LevelOne

WNC-0300

11g Wireless PCI Adapter

User's Manual

Version 2.0

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.

Contents

1. Introduction

1.1 Product Feature

- Compliance with IEEE 802.11g and 802.11b standards
- Highly efficient design mechanism to provide unbeatable performance
- Achieving data rate up to 54Mbps for 802.11g and 11Mps for 802.11b with wide range coverage; high performance to deliver up to 108Mbps raw data rate for 802.11g
- Strong network security with WEP and WPA support
- Auto-switch between the two standards, IEEE 802.11b and 802.11g
- Driver/Utility support most commonly used operating systems including Windows 98SE/ME/2000/XP.

1.2 System Requirement

- Windows 98SE, Millennium Edition (ME), 2000 and XP operating systems
- PC with Pentium III 600MHz system or above is recommended
- Equipped with at least one PCI slot
- One CD-ROM drive

2. Getting Start

2.1 LED Indicators

The Power LED will be ON when the unit is powered up.
The Link LED will be Blinking indicates a WLAN connection.

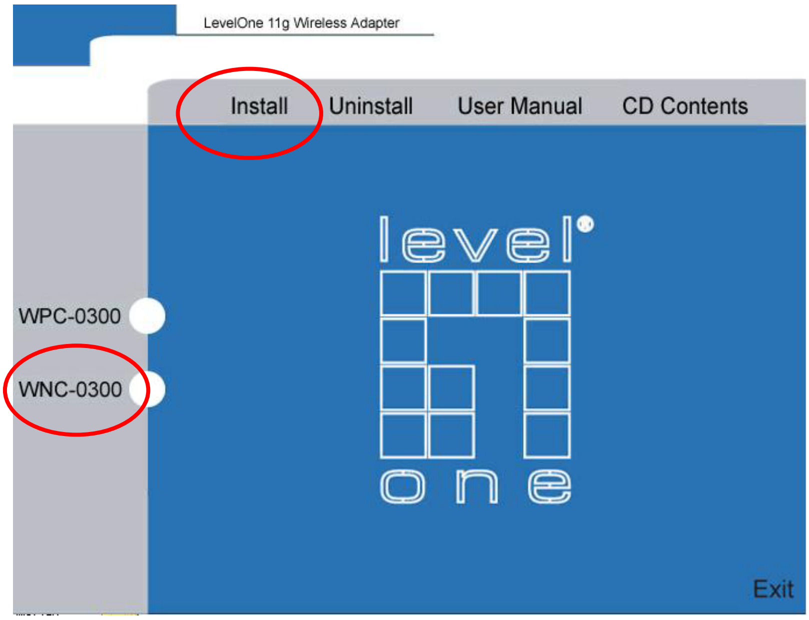
2.2 Install the WNC-0300 11g Wireless Network PCI Adapter

2.2.1 Utility Installation

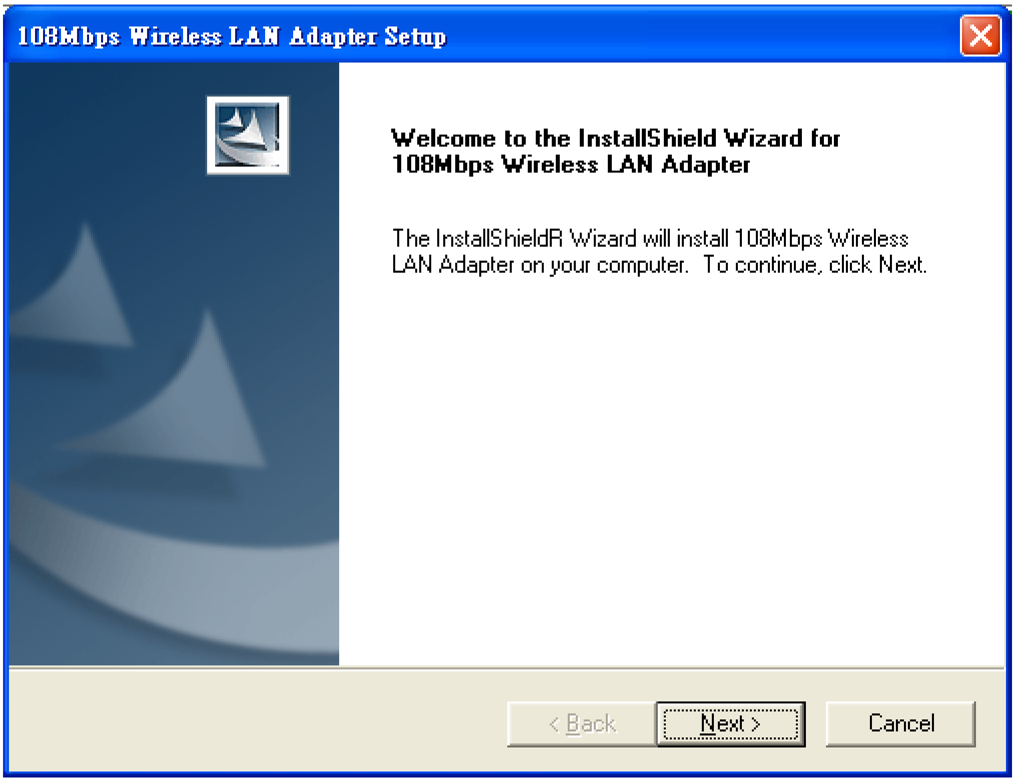
1. Before insert PCI Adapter into the PCI slot of your computer, please install the Utility Program first. Make sure that the LevelOne 11g wireless Network PCI Adapter is **NOT** inserted into the PCI slot.

