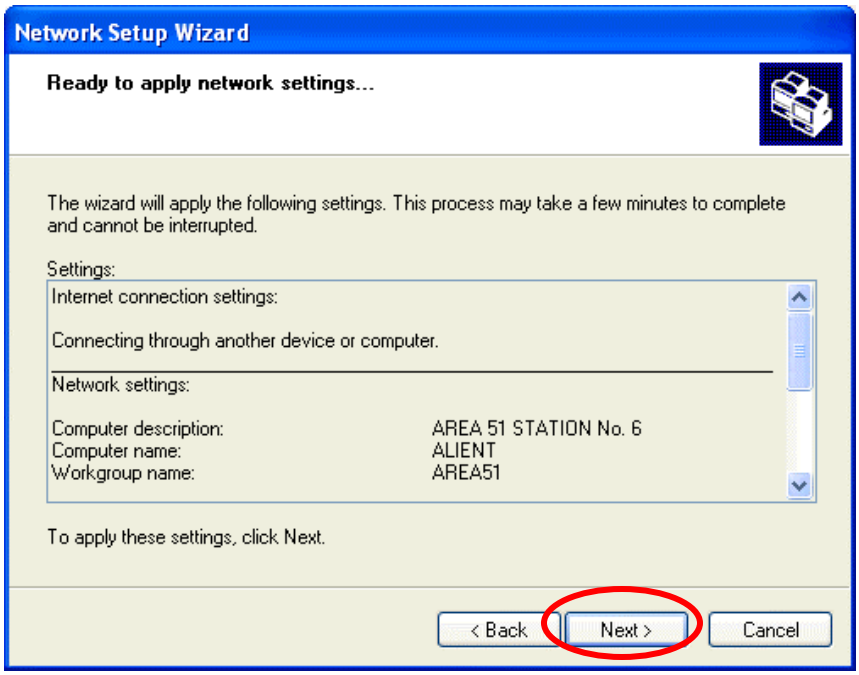
1. Enter a short description for your computer.
2. Enter a name for your computer to be recognized among the network.
3. Click "**Next**" to continue.

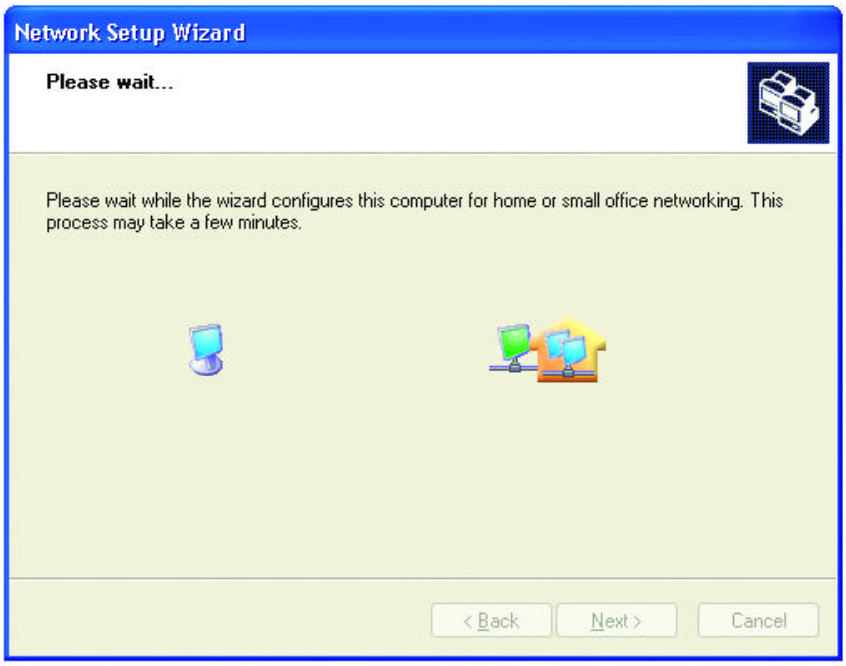


Enter "**Workgroup name**" for your home network. Click "**Next**" to continue"



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

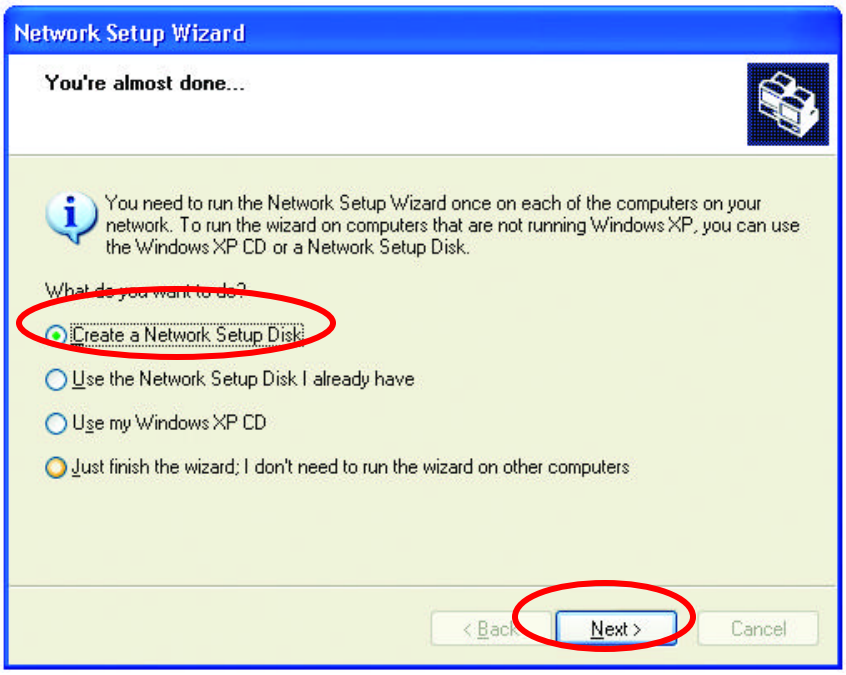




You may create a Network Setup Disk which saves you the trouble of having to configure every PCs in your network.

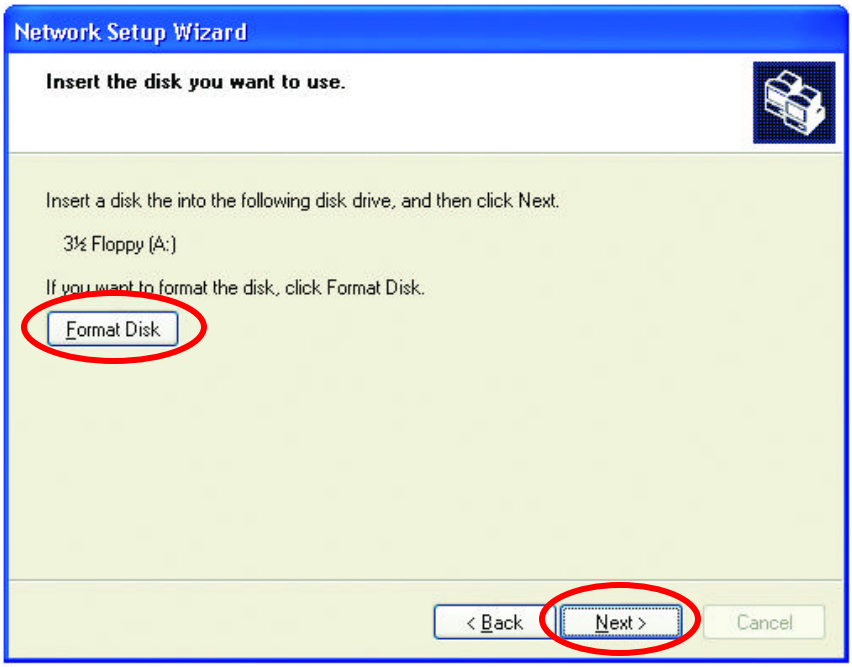
Select the first choice, and insert a floppy disk into your disk drive

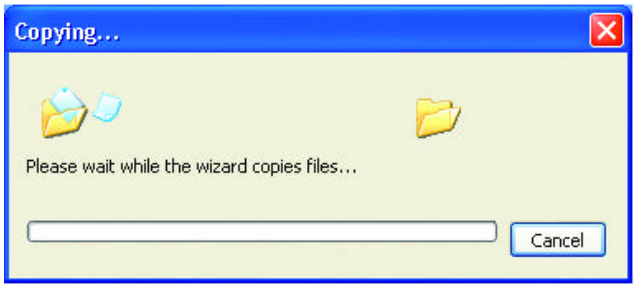
Click "**Next**" to continue.



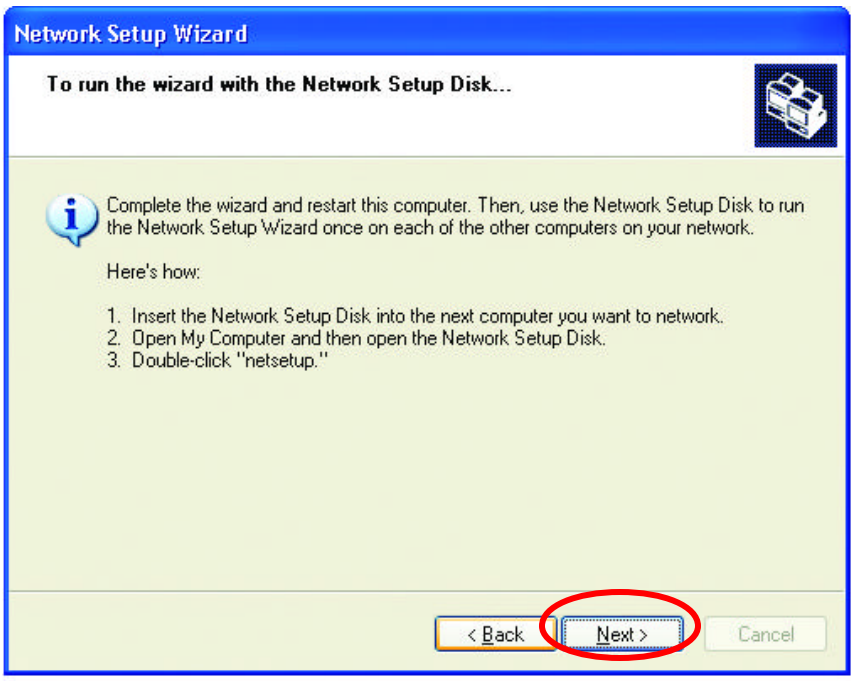
Click "**Format Disk**" if you wish to format the disk.

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



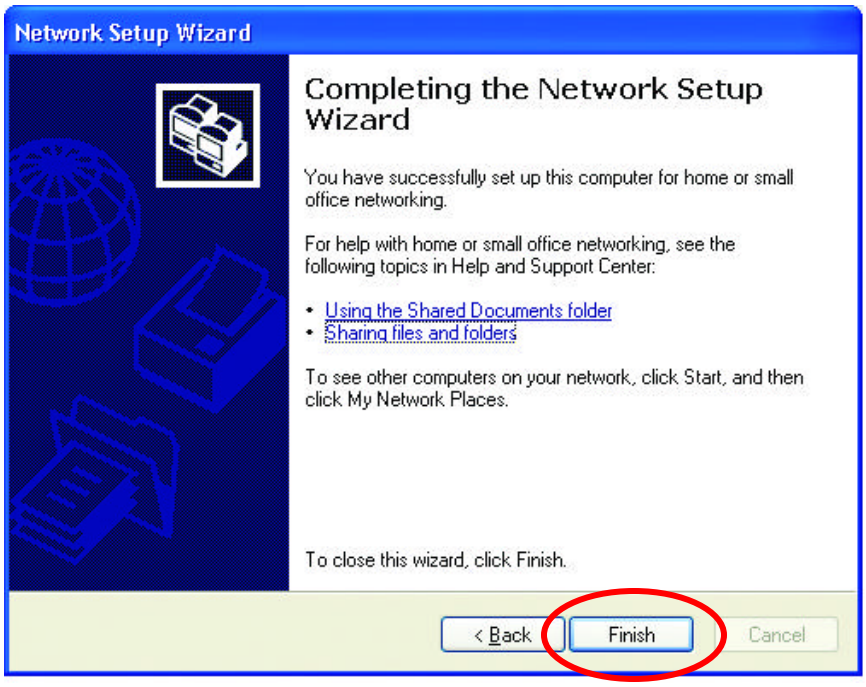


Click "**Next**" to continue with the Network Setup Wizard



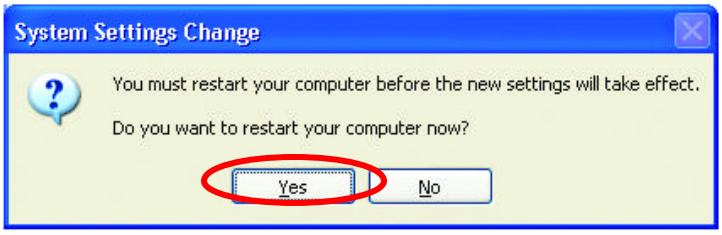
!Note: Now you may use the Network Setup Disk you just created in any PCs in your network that you wish to setup. Simply insert the Network Setup Disk into the disk drive of a PC, and open to browse the content of the disk with "My Computer" or "Windows File Manager". Double-click and run the file "netsetup"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

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



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

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

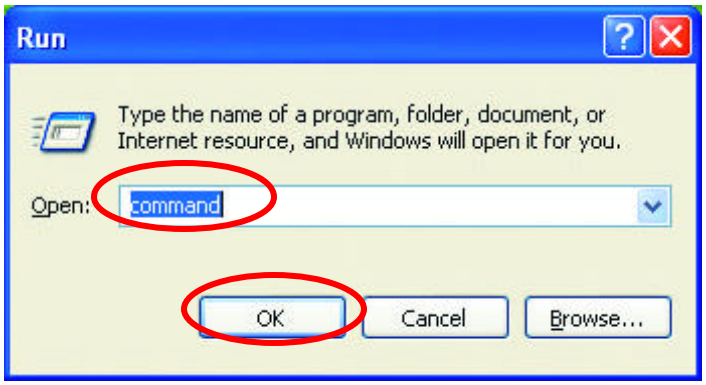


Checking IP Address of Your Computer In Windows XP

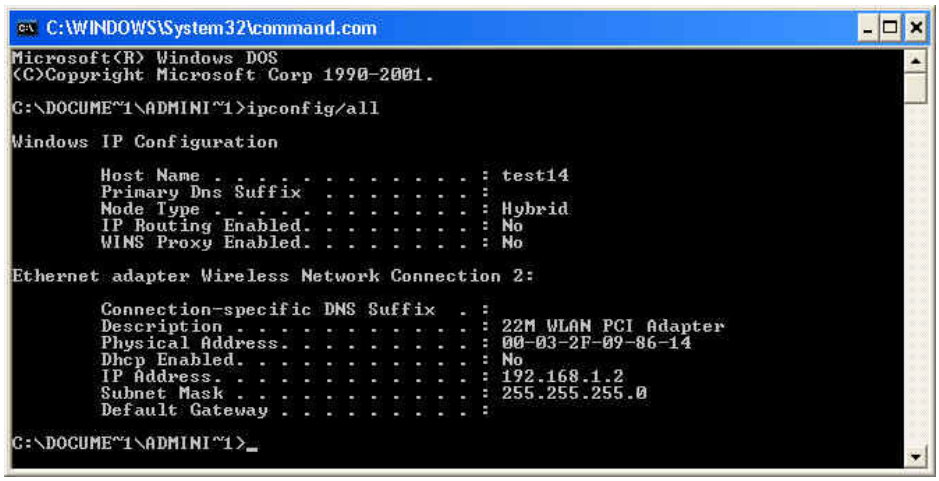
Sometimes you will need to know the IP address of the computer that you are using. For example, when you want to make sure that your computer is in the same network domain as that of your Access Point for you can configure and access the AP.

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

Click "**OK**"



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.

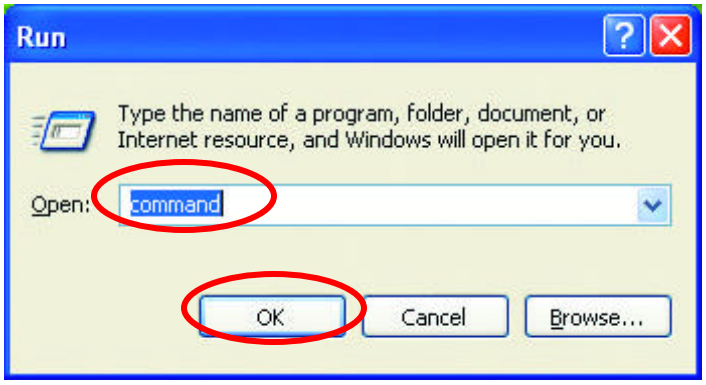


In this case, the IP address of your network adapter is 192.168.1.2, which means your Access Point must have an IP address of 192.168.1.xxx in order for you to be able to access it.

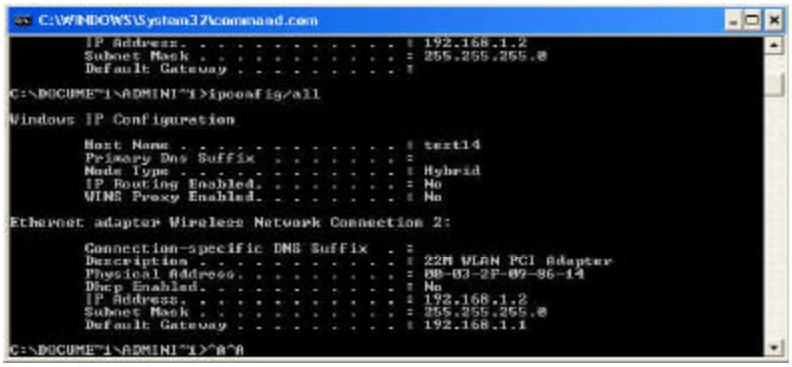
If the IP address is assigned by DHCP server on the network, there are chances you might have to release the IP and acquire it from DHCP server again. Here is how you do it.

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

Click "**OK**"



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.



In this case, the IP address that we acquired is the same as previous one, 192. 168.1.2. 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.

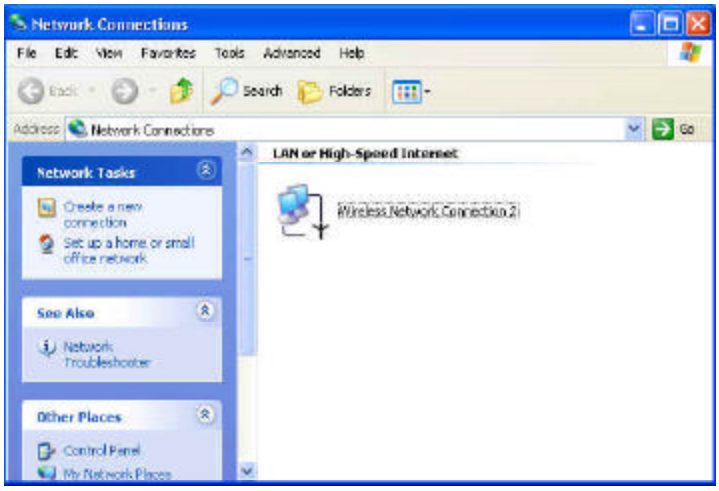
If the above methods for IP renew fail, you will have to try and restart the computer, which will reinitializes the network adapter settings during startup including renewing IP address. If you still have problems getting an IP address after computer restarts, you will have to consult with your MIS in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

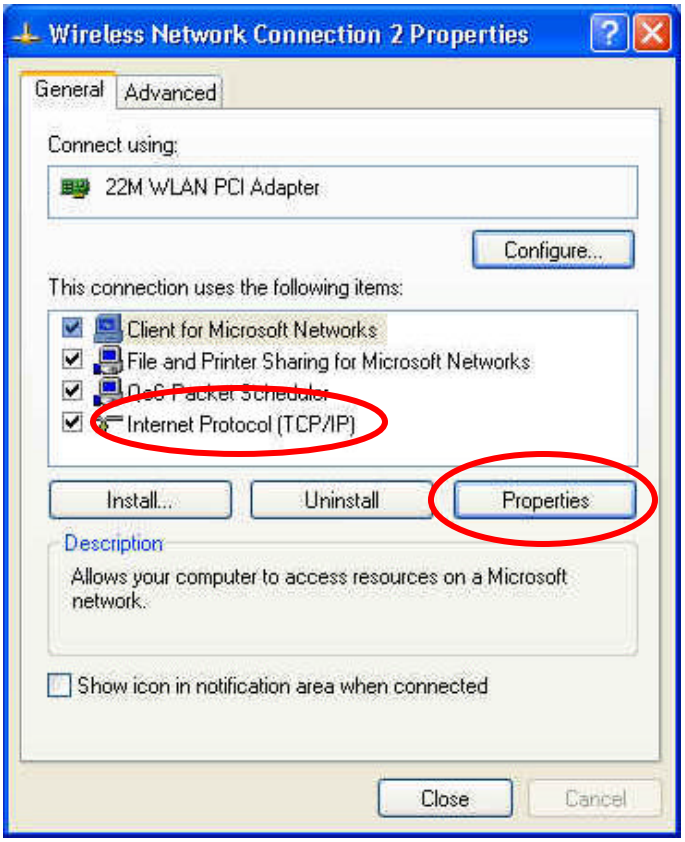
Go to **Start** menu > **Control Panel** > **Network Connections** > Right-click on the active **Local Area connection** > Select "**Properties**"



!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.