   NOTE: all the snapped images of installation mentioned in this manual are based on Windows XP. For other windows operating system, all the procedures are the same but the screens are not the exactly same.

2. Turn on the computer. Insert the CD into the CD-ROM Drive. Please select "WNC-0300" and then click the "Install".

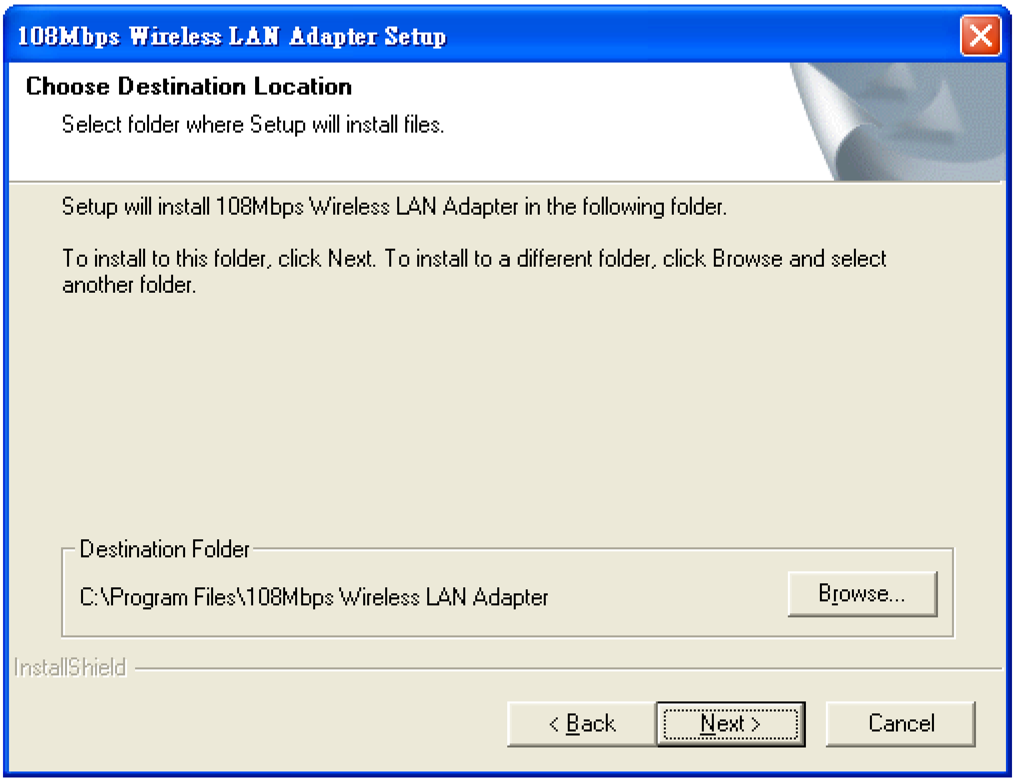


3. InstallShield Wizard will automatically start. Please click “Next” to continue.



Welcome to the InstallShield Wizard for 108Mbps Wireless LAN Adapter

The InstallShieldR Wizard will install 108Mbps Wireless LAN Adapter on your computer. To continue, click Next.



Choose Destination Location

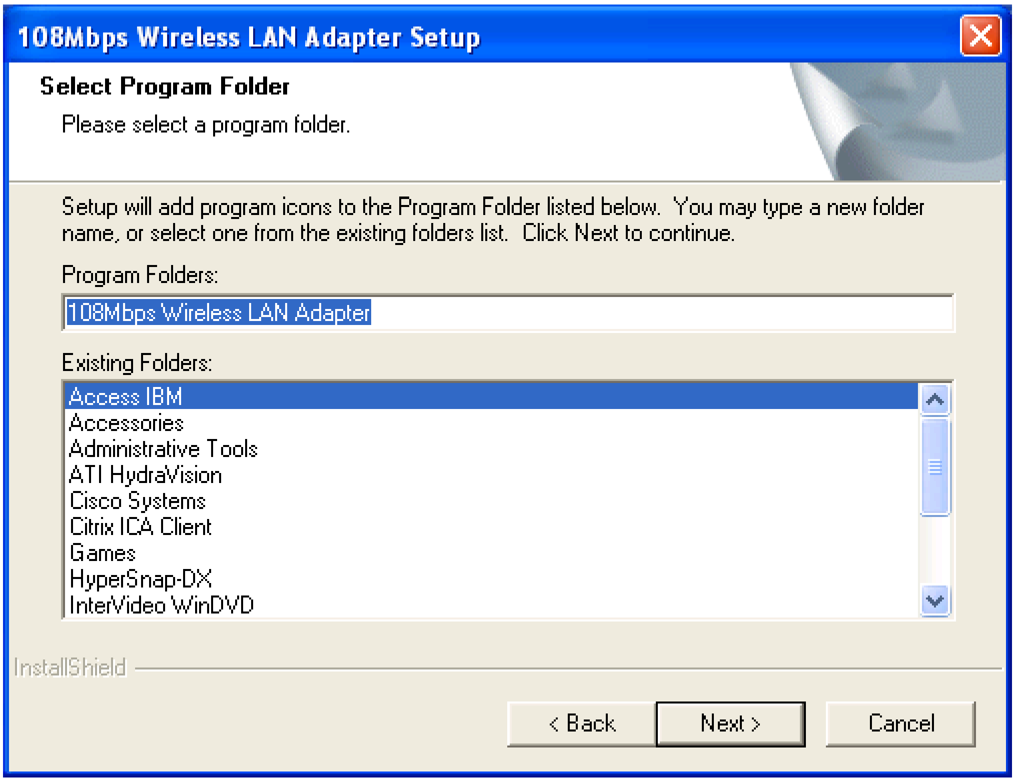
Select folder where Setup will install files.

Setup will install 108Mbps Wireless LAN Adapter in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\108Mbps Wireless LAN Adapter



Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

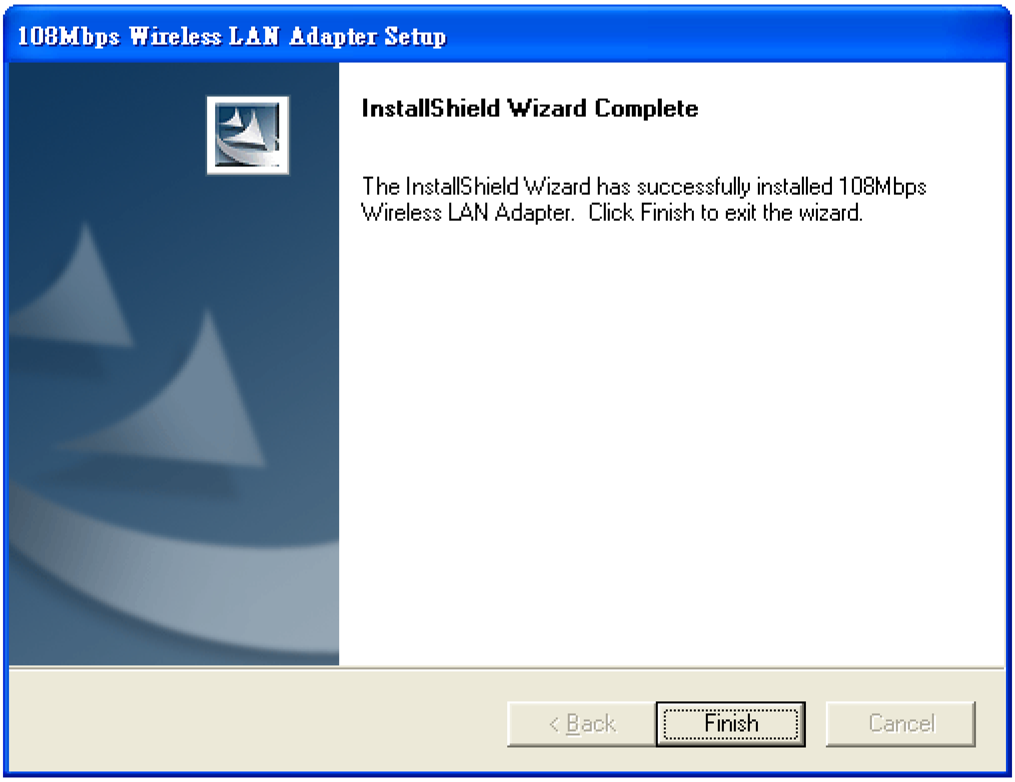
Program Folders:

108Mbps Wireless LAN Adapter

Existing Folders:

Access IBM
Accessories
Administrative Tools
ATI HydraVision
Cisco Systems
Citrix ICA Client
Games
HyperSnap-DX
InterVideo WinDVD