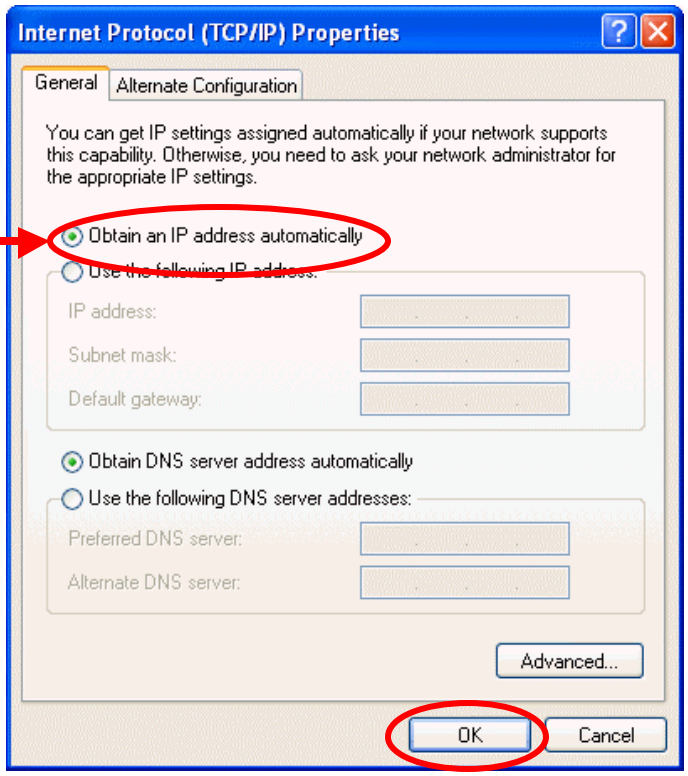


Dynamically Assigned IP Address

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



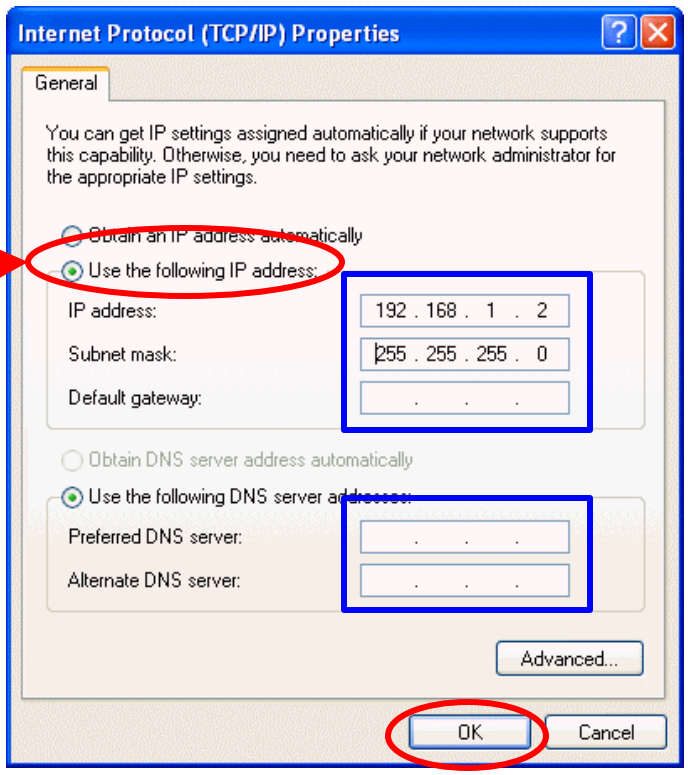
Static IP Address

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

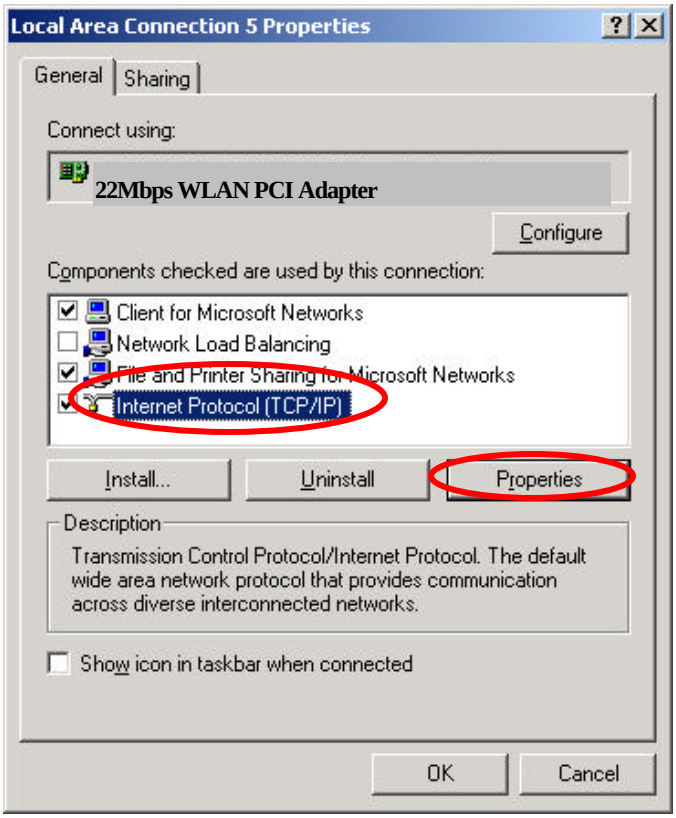


!Note: The IP address must be within the same range as the wireless route or Access Point.

Wireless Network in Windows 2000

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

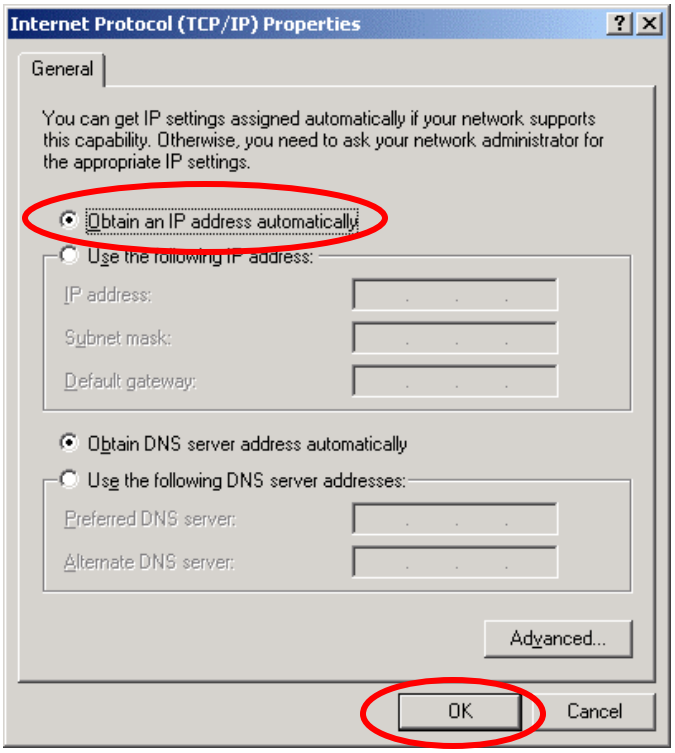
Select "**Internet Protocol (TCP/IP)**" and click "**Properties**"



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

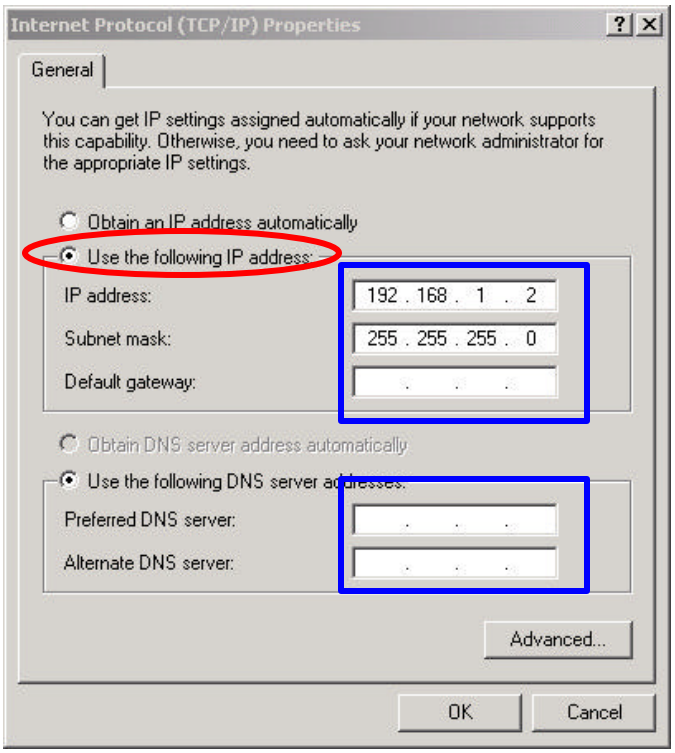


Select "**Use the following IP address**"
Enter the **IP address** and **subnet** mask fields.

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

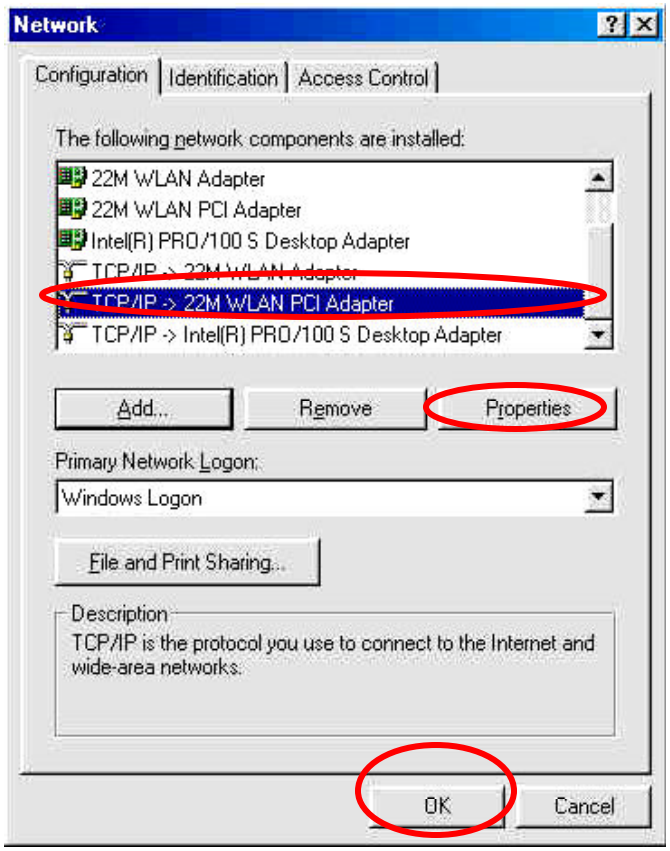


Wireless Network In Windows 98 and Windows ME

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

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

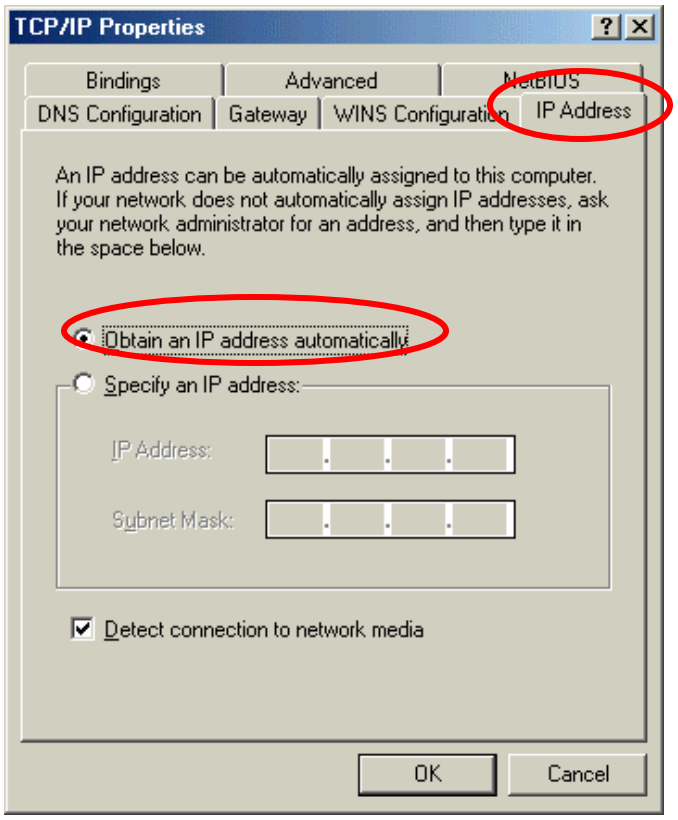
Click "**Properties**" to continue



The TCP/IP Properties window appears.

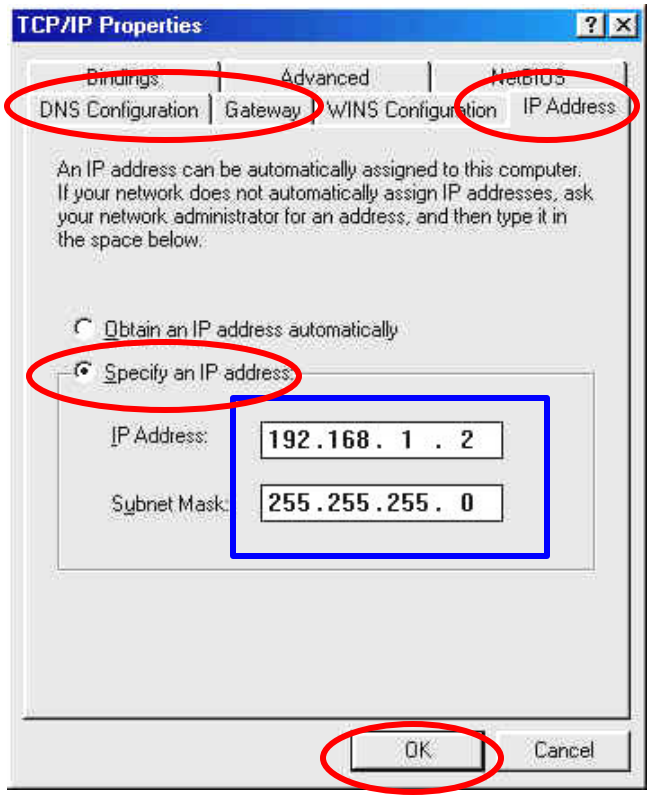
Select "**Obtain an IP address automatically**" if you are on a DHCP enabled network.

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



Select "**Use the following IP address**"
Enter the **IP address** and **subnet** mask fields.

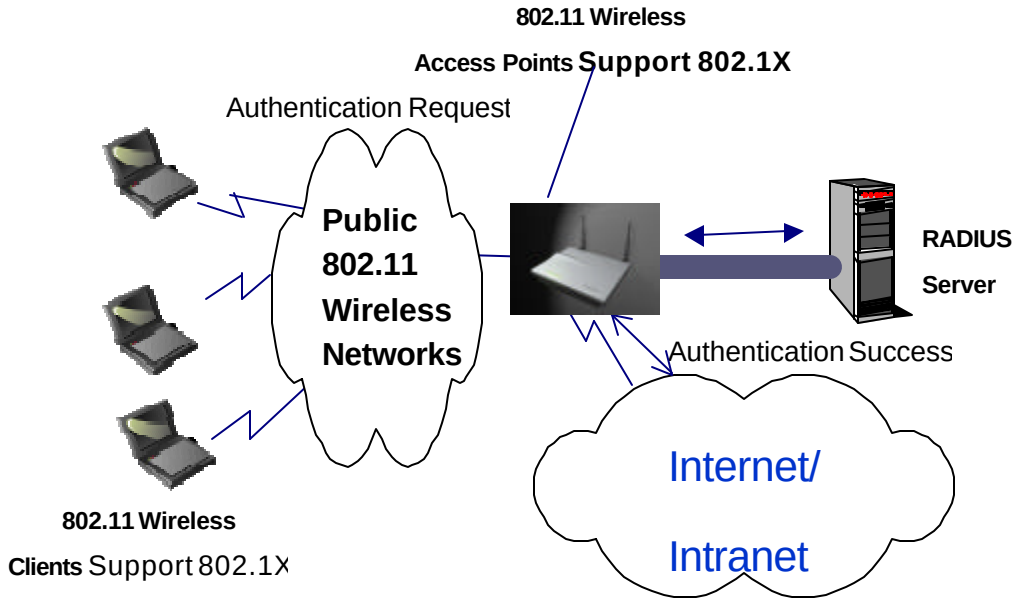
In the **DNS Configuration** Tab Page, (1) enter the IP address of the Router in the **Default gateway** field.
(2) Enter the IP address of the Router in the **DNS server** field



APPENDIX C: 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:

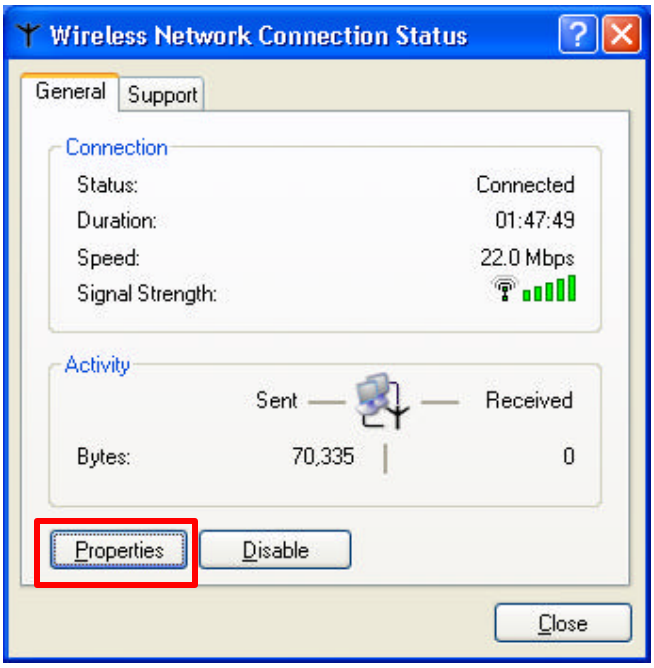
1. The client sends an EAP start message to the Access Point
2. The Access Point replies with an EAP Request ID message
3. The client sends its Network Access Identifier (NAI) – its user name – to the Access Point in an EAP Respond message.
4. The Access Point forwards the NAI to the RADIUS server with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

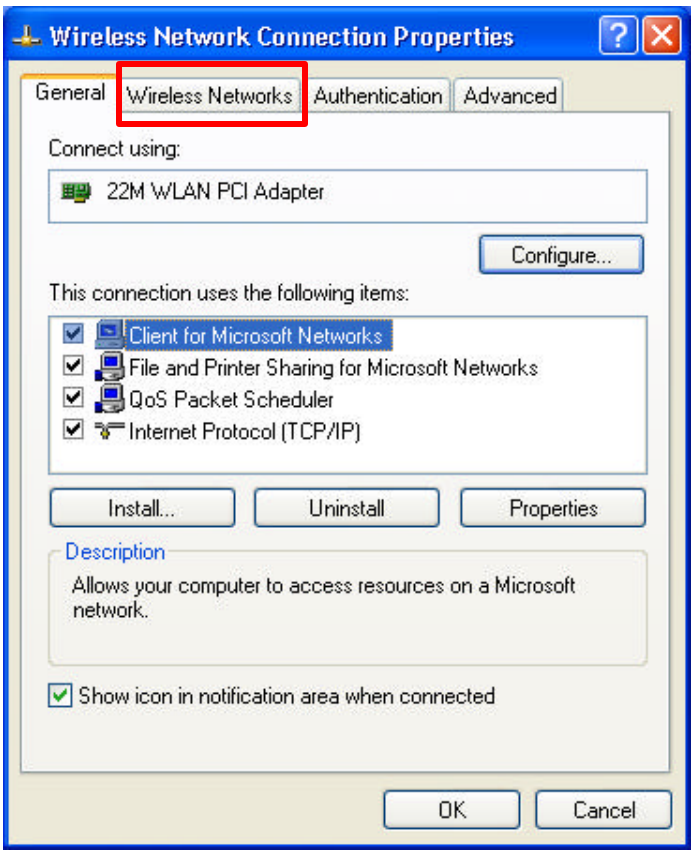
Here is the setup for the Wireless Network PC Card under Windows XP, which is the only Operating System that our driver supports for 802.1x. Microsoft is planning on supporting 802.1x security in all common Windows Operating System including Win98SE/ME/2000 by releasing Service Pack in 2003.

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.

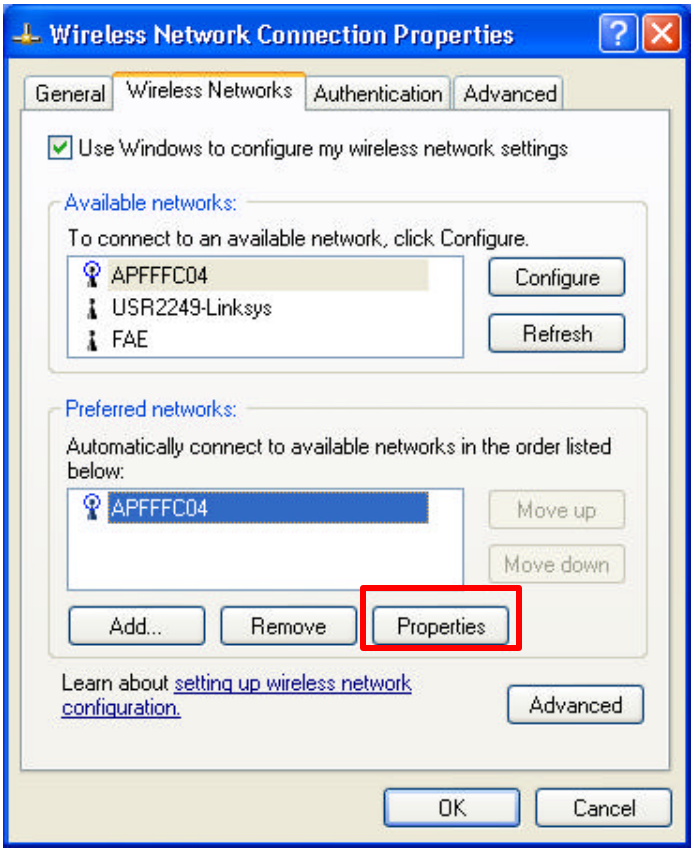


5. Click on the "**Wireless Network**" tab.



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.

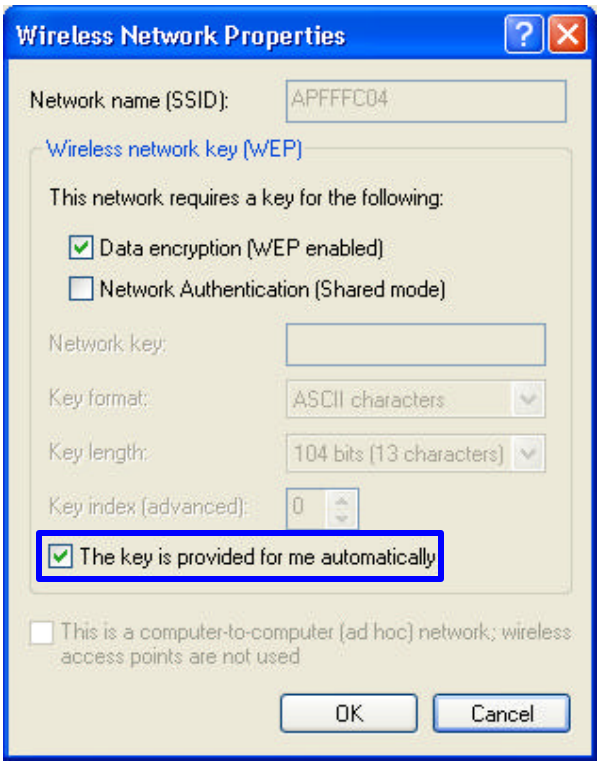


To configure for using TLS authentication method, please follow steps 7 ~ 25.

Please follow steps 26 ~ for using MD5 authentication method.

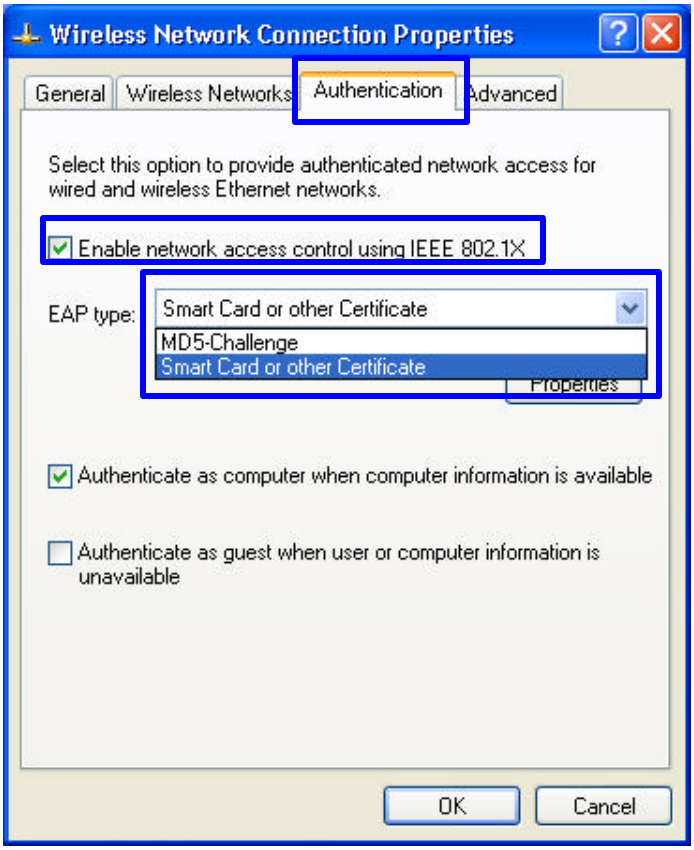
TLS Authentication

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



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.



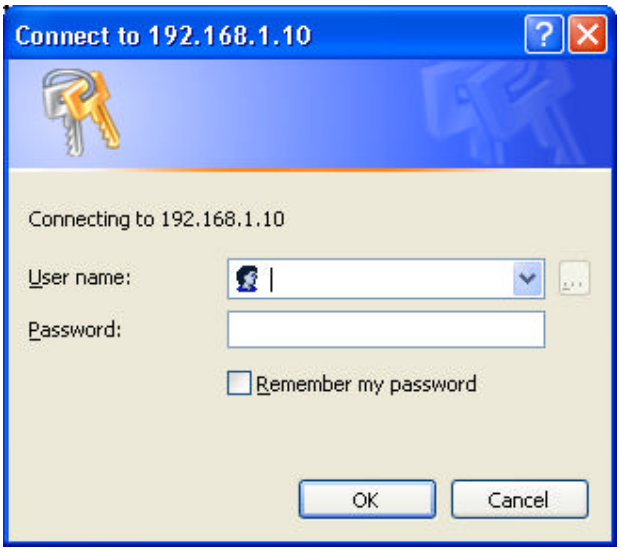
12. Click "**OK**" to close the Wireless Network Connection Properties window, thus make the changes effective.

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.

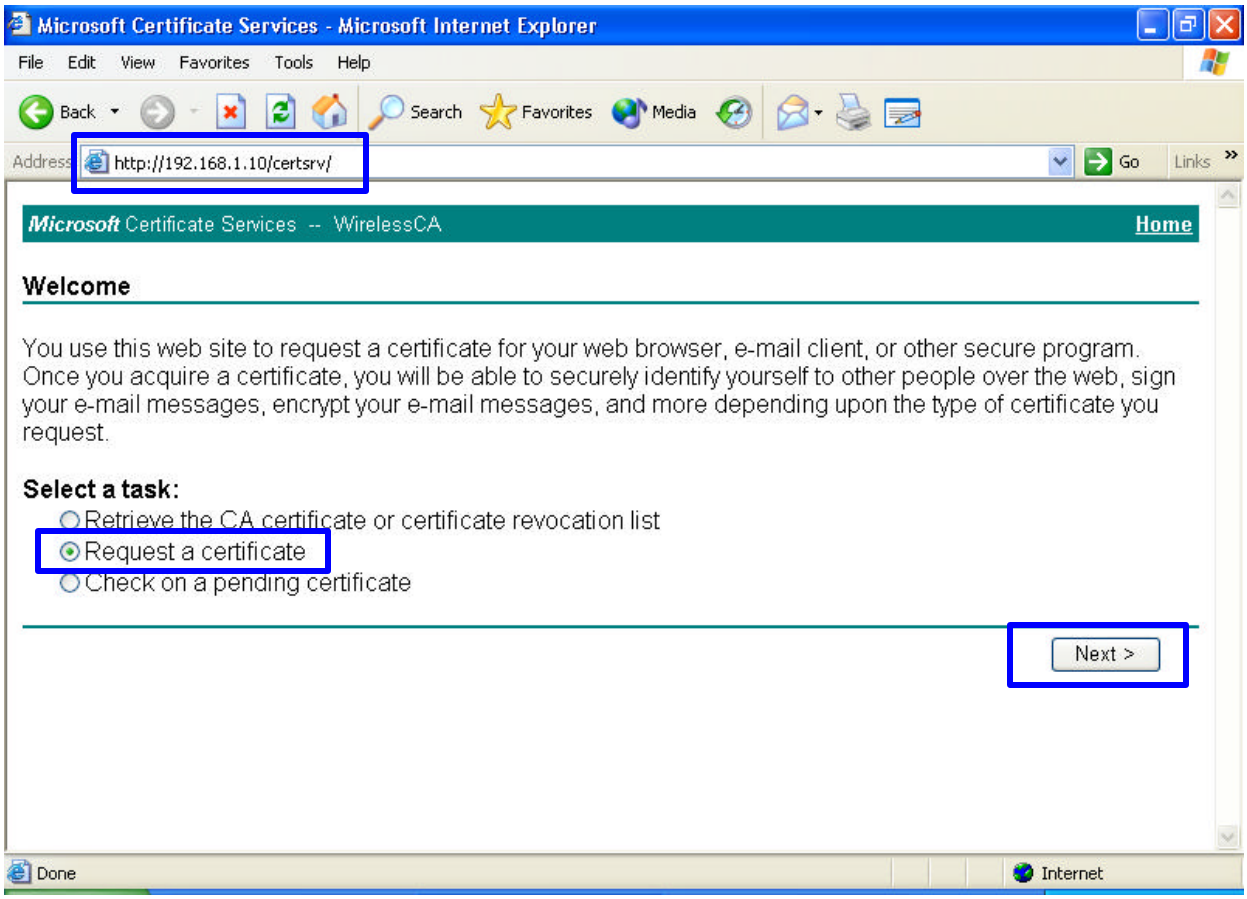


Please note that we use IP addresses for connection with the server for our illustration, and the IP of the server is 192.168.1.10.

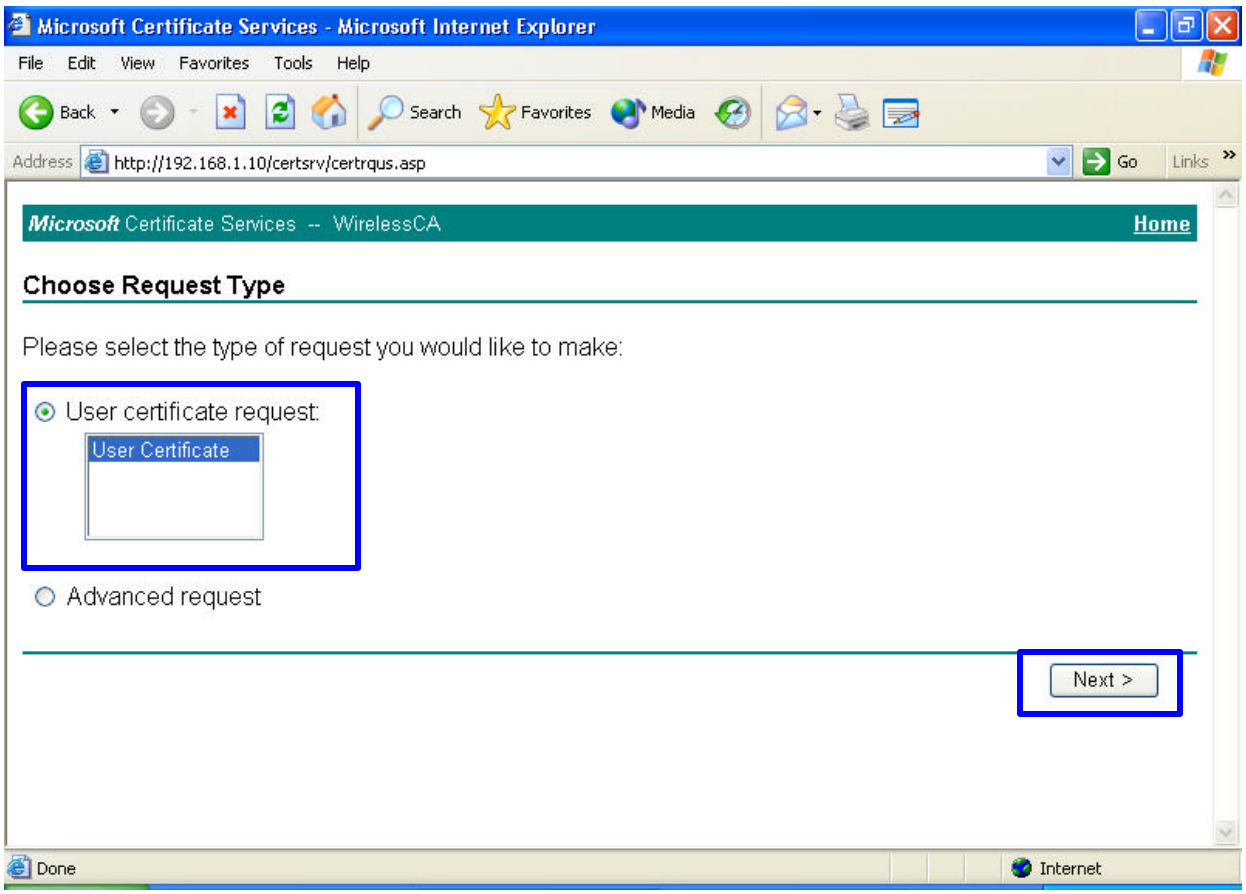
15. After successful login, open up your Internet Browser, and type the following in the address field.
    http://192.168.1.10/certsrv

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

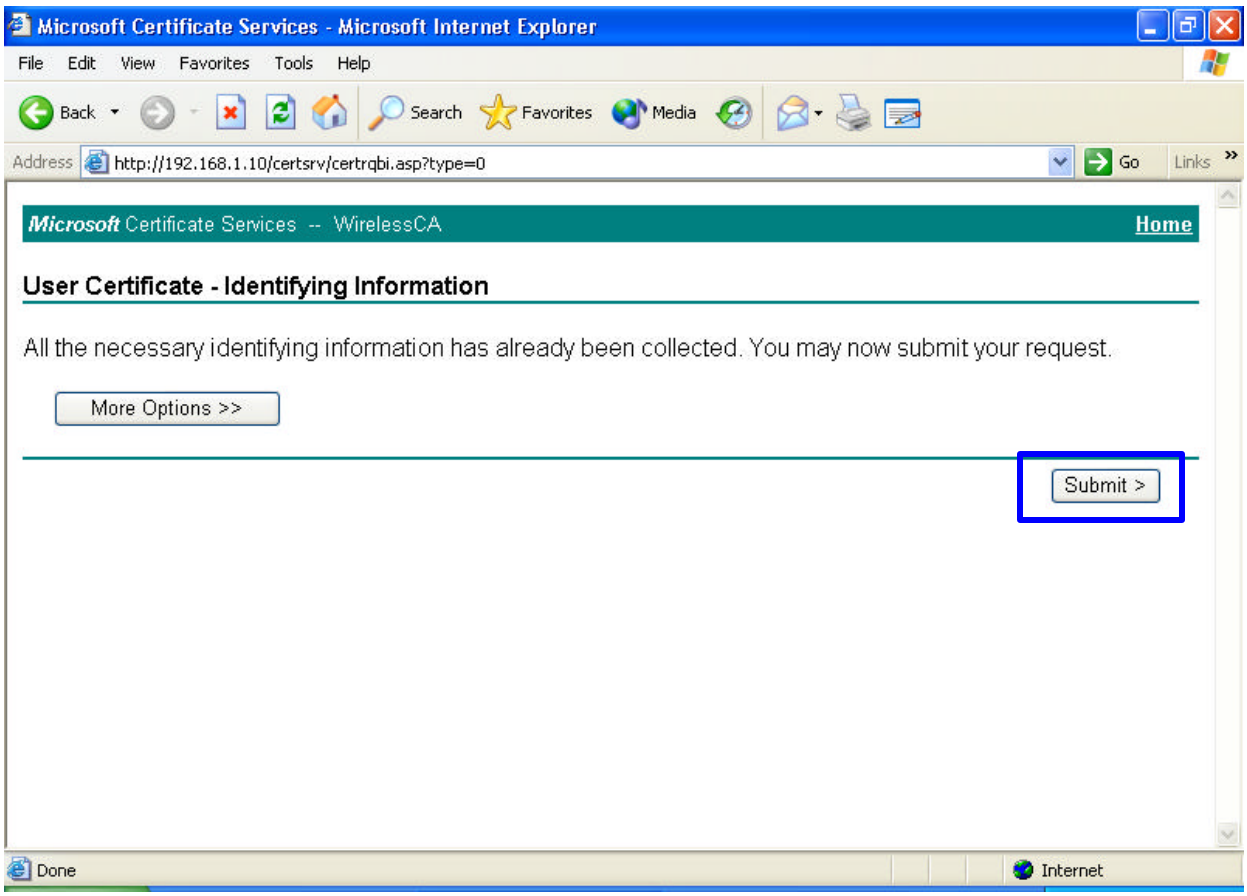
16. Now we are connected to the Certificate Service. Select "**Request a certificate** ", and click "**Next**" to continue.



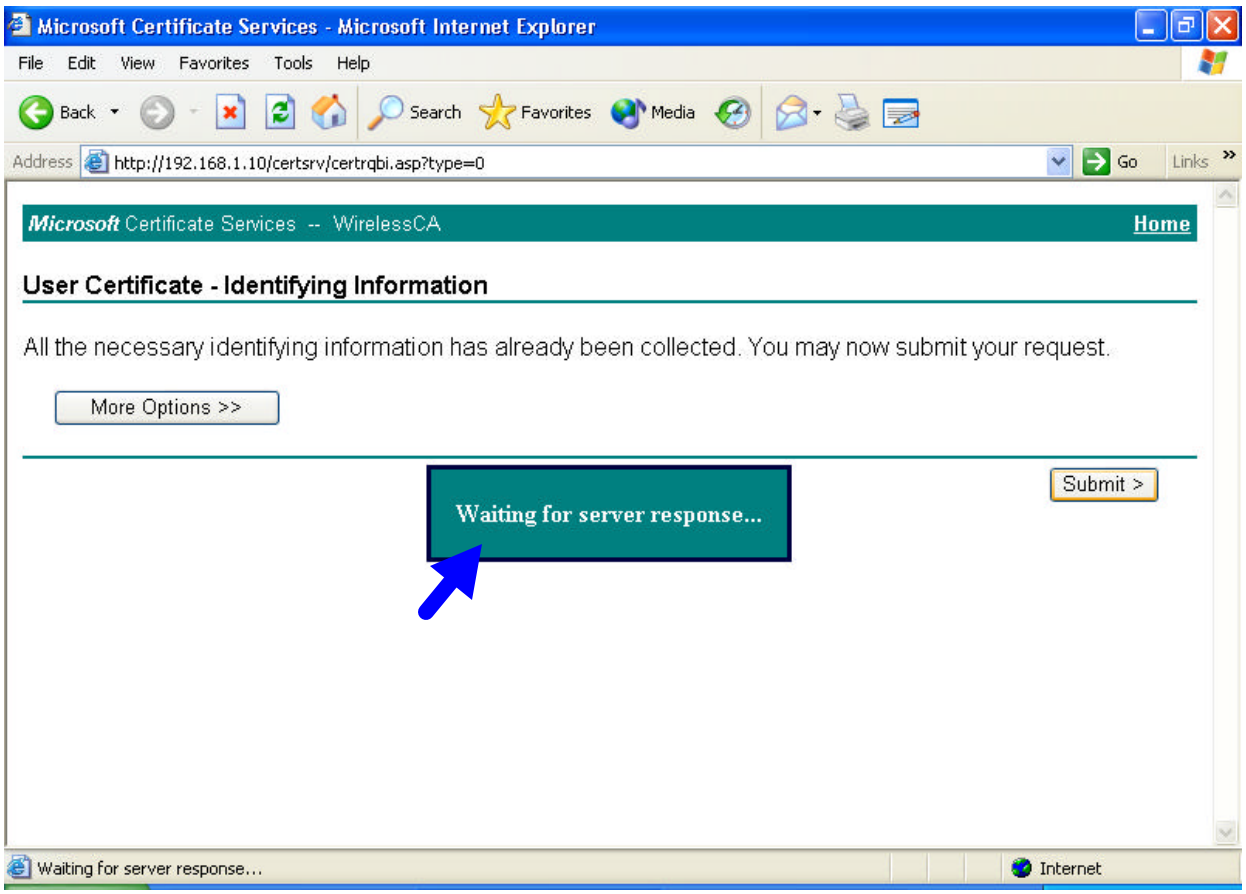
17. Select "**User Certificate request**", and click "**Next**" to continue.