4. Please click “Finish”



108Mbps Wireless LAN Adapter Setup

InstallShield Wizard Complete

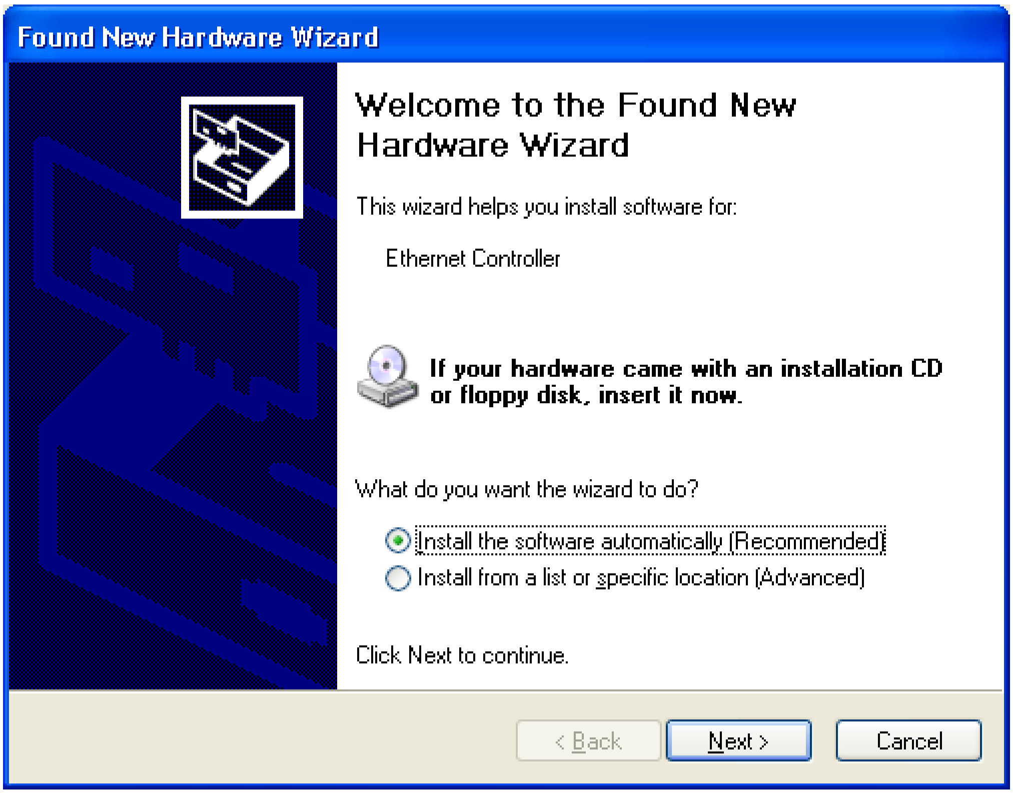
The InstallShield Wizard has successfully installed 108Mbps Wireless LAN Adapter. Click Finish to exit the wizard.

NOW.

1. Turn off your computer, and remove the power cord from your PC.
2. Open up the cover of your PC.
3. Remove the PCI slot cover from PC case.
4. Insert the 11g Wireless Network PCI Adapter into the empty PCI slot.
5. Place the computer case back on and plug the power cord.
6. Turn on your computer.
7. Continue with **Driver Installation**.

2.2.2 Driver Installation

1. Please select the first option and click “Next”.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

Ethernet Controller

If your hardware came with an installation CD or floppy disk, insert it now.

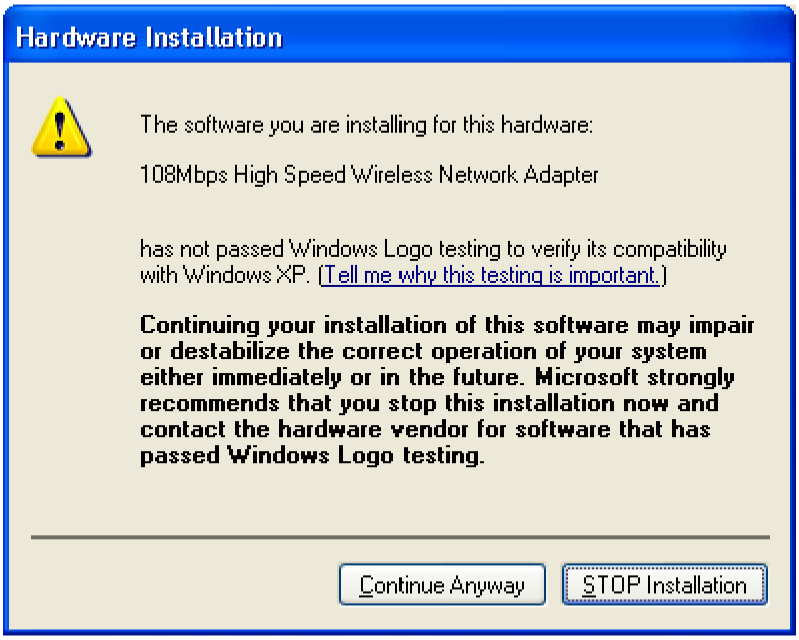
What do you want the wizard to do?

● Install the software automatically (Recommended)

○ Install from a list or specific location (Advanced)

Click Next to continue.