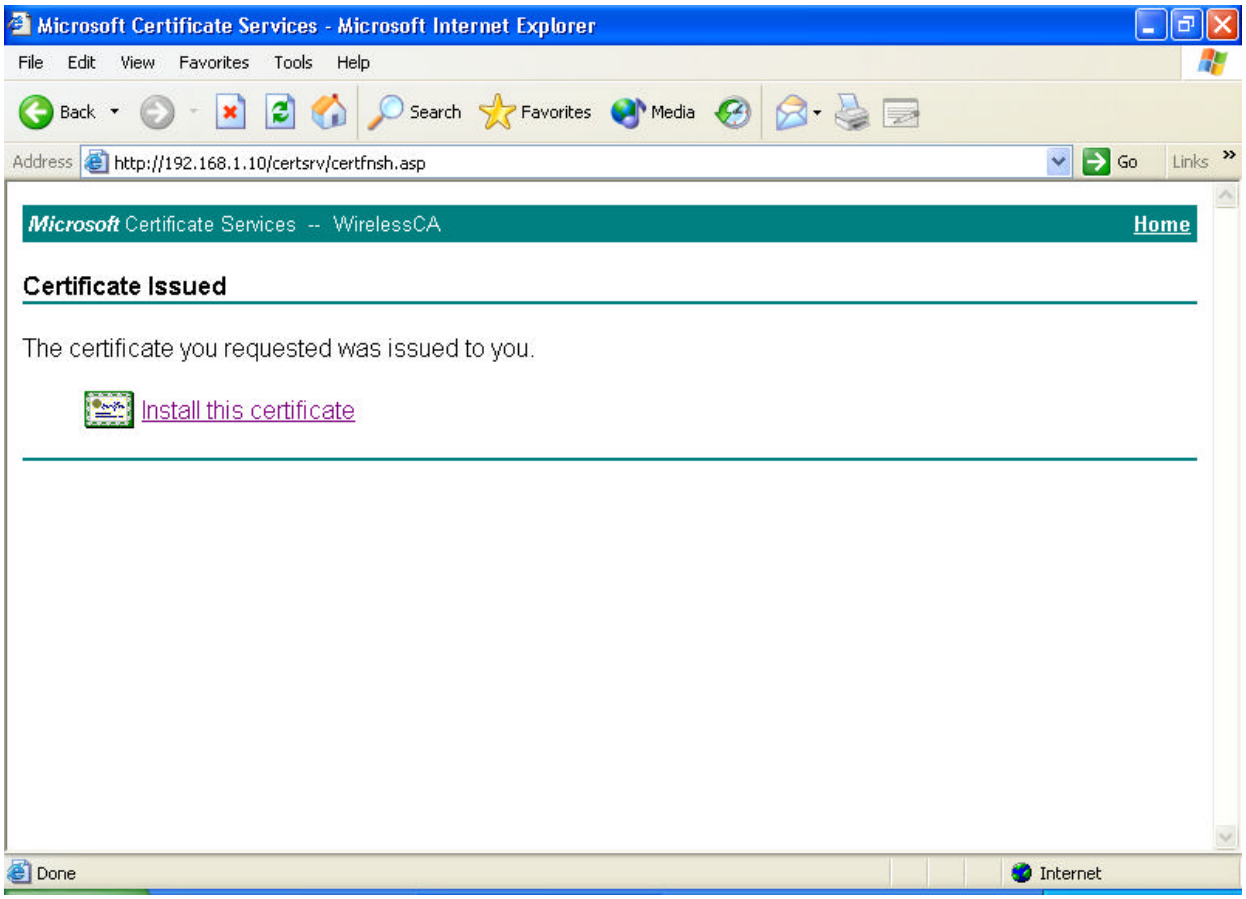
18. Click '**Submit >**" to continue.



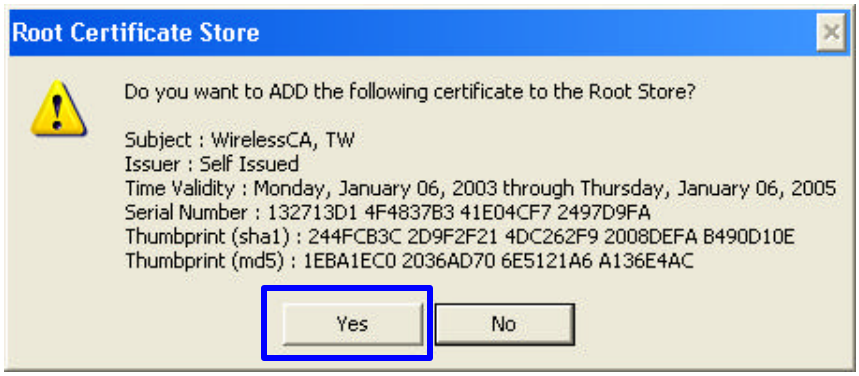
19. The Certificate Service is now processing the certificate request.



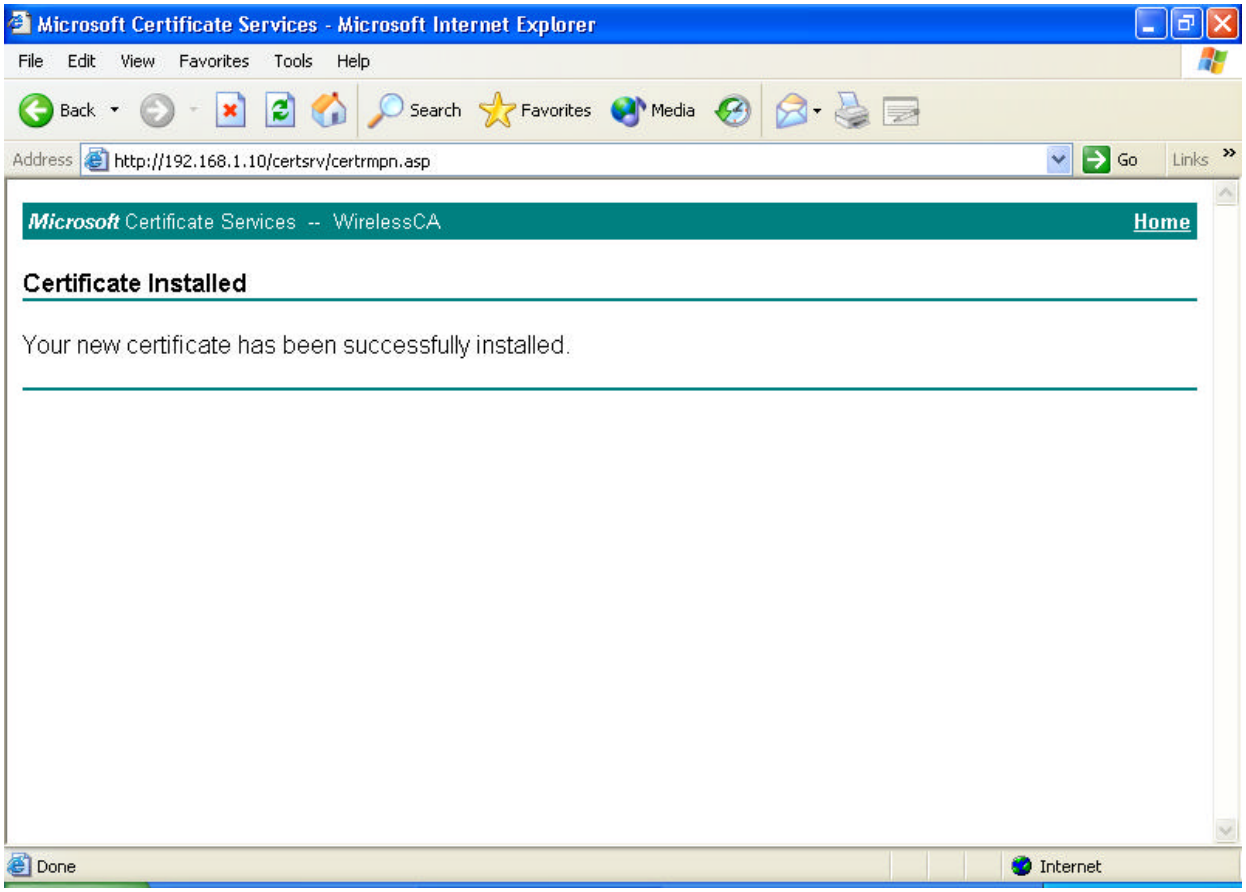
20. The certificate is issued by the server, click “Install this certificate” to download and store the certificate to your local computer.



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

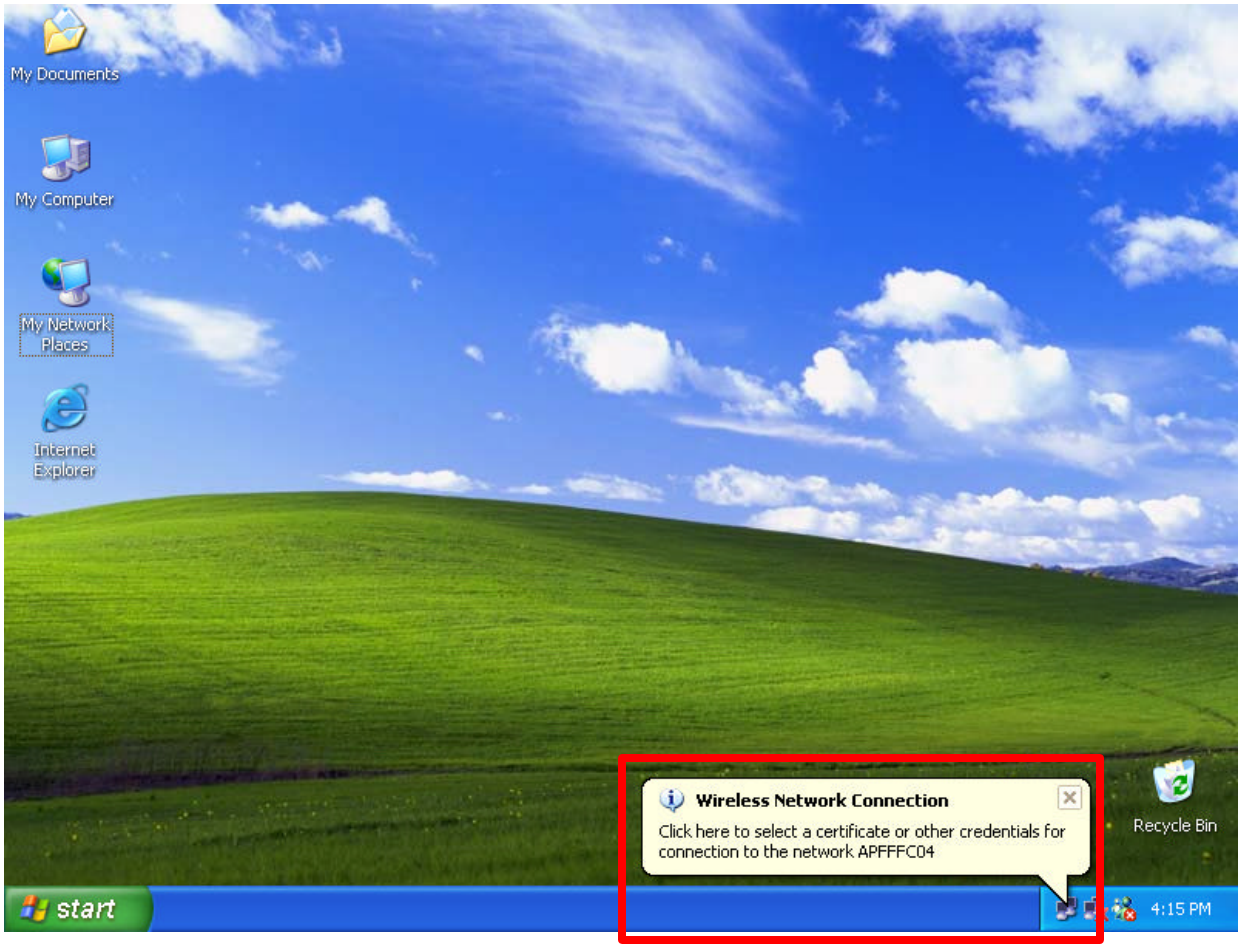


22. Certificate is now installed.

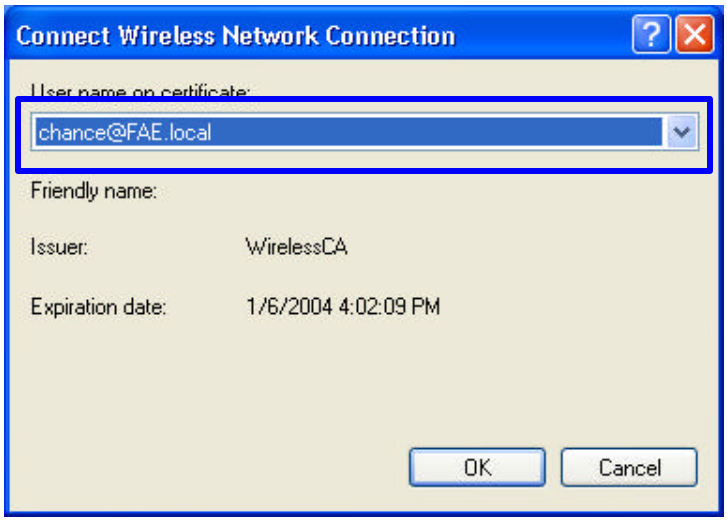


All the configuration and certificate download are now complete. Let's try to connect to the Access Point using 802.1x TLS Authentication.

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.



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

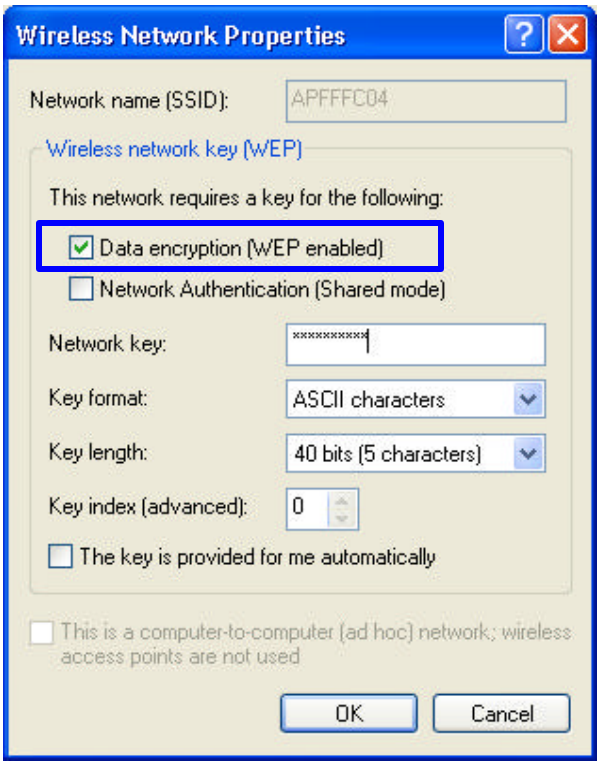


25. Check the server to make sure that it's the server that issues certificate, and click "**OK**" to complete the authentication process.

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.



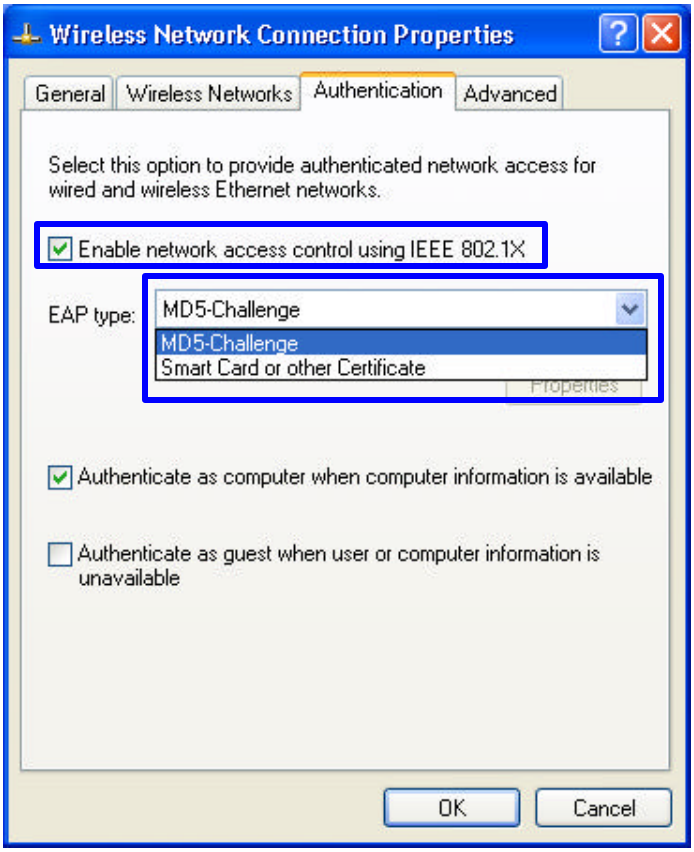
Please note that that value of Network key entered, and key format/length used, must be the same as that used in the Access Point. Although there are 4 set of keys can be set in the Access Point WEP configuration, it's the ***first set*** of key that must be the same as that we used by the supplicant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

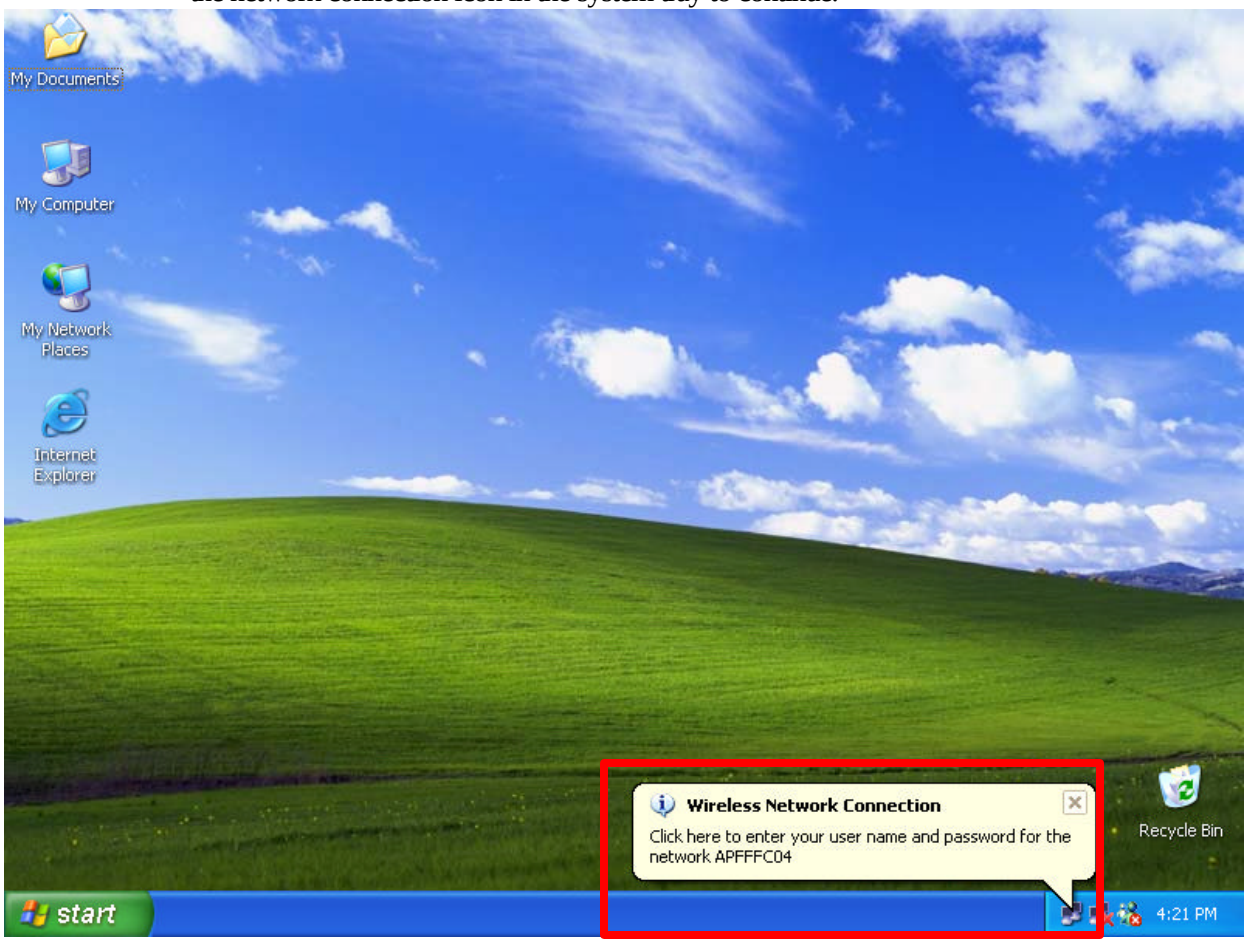
33. Select "**MD-5 Challenge**" from the drop-down list box for EAP type.



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

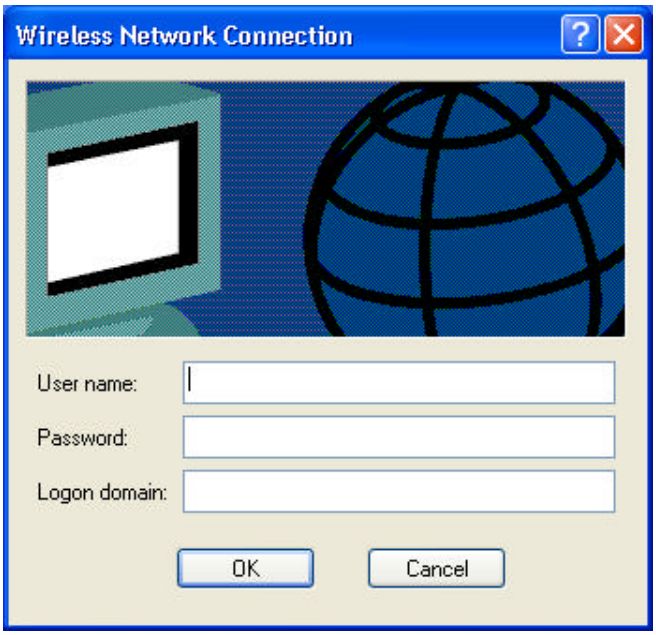
Unlike TLS, which uses digital certificate for validation, the MD-5 Authentication is based on the user account/password. Therefore, you must have a valid account used by the server for validation.

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



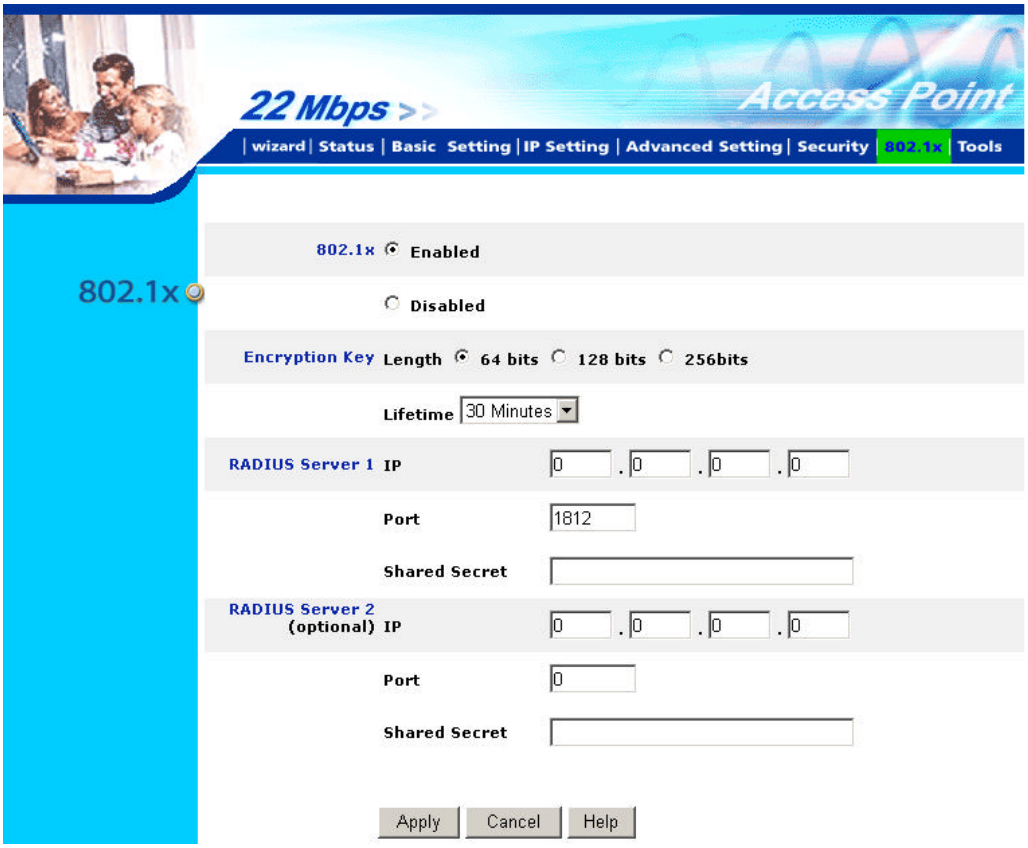
36. Enter the user name, password and the logon domain that your account belongs if you have one or more network domain exist in your network.

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



Authenticator: Wireless Network Access Point

This is the web page configuration in the Access Point that we use.



1. Enable 802.1x security by selecting "**Enable** ".
2. If **MD5** EAP methods is used then you can skip step 3 and go to step 4.
3. 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.
4. Enter the **IP address** of and the **Port** used by the **Primary** Radius Server

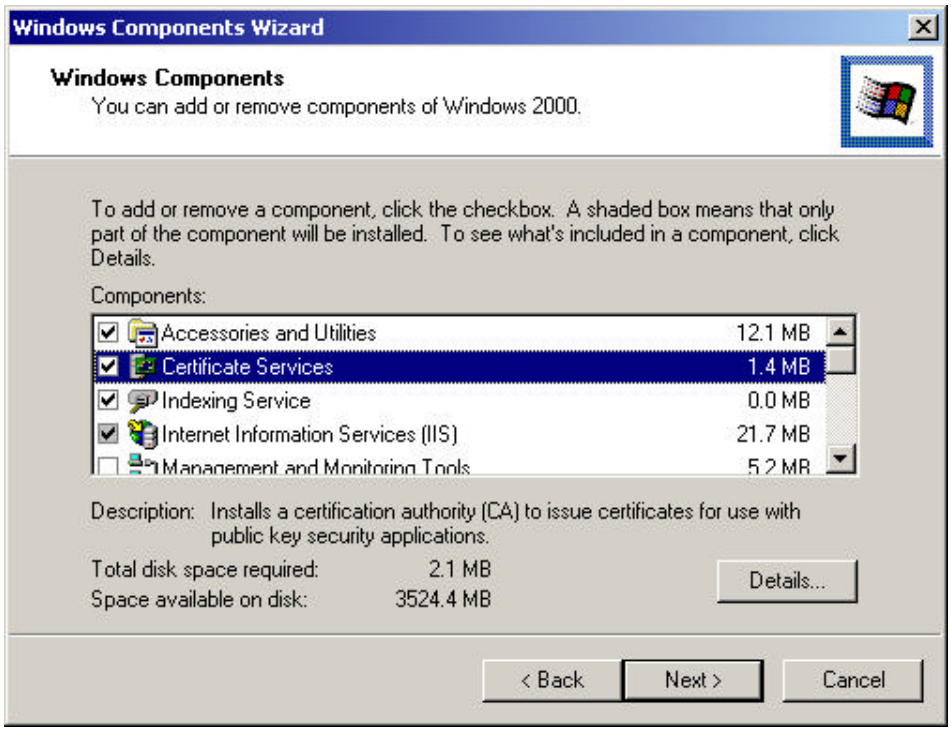
   Enter the **Shared Secret**, which is used by the Radius Server.
5. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.
6. Click "**Apply**" button for the 802.1x settings to take effect after Access Point reboots itself.

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

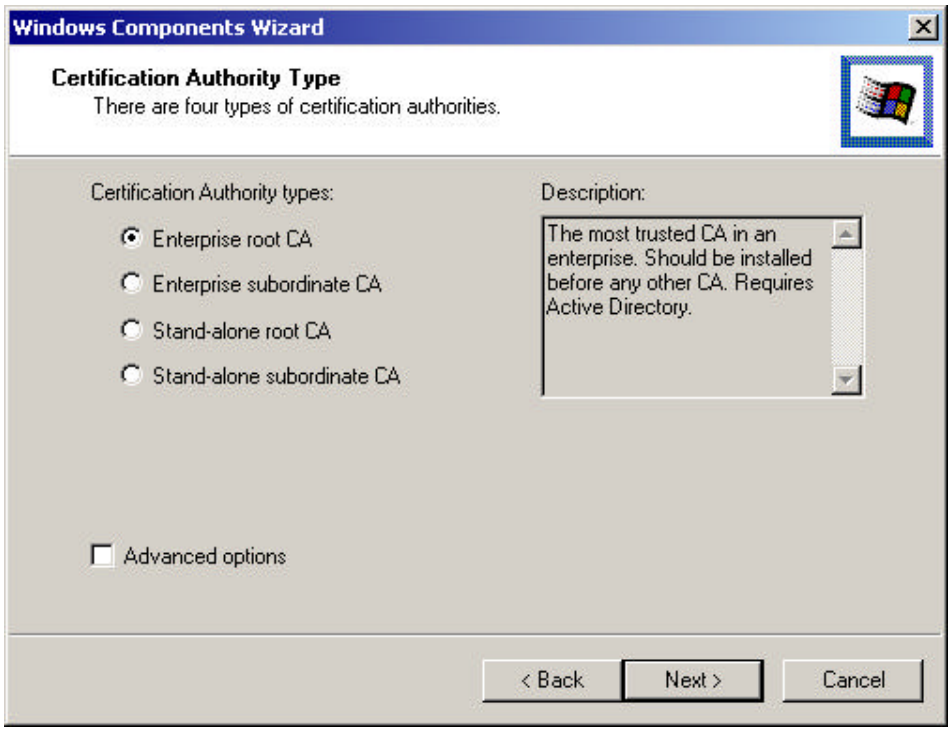
Radius Server: Window2000 Server

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.

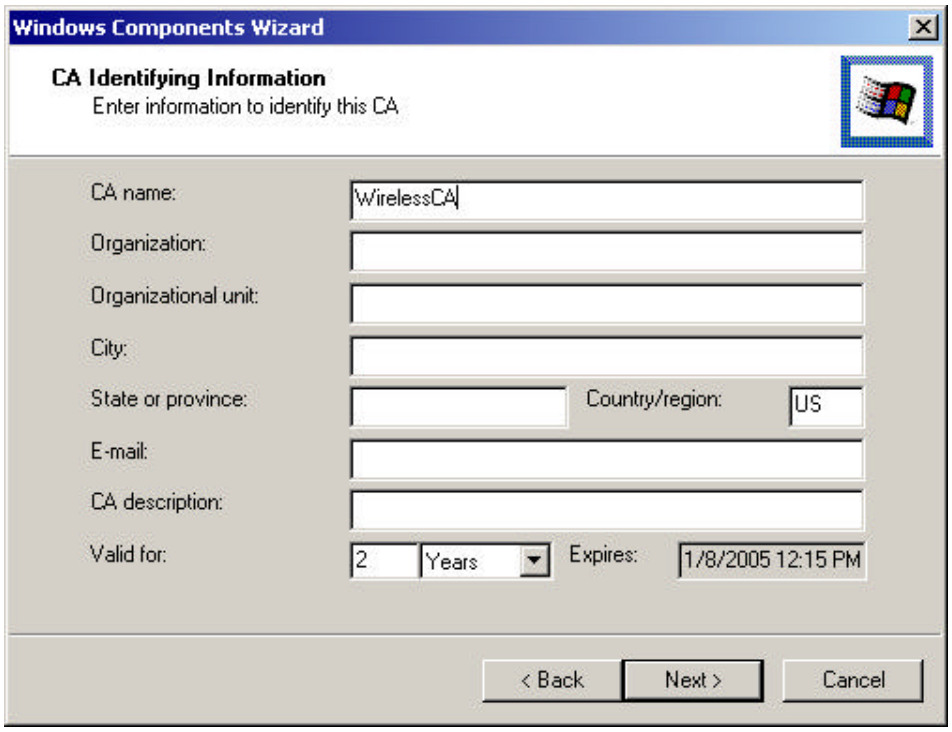
1. Login into your Windows 2000 Server as Administrator, or account that has Administrator authority.
2. Go to **Start** > **Control Panel**, and double-click "Add or Remove Programs"
3. Click on "**Add/Remove Windows components**"
4. Check "**Certificate Services**", and click "Next" to continue.



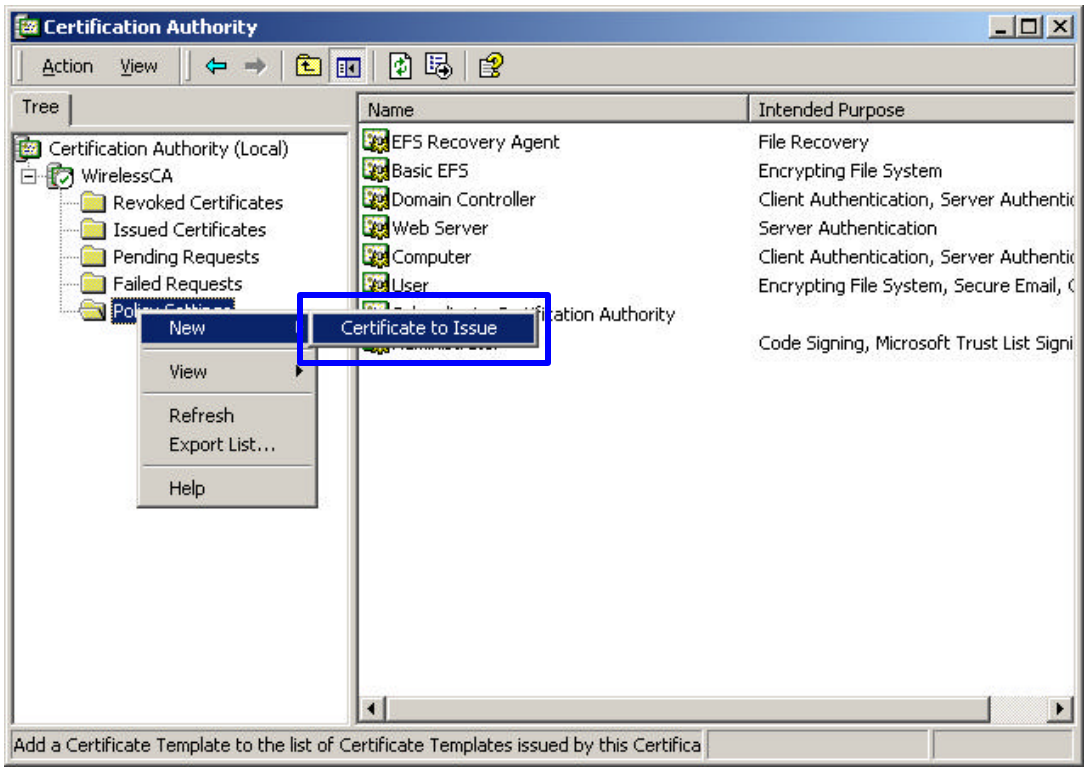
5. Select "**Enterprise root CA**", and click "**Next**" to continue.



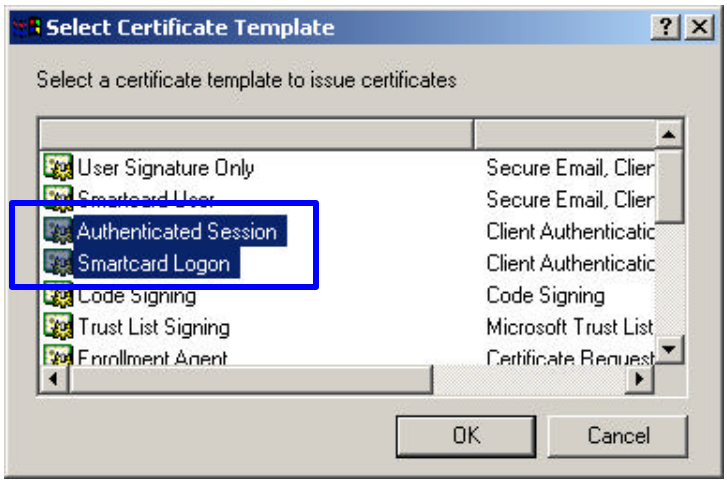
6. Enter the information that you want for your Certificate Service, and click "**Next**" to continue.



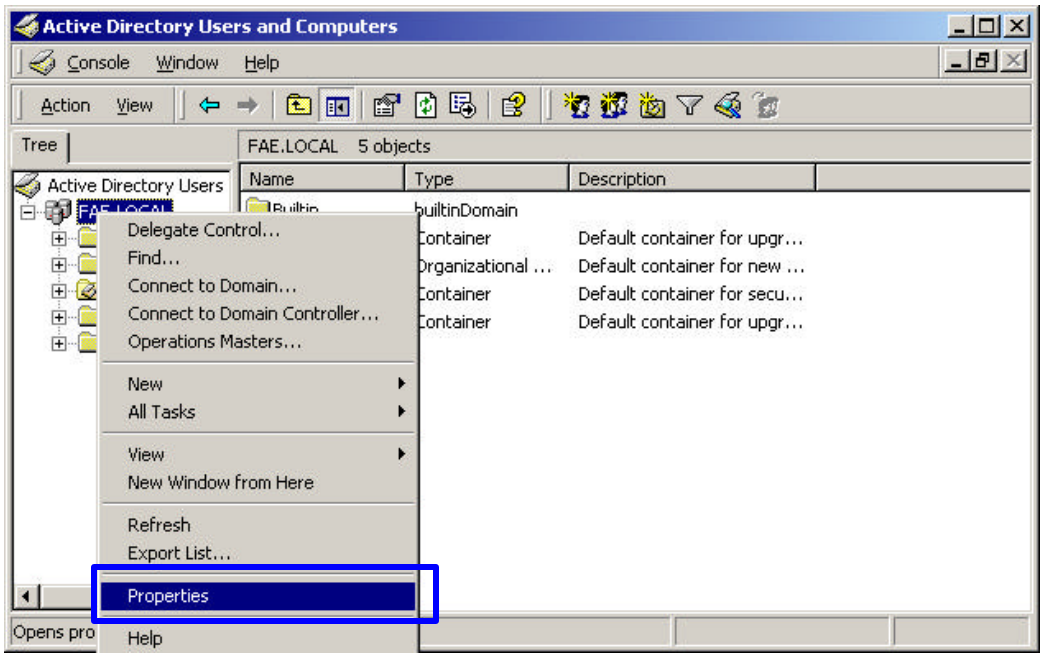
7. Go to Start > Program > Administrative Tools > **Certificate Authority**
8. Right-click on the "**Policy Setting**", select "**new**"
9. Select "**Certificate to Issue**"



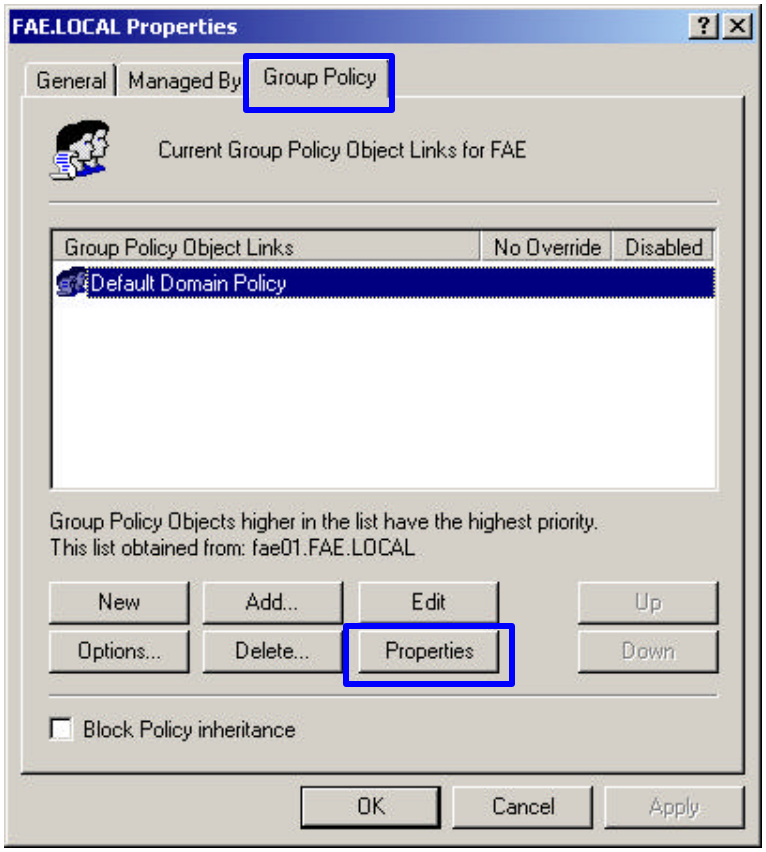
10. Select "**Authenticated Session**" and "**Smartcard Logon**" by holding down to the Ctrl key, and click "**OK**" to continue.