2. Please click “Continue Anyway”



Hardware Installation

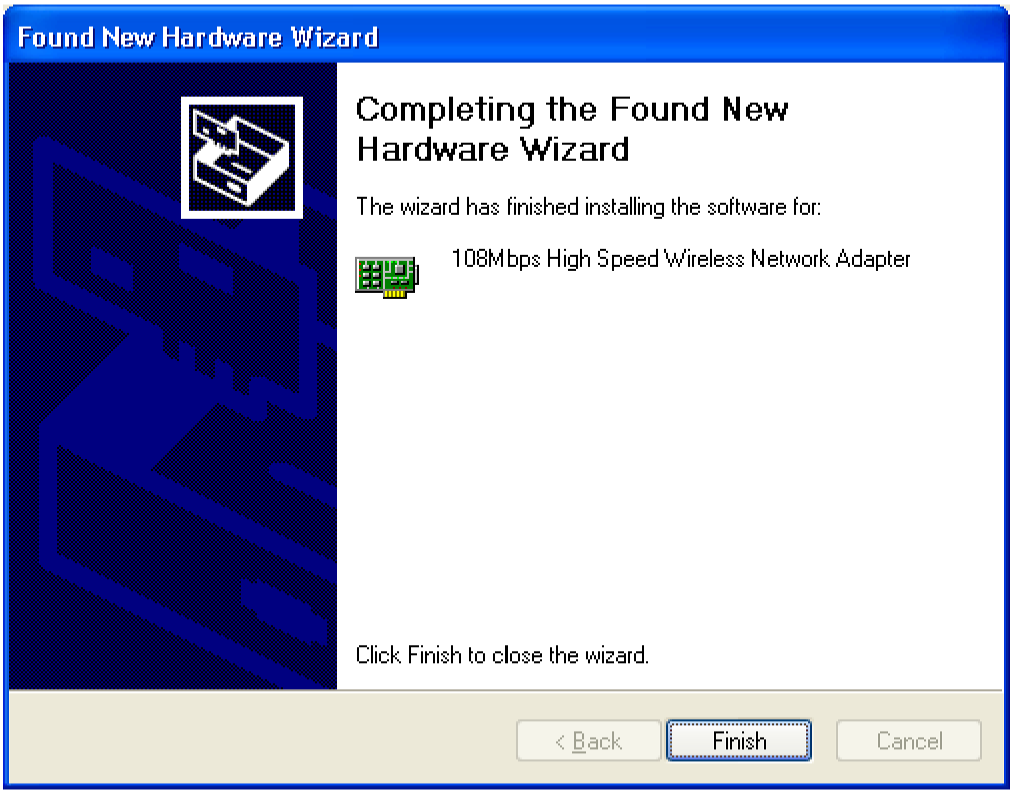
The software you are installing for this hardware:

108Mbps High Speed Wireless Network Adapter

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

3. Please click “Finish”



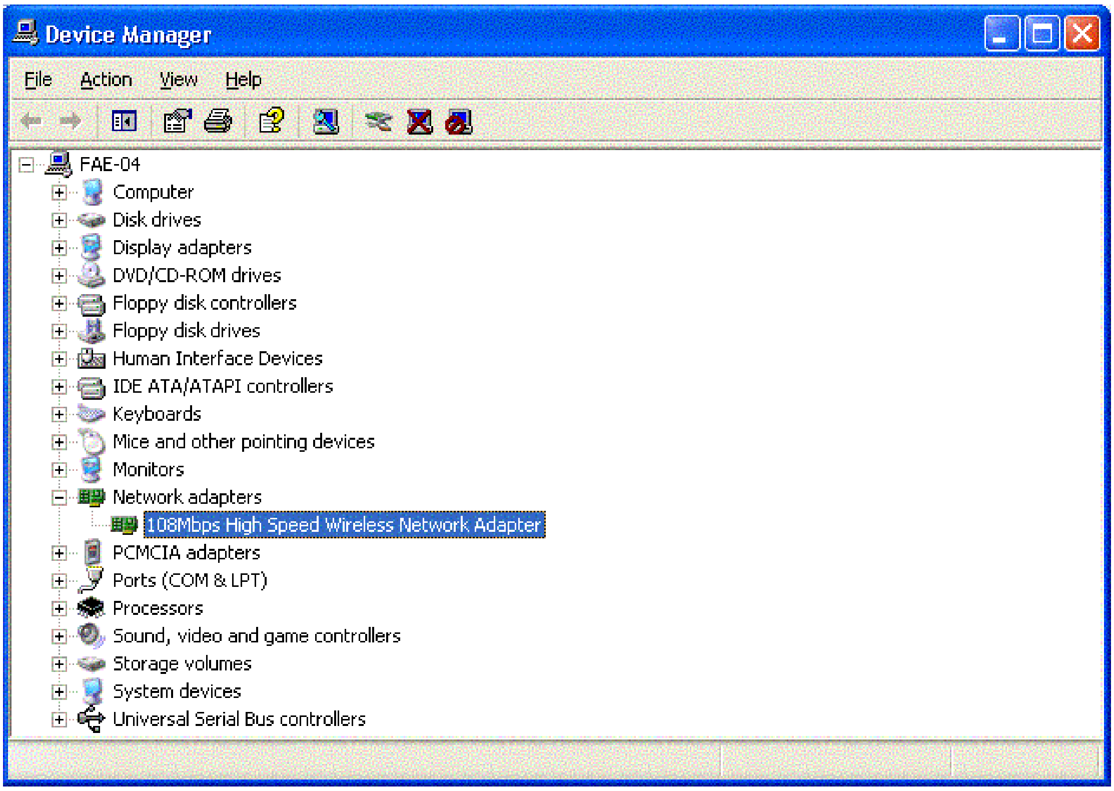
Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

108Mbps High Speed Wireless Network Adapter

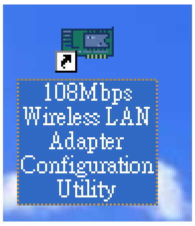
Click Finish to close the wizard.