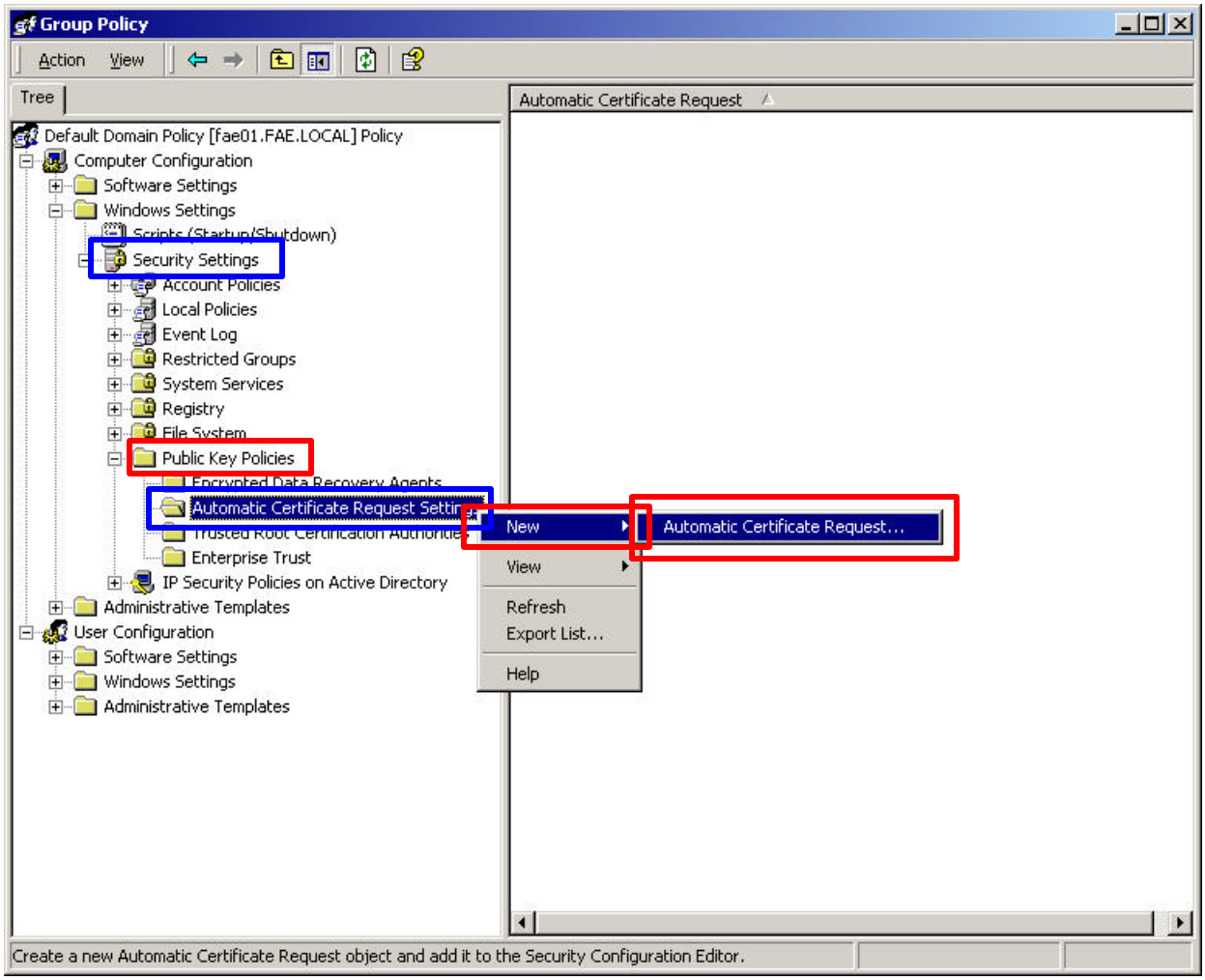
11. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.
12. Right-click on domain, and select "**Properties**" to continue.



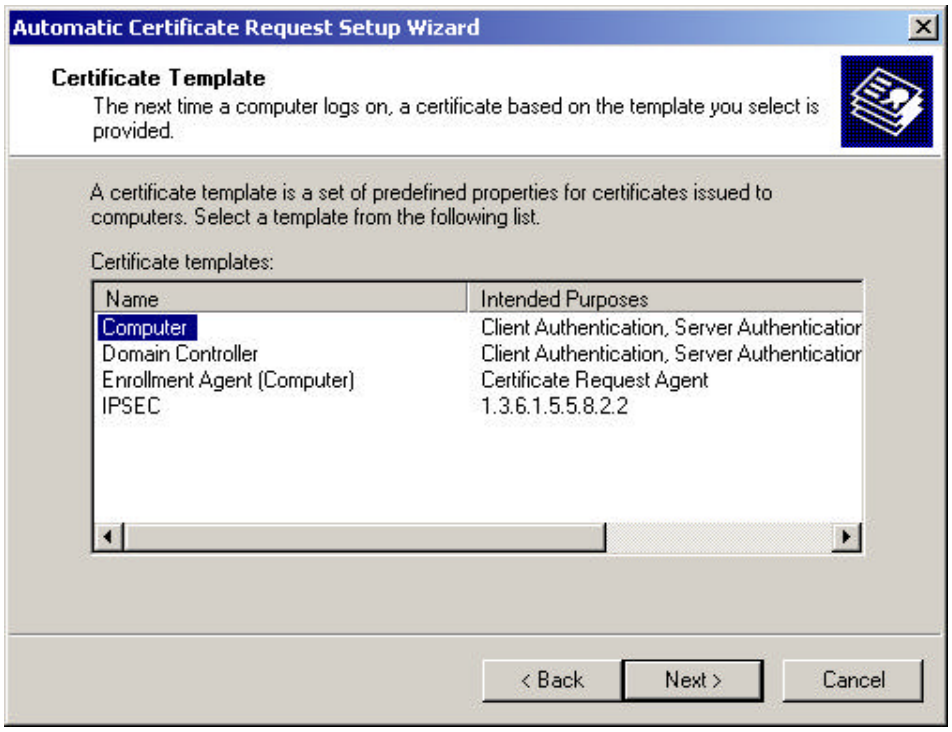
13. Select "**Group Policy**" tab and click "**Properties**" to continue.



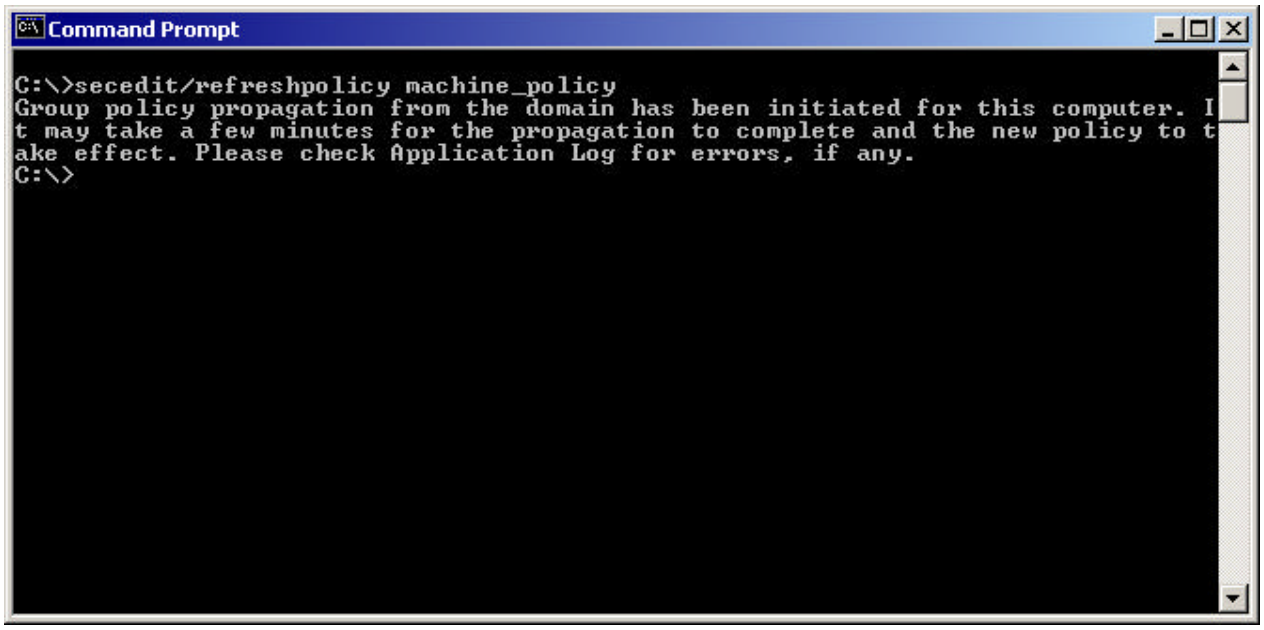
14. Go to “Computer Configuration” > “Security Settings” > “**Public Key Policies**”
15. Right-click “**Automatic Certificate Request Setting**”, and select “**New**”
16. Click “**Automatic Certificate Request ...**”



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

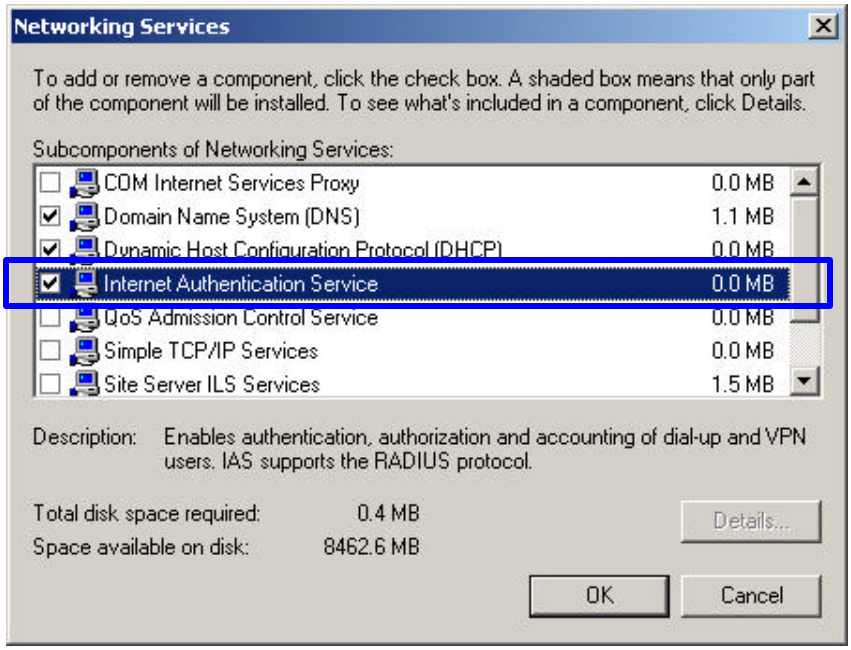


18. Click "**Finish**" to complete the Automatic Certificate Request Setup
19. Go to Start > **Run**, and type "**command**" and click "**Enter**" to open Command Prompt.
20. Type "secedit/refreshpolicy machine_policy" to refresh policy.



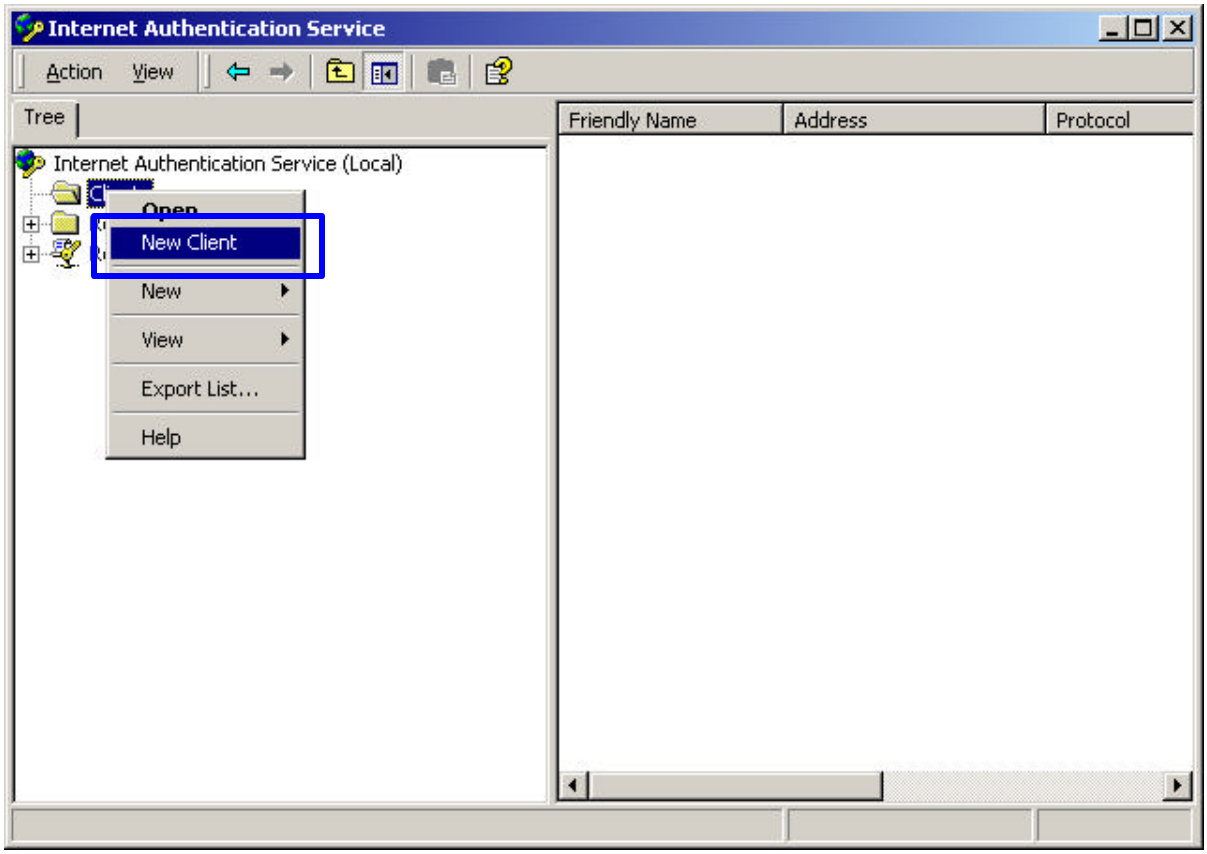
Adding Internet Authentication Service

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.

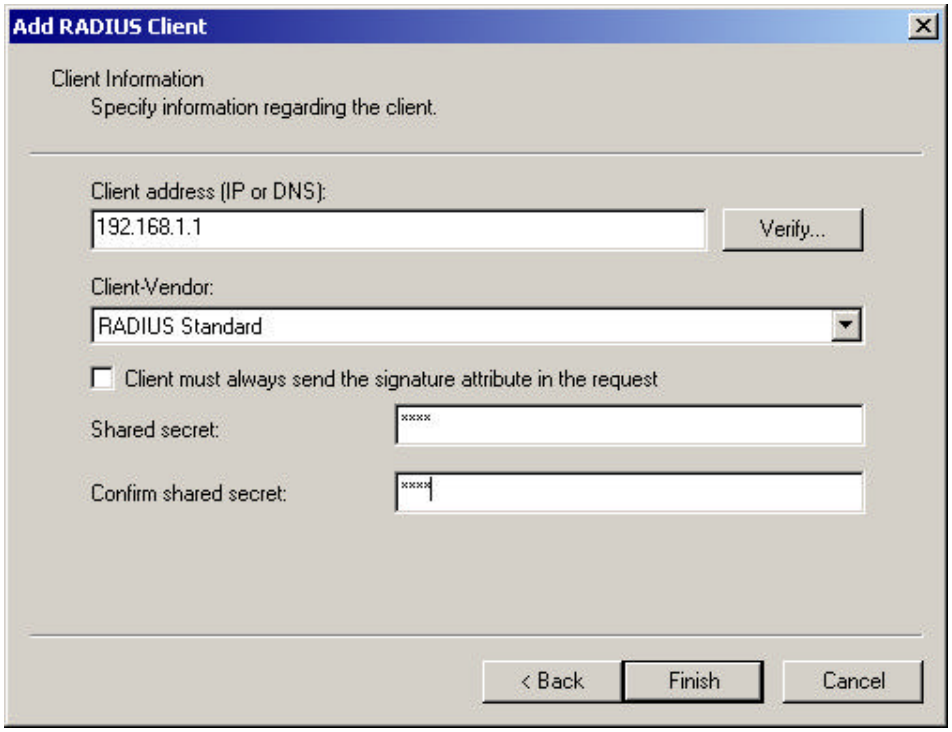


Setting Internet Authentication Service

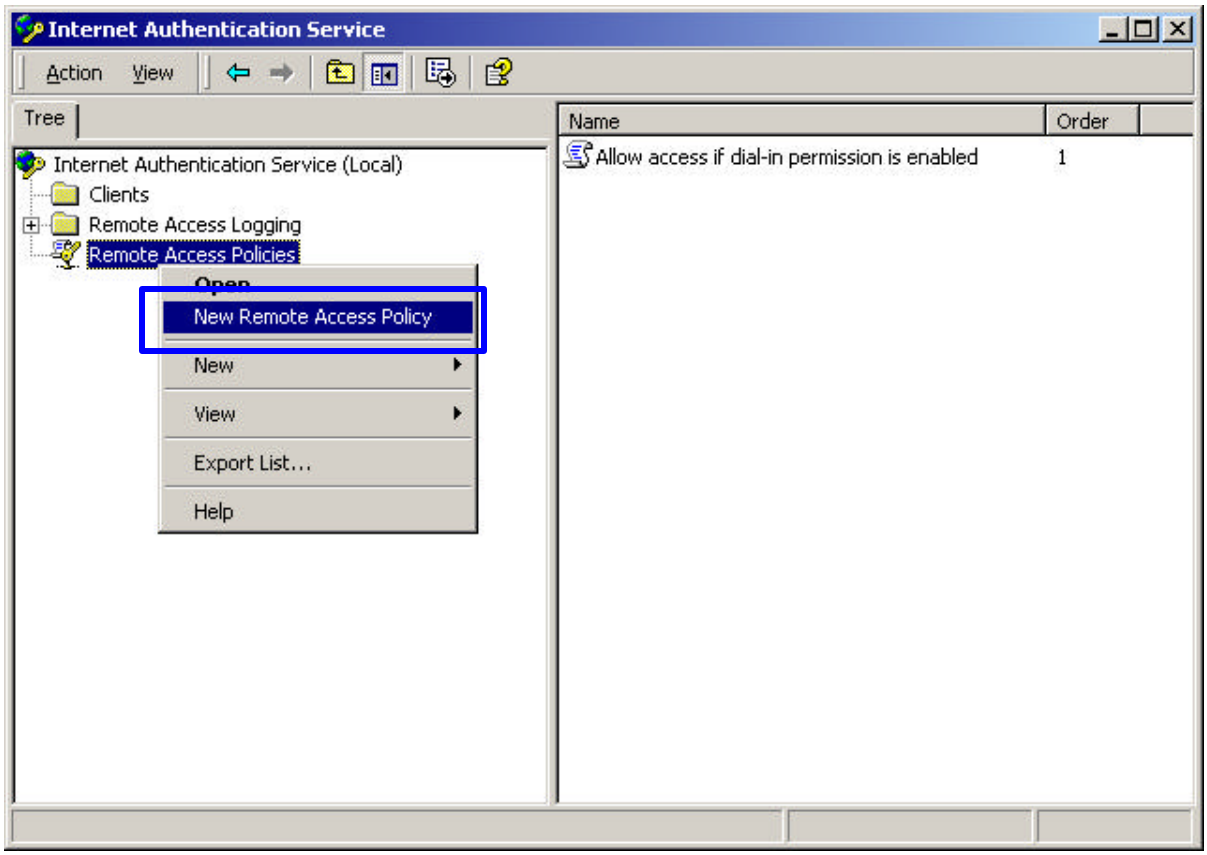
24. Go to Start > Program > Administrative Tools > **Internet Authentication Service**
25. Right-click "**Client**", and select "**New Client**"



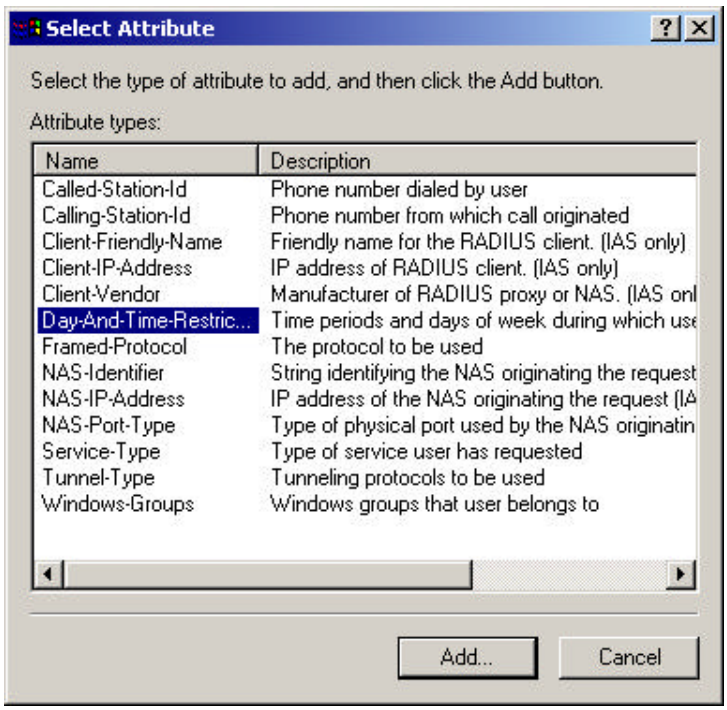
26. Enter the IP address of the Access Point in the **Client address** text field, a memorable name for the Access Point in the **Client-Vendor** text field, the access password used by the Access Point in the **Shared secret** text field. Re-type the password in the **Confirmed shared secret** text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



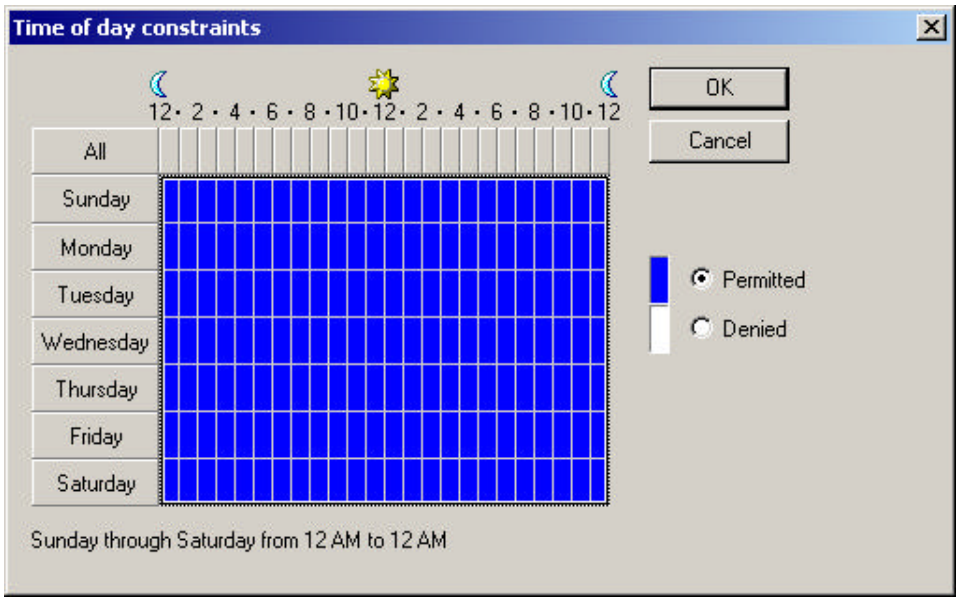
28. In the Internet Authentication Service, right-click "**Remote Access Policies**"
29. Select "New Remote Access Policy".