4. To make sure if the installation is successful, you could check it through the device management.



```
FAE-04
  Computer
  Disk drives
  Display adapters
  DVD/CD-ROM drives
  Floppy disk controllers
  Floppy disk drives
  Human Interface Devices
  IDE ATA/ATAPI controllers
  Keyboards
  Mice and other pointing devices
  Monitors
  Network adapters
    108Mbps High Speed Wireless Network Adapter
  PCMCIA adapters
  Ports (COM & LPT)
  Processors
  Sound, video and game controllers
  Storage volumes
  System devices
  Universal Serial Bus controllers
```

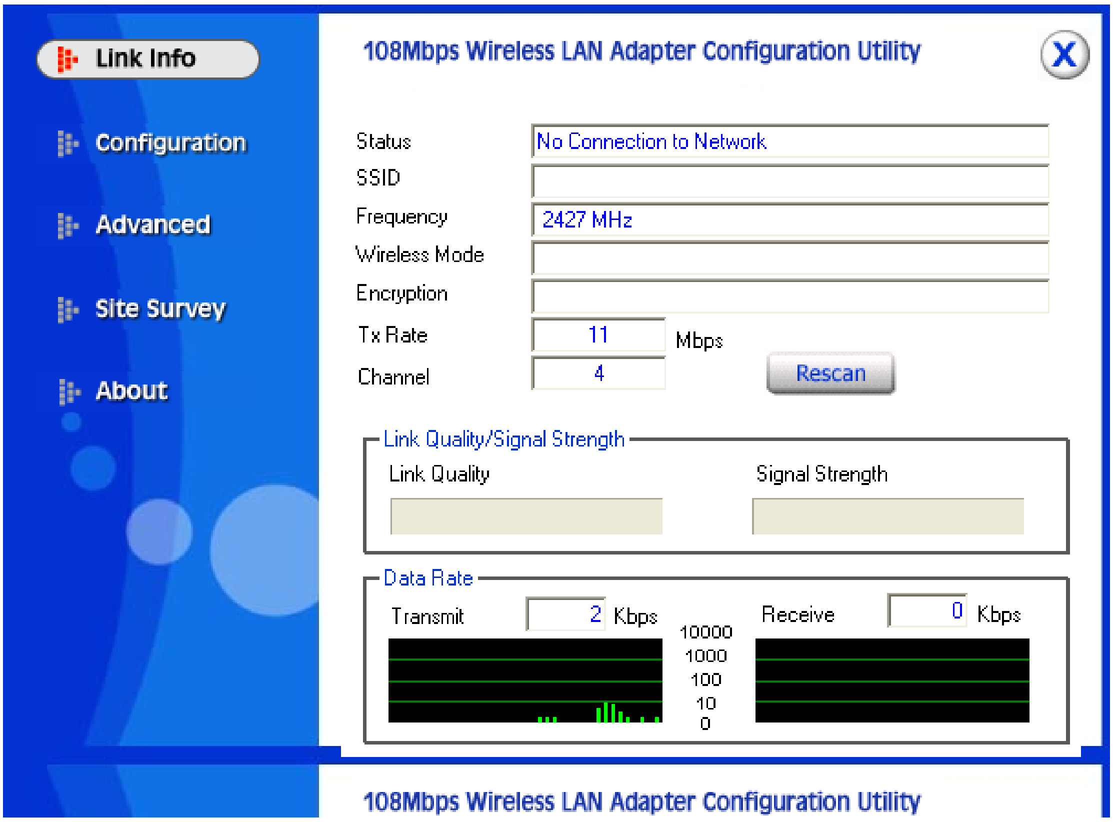
5. Once the installation is successful, a utility program icon will show on your desktop. To lunch the utility, just double click the icon.



3. Configuration

3.1 Link Information

The default page is as below after you launch the Utility program.



108Mbps Wireless LAN Adapter Configuration Utility

Status: No Connection to Network
SSID:
Frequency: 2427 MHz
Wireless Mode:
Encryption:
Tx Rate: 11 Mbps
Channel: 4