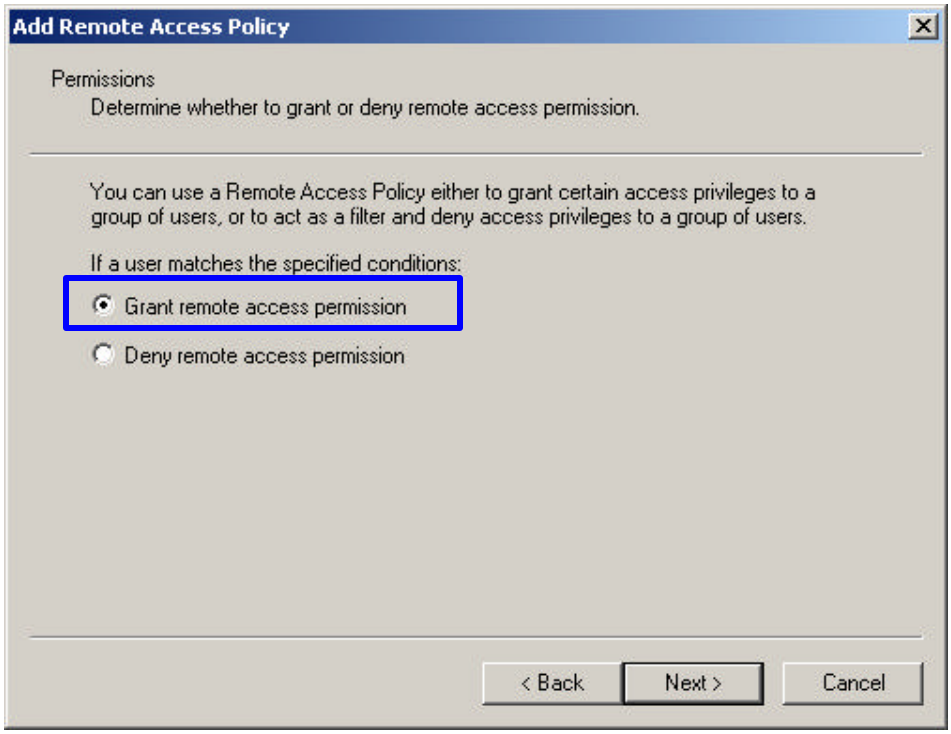
30. Select "**Day-And-Time-Restriction**", and click "**Add**" to continue.



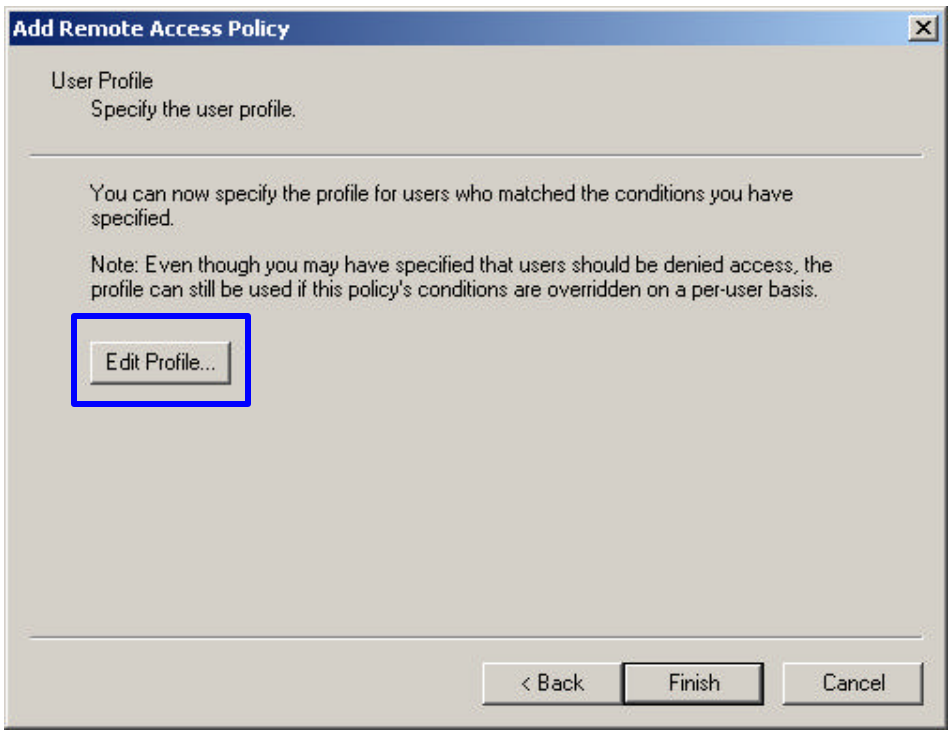
31. Unless you want to specify the active duration for 802.1x authentication, click "**OK**" to accept to have 802.1x authentication enabled at all times.



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

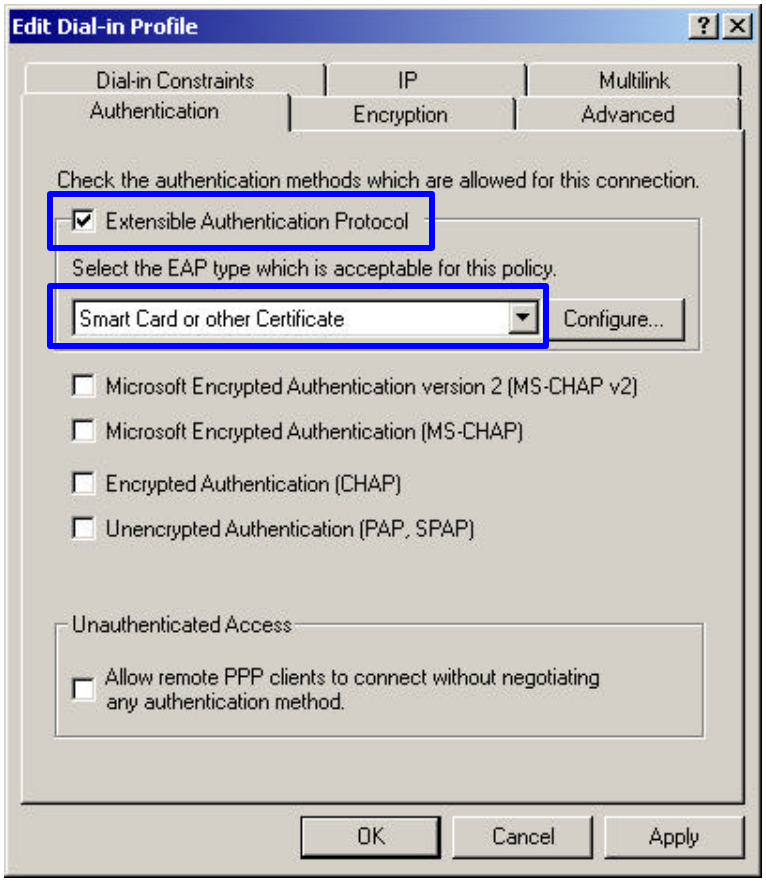


33. Click “Edit Profile” to open up

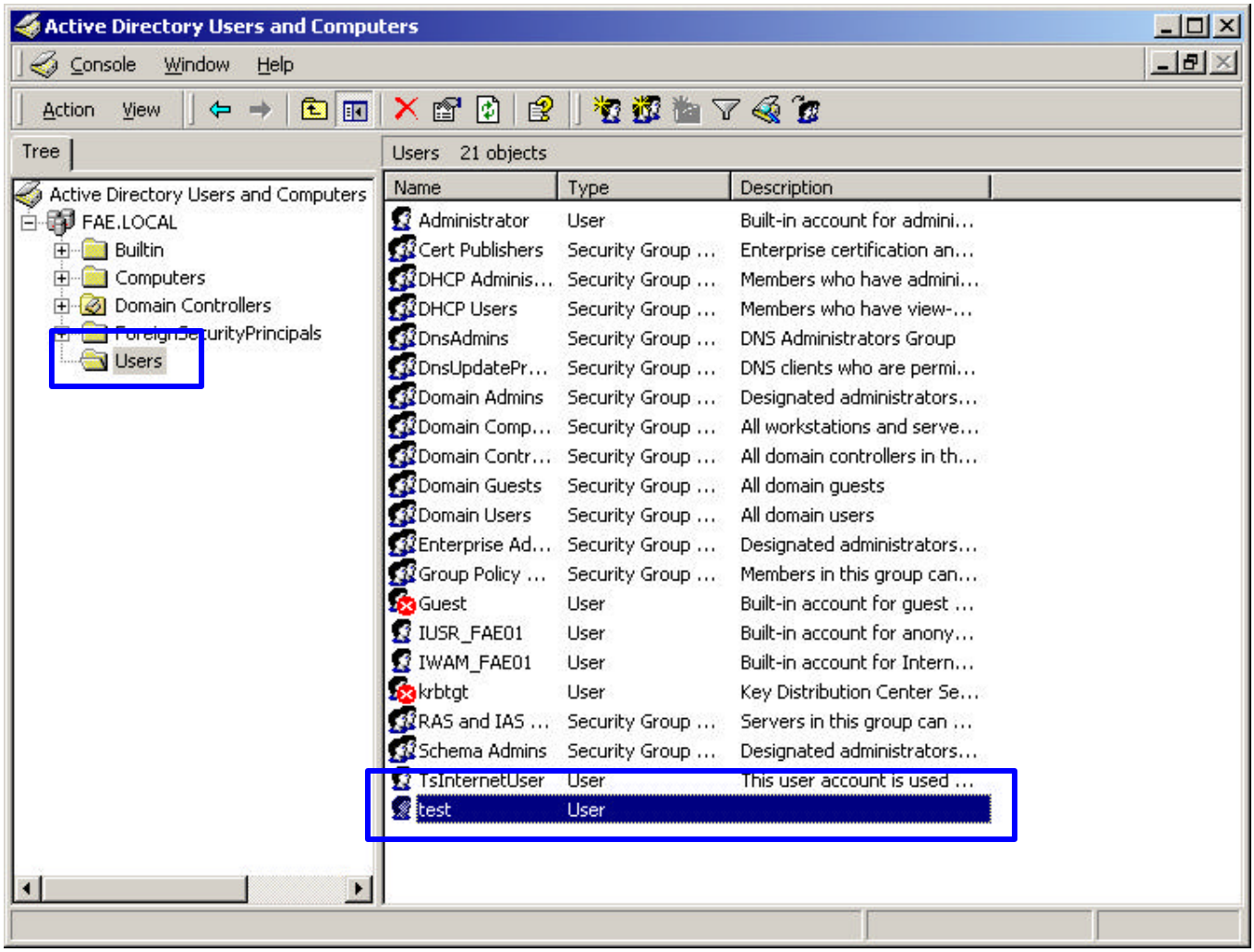


For TLS Authentication Setup (Steps 34 ~ 38)

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

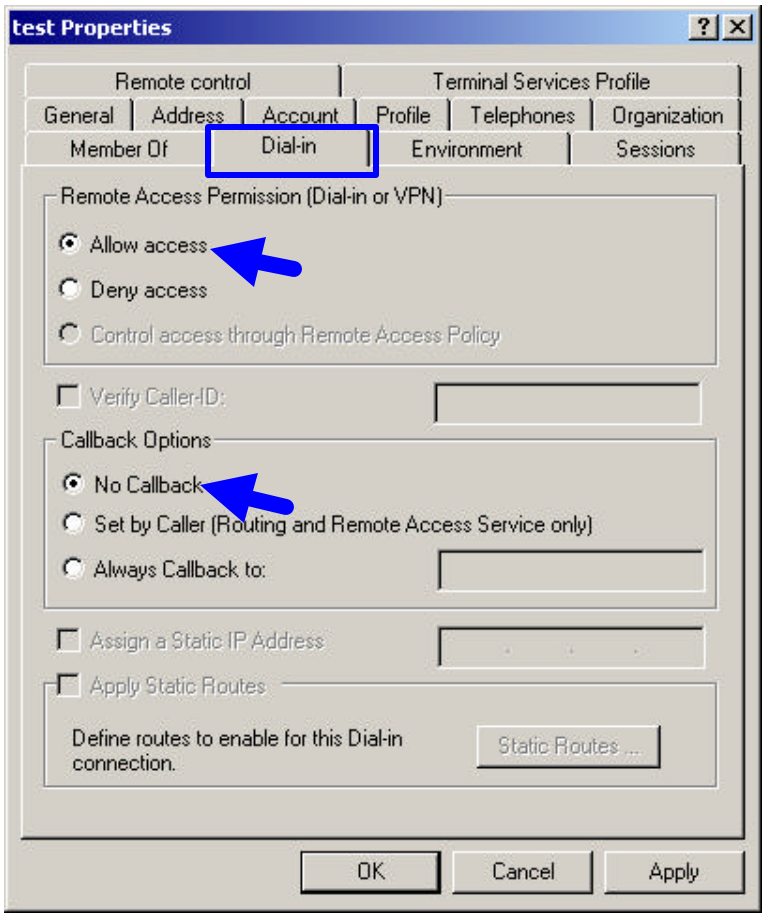


36. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**
37. Select "**Users** ", and double-click on the user that can be newly created or currently existing, who will be configured to have the right to obtain digital certificate remotely.



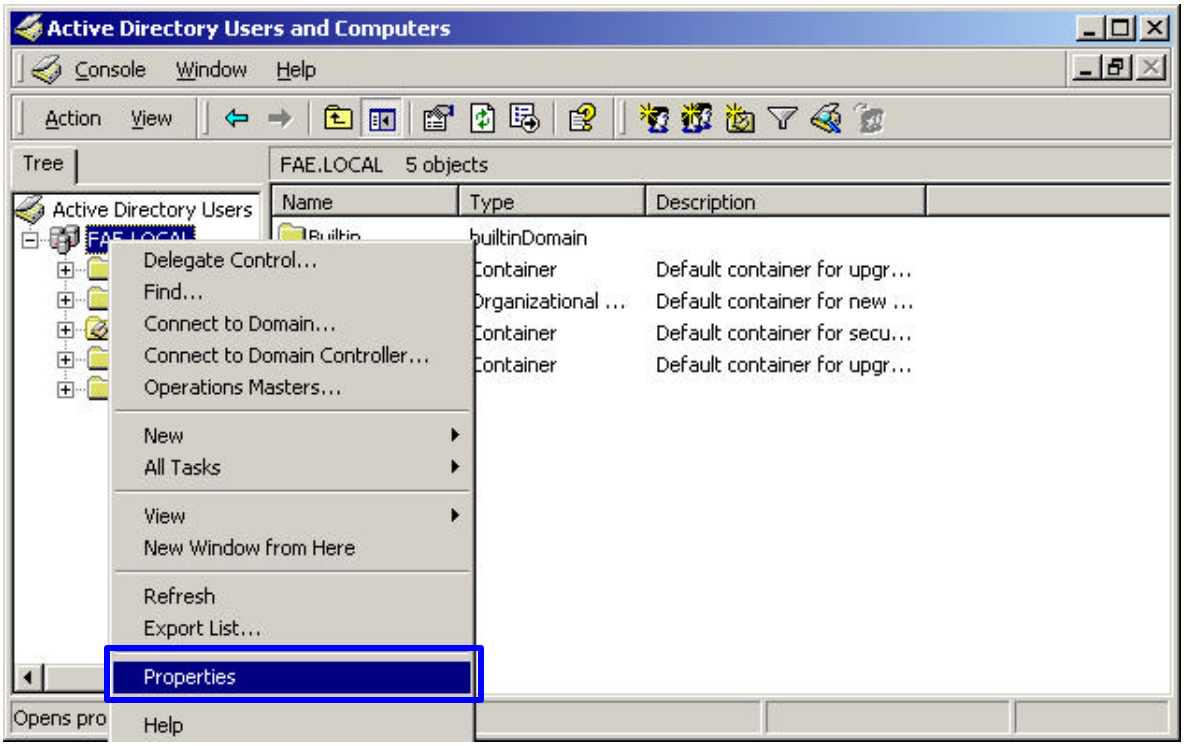
Please note that in this case, we have a user called, **test**, whose account/password are used to obtain the digital certificate from server.

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

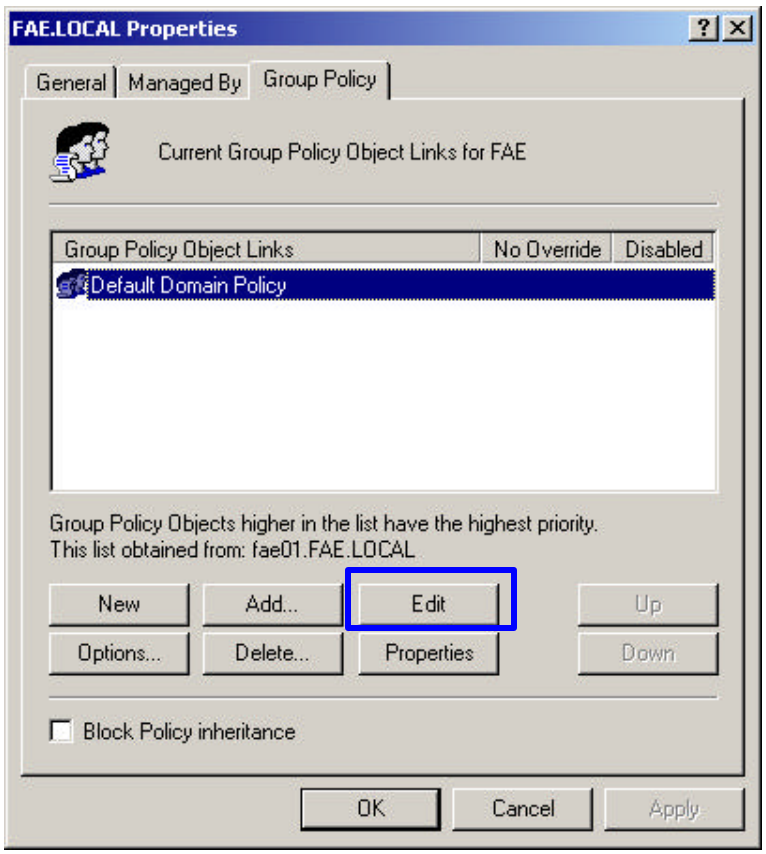


For MD5 Authentication (Steps 39 ~ 54)

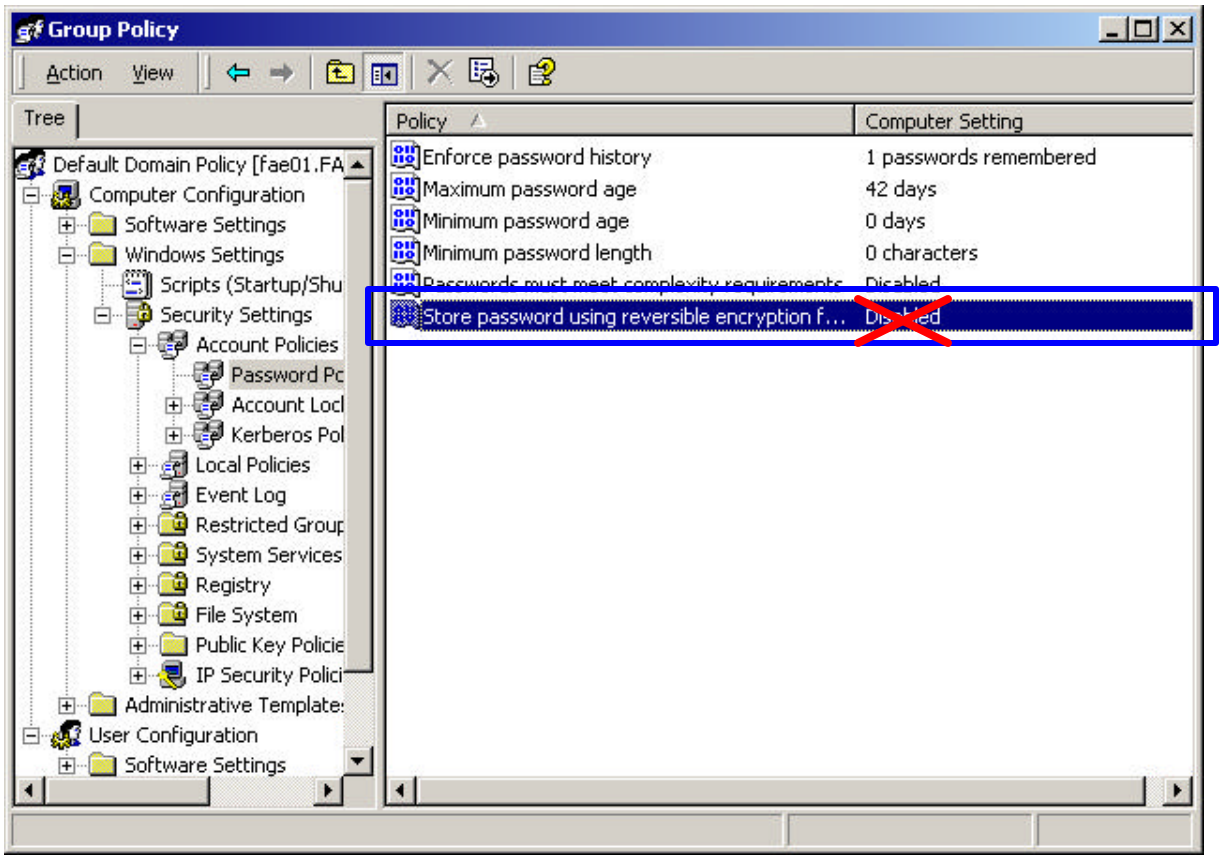
39. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers.**
40. Right click on the domain, and select "**Properties**"



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

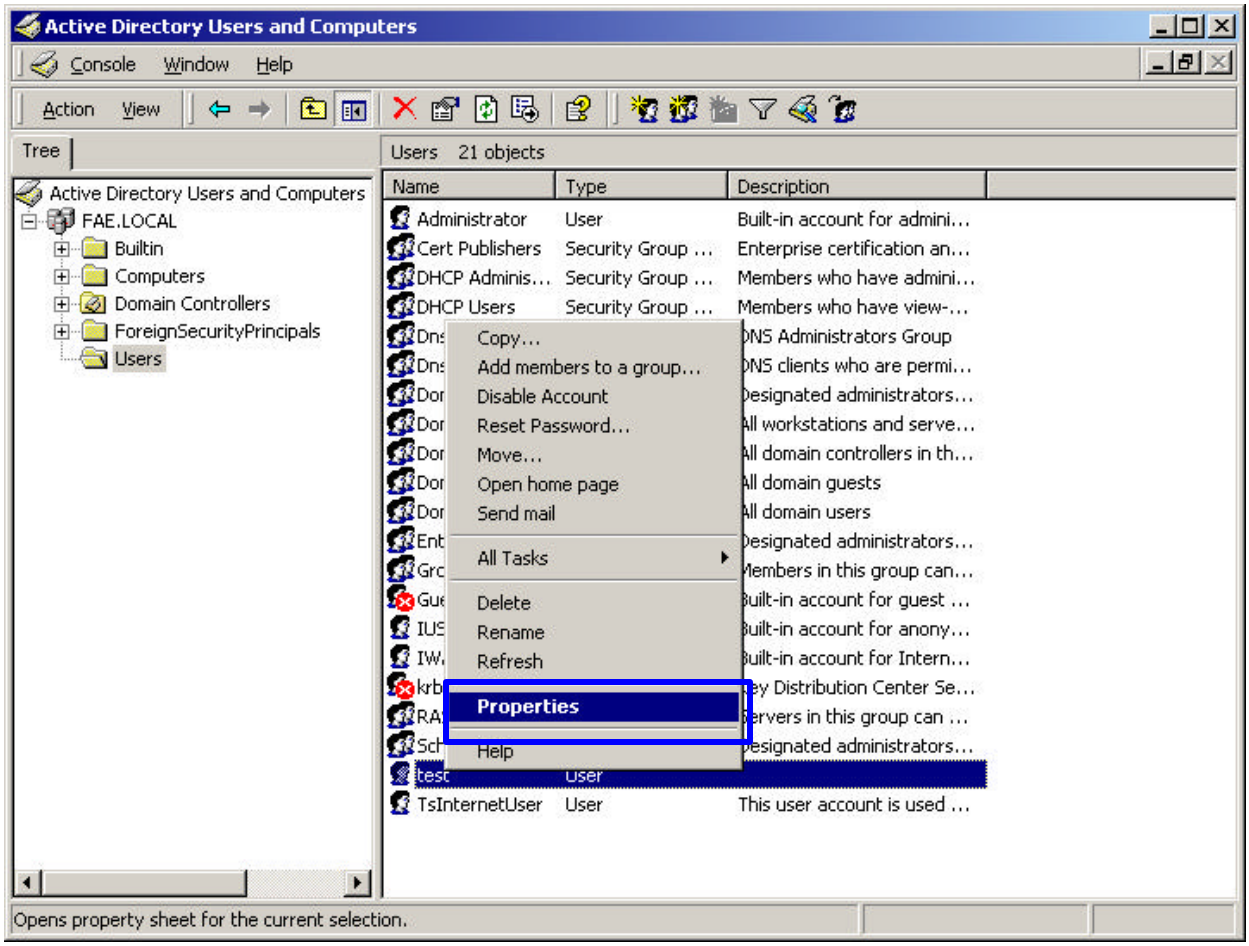


42. Go to “Computer Configuration” > “Windows Settings” > “Security Settings” > “Account Policies” > “**Password Policies**”

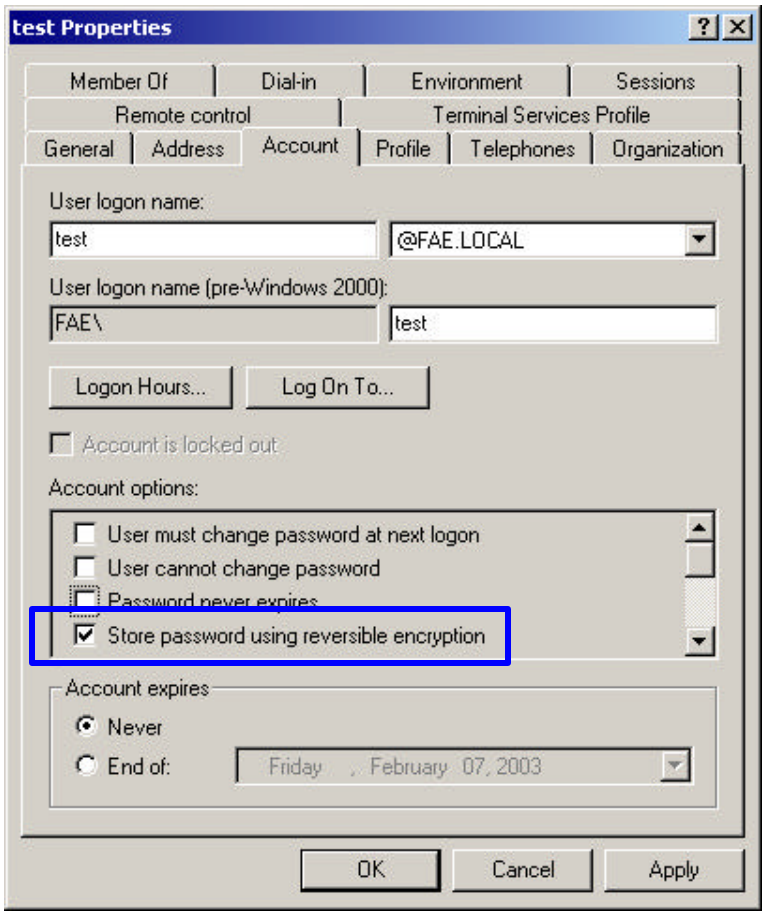


43. Click “**Define this policy setting**”, select “**Enabled**”, and click “**OK**” to continue.

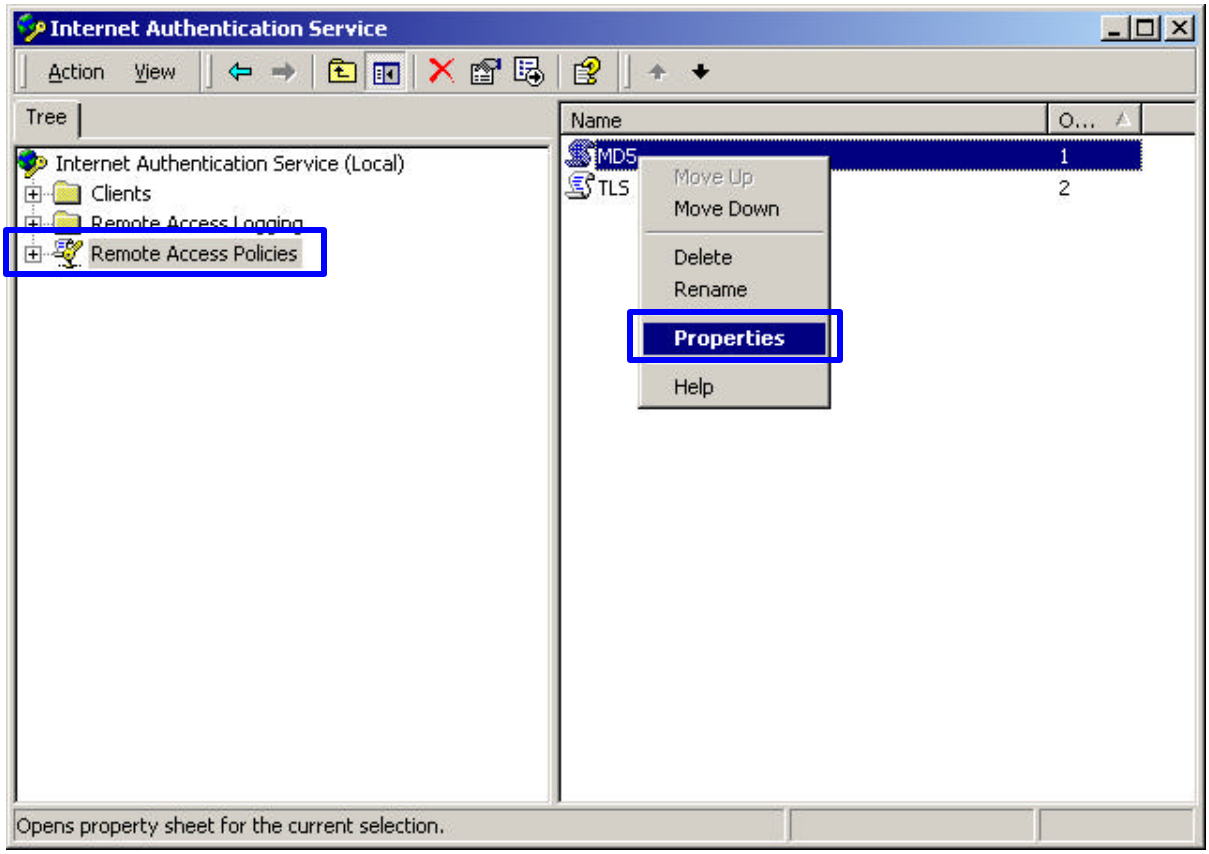
44. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.
45. Go to **Users**. Right-click on the user that you are granting access, and select "**Properties**"



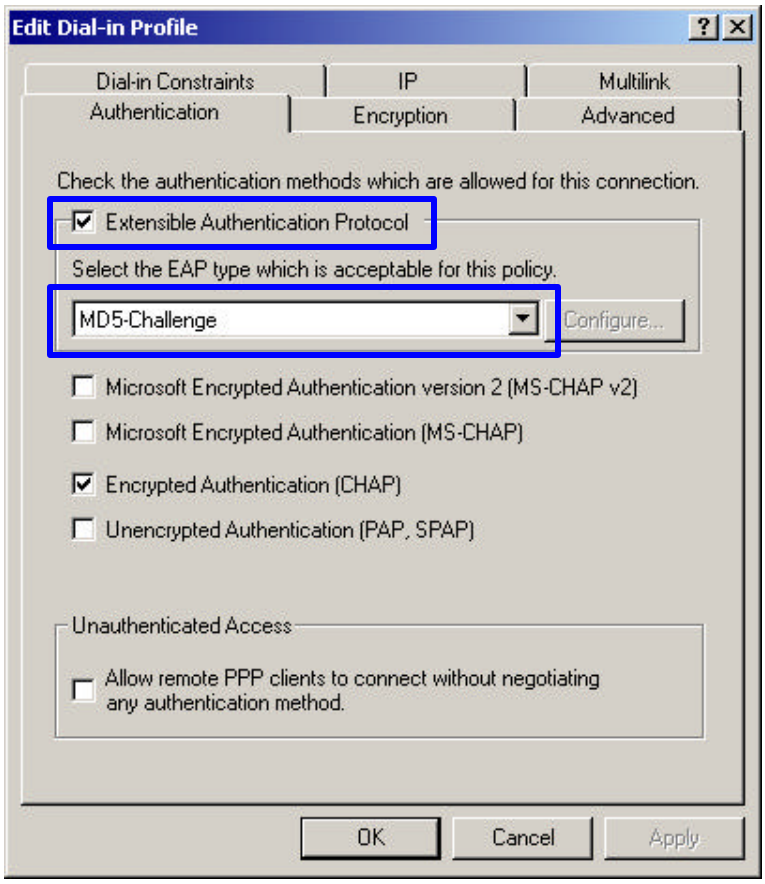
46. Go to "**Account**" tab, and enable "**Store password using reversible encryption**"
47. Click "**OK**" to continue.



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**"



52. Go to "**Authentication**" tab
53. Enable "**Extensible Authentication Protocol**"
54. Select "**MD5-Challenge**" for EAP type.



APPENDIX D: GLOSSARY

Access Point ? An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc ? An independent wireless LAN network formed by a group of computers, each with an network adapter.

AP Client – One of the additional AP operating modes offered by 22Mbps Access Point, which allows the Access Point to act as an Ethernet-to-Wireless Bridge, thus a LAN or a single computer station can join a wireless ESS network through it.

ASCII – American Standard Code for Information Interchange, ASCII, is one of the two formats that you can use for entering the values for WEP key. It represents English letters as numbers from 0 to 127.

Authentication Type ? Indication of an authentication algorithm which can be supported by the Access Point:

1. Open System : Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if 802.11 Authentication Type at the recipient station is set to Open System authentication.
2. Shared Key : Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key or a member of those who does not.

Backbone ? The core infrastructure of a network, which transports information from one central location to another where the information is unloaded into a local system.

Bandwidth ? The transmission capacity of a device, which is calculated by how much data the device can transmit in a fixed amount of time expressed in bits per second (bps).

Basic Rate ? the fixed transmitted and receiving data rate allowed by the AP with the value 1,2,5.5, 11 and 22 Mbps for selection.

Beacon ? A beacon is a packet broadcast by the Access Point to keep the network synchronized. Included in a beacon are information such as wireless LAN service area, the AP address, the Broadcast destination addresses, time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit ? A binary digit, which is either -0 or -1 for value, is the smallest unit for data.

Bridge ? An internetworking function that incorporates the lowest 2 layers of the OSI network protocol model.

Browser ? An application program that enables one to read the content and interact in the World Wide Web or Intranet.

BSS ? BSS stands for "Basic Service Set". It is an Access Point and all the LAN PCs that associated with it.

Channel? The bandwidth which wireless Radio operates is divided into several segments, which we call them "Channels". AP and the client stations that it associated work in one of the channels.

CSMA/CA ? In local area networking, this is the CSMA technique that combines slotted time-division multiplexing with carrier sense multiple access /collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD ? Carrier Sense Multiple Access/Collision Detection, which is a LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and wait a random amount of time before retrying.

DHCP ? Dynamic Host Configuration Protocol, which is a protocol that lets network administrator s manage and allocate Internet Protocol (IP) addresses in a network. Every computer has to have an IP address in order to communicate with each other in a TCP/IP based infrastructure network. Without DHCP, each computer must be entered in manually the IP address. DHCP enables the network administrators to assign the IP from a central location and each computer receives an IP address upon plugged with the Ethernet cable everywhere on the network.

DSSS ? Direct Sequence Spread Spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even

if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Dynamic IP Address ? An IP address that is assigned automatically to a client station in a TCP/IP network by a DHCP server.

Encryption ? A security method that uses a specific algorithm to alter the data transmitted, thus prevent others from knowing the information transmitted.

ESS ? ESS stands for "Extended Service Set". More than one BSS is configured to become Extended Service Set. LAN mobile users can roam between different BSSs in an ESS.

ESSID ? The unique identifier that identifies the ESS. In infrastructure association , the stations use the same ESSID as AP's to get connected.

Ethernet? A popular local area data communications network, originally developed by Xerox Corp., that accepts transmission from computers and terminals. Ethernet operates on a 10/100 Mbps base transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation ? When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.

Fragmentation Threshold – The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of "Fragmentation Threshold" is to increase the transfer reliability thru cutting a MAC Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission can not allow to transmit too big frame size due to the heavy interference caused by the big size of transmission frame. But if the frame size is too small, it will create the overhead during the transmission.

Gateway ? a device that interconnects networks with different, incompatible communication protocols.

HEX – Hexadecimal, HEX, consists of numbers from 0 – 9 and letters from A – F.

IEEE ? The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers, which is the largest technical professional society that promotes the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession. The IEEE fosters the development of standards that often become national and international standards.

Infrastructure ? An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point which connects them to the rest of the network.

ISM Band ? The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4GHz, in particular, is being made available worldwide.

MAC Address ? Media Access Control Address is a unique hex number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Multicasting ? Sending data to a group of nodes instead of a single destination.

Multiple Bridge – One of the additional AP operating modes offered by 22Mbps Access Point, which allows a group of APs that consists of two or more APs to connect two or more Ethernet networks or Ethernet enabled clients together. The way that multiple bridge setup is based on the topology of Ad-Hoc mode.

Node ? A network junction or connection point, typically a computer or workstation.

Packet ? A unit of data routed between an origin and a destination in a network.

PLCP ? Physical layer convergence protocol

PPDU ? PLCP protocol data unit

Preamble Type ? During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined as the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non-short-preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU ? PLCP service data unit

Roaming ? A LAN mobile user moves around an ESS and enjoys a continuous connection to an Infrastructure network.

RTS ? **R**equest **T**o **S**end. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

RTS Threshold ? Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. If the packet size

is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

SSID ? Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

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

TCP/IP ? Transmission Control Protocol/ Internet Protocol. The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network, i.e. intranet or internet. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

Throughput ? The amount of data transferred successfully from one point to another in a given period of time.

WEP ? Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication. To enable the icon will prevent other stations without the same WEP key from linking with the AP.

Wireless Bridge – One of the additional AP operating modes offered by 22mpbs Access Point, which allows a pair of APs to act as the bridge that connects two Ethernet networks or Ethernet enabled clients together.

APPENDIX E: TECHNICAL SPECIFICATION

Standard	802.11b compliant (wireless)
Data Rate	1 / 2 / 5.5 / 11 / 22 Mbps
Emission Type	Direct Sequence Spread Spectrum (DSSS)
Data Modulation	1 Mbps – BPSK
	2 Mbps – QPSK
	5.5 / 11 Mbps – CCK
	5.5 / 11 / 22 Mbps - PBCC
RF Frequency	2412 MHz – 2462 MHz (North America)
	2412 MHz – 2472 MHz (General Europe)
	2412 MHz – 2484 MHz (Japan)
Operating Channel	11 Channels (North America)
	13 Channels (Europe)
	14 Channels (Japan)
RF Output Power	16 ~ 18 dBm (typical)
Sensitivity	22Mpbs PBCC -80 dBm (Typically @25? ±5?)
	11Mbps PBCC - 85 dBm (Typically @25? ±5?)
	11Mbps CCK - 82 dBm (Typically @25? ±5?)
Security	Wired Equivalent Privacy (WEP) 64 / 128 / 256 bit
Antenna Type	Dipole with Antenna Gain of 2 dBi max.
Antenna Connector	Reverse SMA
Interface	PCI Standard v2.2
Dimension	133.0 x 121.0 x 22.1 mm
Memory	8Kbytes EEPROM
Power Voltage	5V ± 5%
Power Consumption	Operation max. 650 mA by TX
	350 mA by RX