Link Quality/Signal Strength
Link Quality
Signal Strength

Data Rate
Transmit 2 Kbps
Receive 0 Kbps
10000
1000
100
10
0

108Mbps Wireless LAN Adapter Configuration Utility

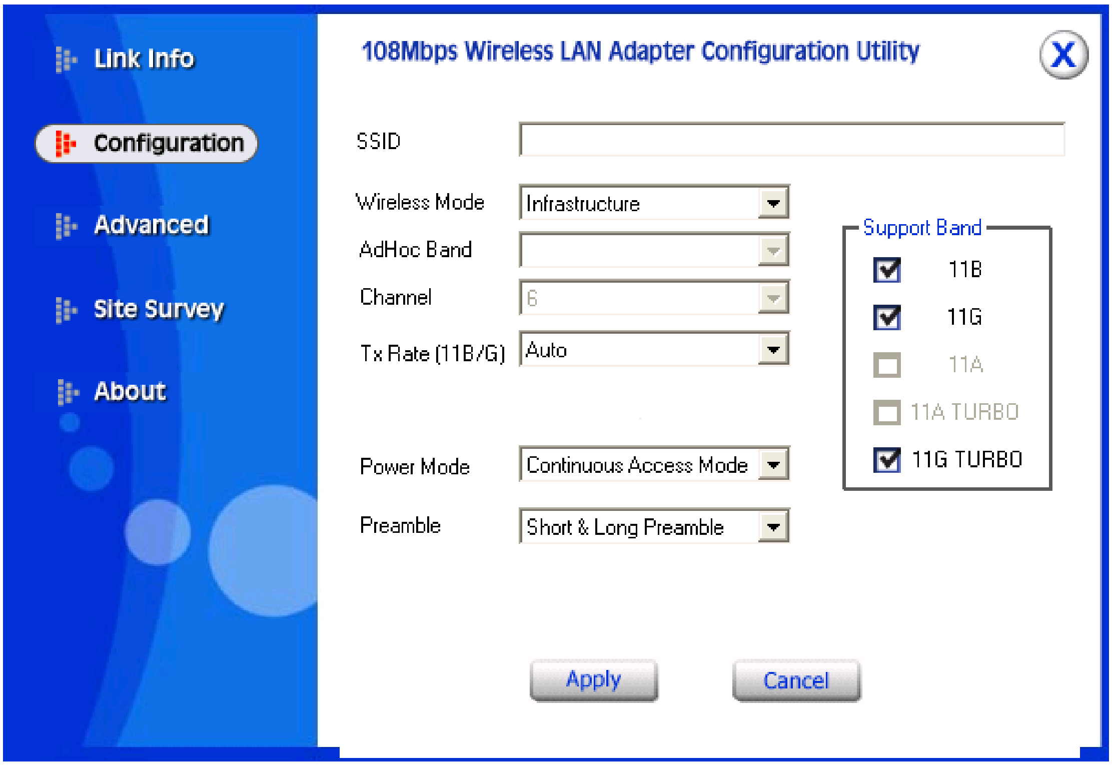
Status: Shows the BSSID associated, which can be used to identify the wireless network.

SSID: Shows current SSID, which must be the same for the wireless client and AP in order for communication to be established.

Frequency: Shows the current frequency used for wireless network.
Wireless Mode: Shows the current wireless mode used for wireless communication.
Encryption: Shows the current encryption mode used for wireless network.
TxRate: Shows the current data rate used for transmitting.
Channel: Shows the current channel for communication.
Link Quality: Shows the link quality of the 108Mbps wireless LAN PCI Adapter with the Access Point when operating under Infrastructure mode.
Signal Strength: Shows the wireless signal strength of the connection between the 11g wireless 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.

3.2 Configuration

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



108Mbps Wireless LAN Adapter Configuration Utility

SSID	
Wireless Mode	Infrastructure
AdHoc Band	
Channel	6
Tx Rate (11B/G)	Auto
Power Mode	Continuous Access Mode
Preamble	Short & Long Preamble

Support Band
☑ 11B
☑ 11G
□ 11A
□ 11A TURBO
☑ 11G TURBO

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.

Wireless Mode: 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.

AdHoc Band: There are two bands available for selection- 11B and 11G

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 and 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain.

Tx Rate: Select the data rate for data transmission.

Power Mode: There are 3 modes to choose.

●Continuous Access Mode (default) – the PCIsAconstantly operating with full power and it consum es the most power.

●Maximum Power Save – the device consumes the least power and only operates when there is wireless network activity.

●Power Save – the device consumes the moderate level of power.

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.

Click "**Apply**" for the changes to take effect. And then the screen will return to **Link Info.** Page.

Support Band:

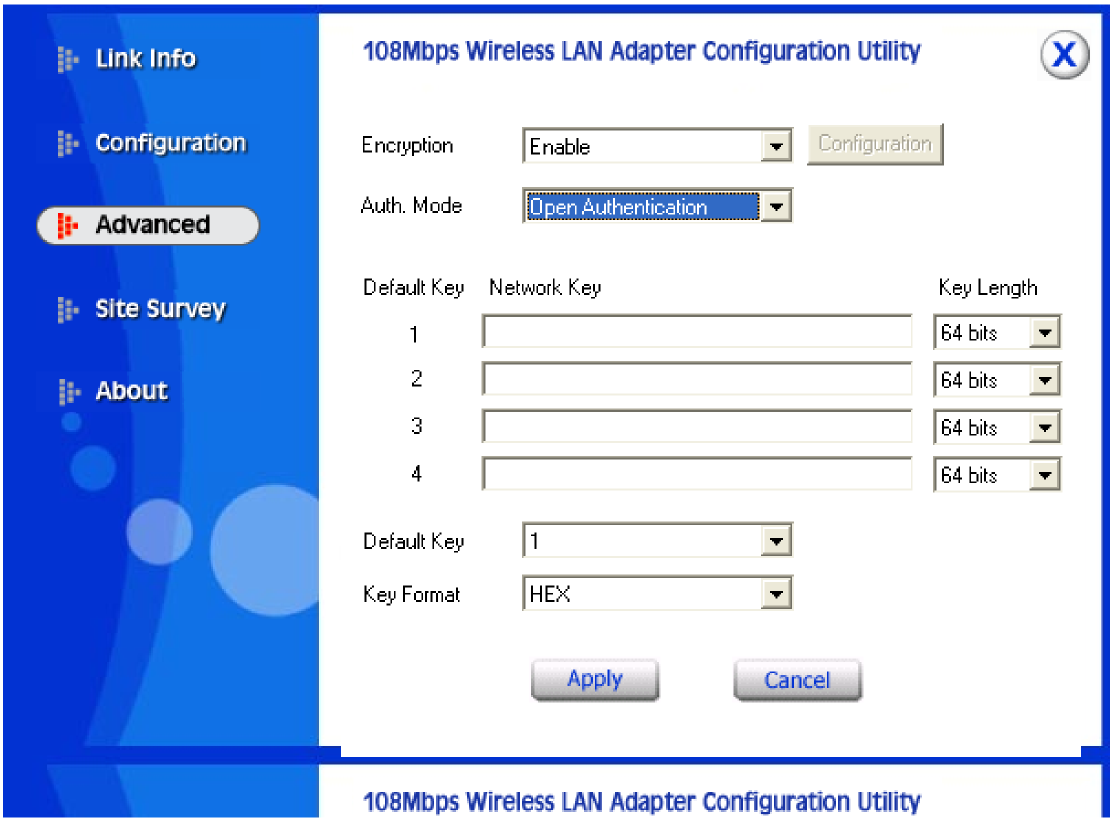
●11B – IEEE802.11b only

●11G – IEEE802.11g only

●11G Turbo – Super G mode support

3.3 Advanced

This is the page where you configure Security settings of your 108Mbps wireless LAN PCI Adapter


Link Info
Configuration
Advanced
Site Survey
About
108Mbps Wireless LAN Adapter Configuration Utility
X
Configuration
Apply
Cancel
108Mbps Wireless LAN Adapter Configuration Utility

Encryption: Enable

Auth. Mode: Open Authentication

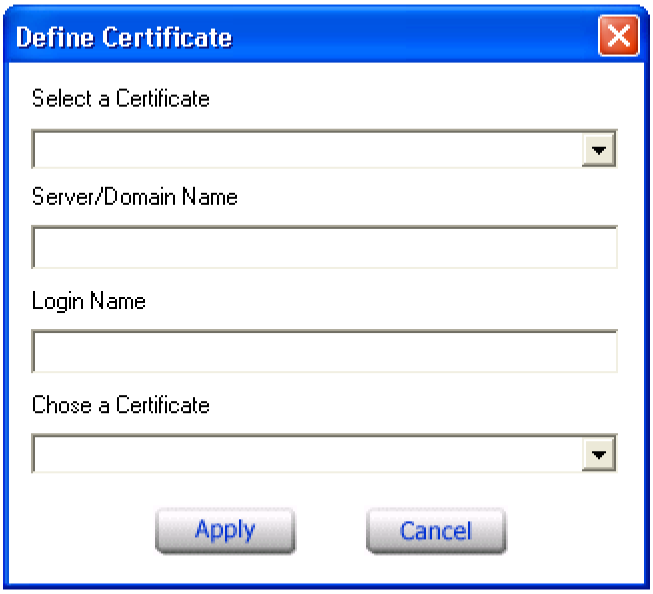
Default Key	Network Key	Key Length
1		64 bits
2		64 bits
3		64 bits
4		64 bits

Default Key: 1

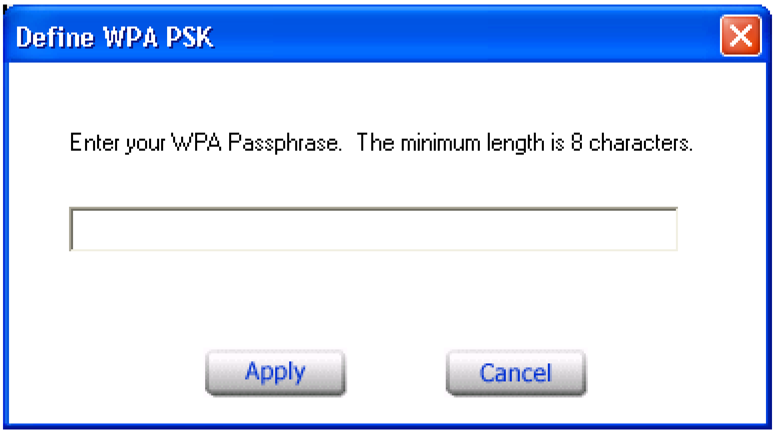
Key Format: HEX

Encryption: 4 options are available: **Disable**, **Enable**, **WPA** and **WPA-PSK**. Select **Enable** or **Disable** for WEP data encryption feature. If one of the two options is selected, it is required to select the **Authentication mode** from the next dropping list.

If **WPA** is selected, configuration is enabled. Please click the configuration. The below window is pop up. Then, please select the certificate that you like to use and enter the server name and login name



If WPA-PSK is selected, click the configuration button. The popping window is as the below. Please enter the key.(the character length is 8)



Enter your WPA Passphrase. The minimum length is 8 characters.

Auth. Mode: There are three modes available to choose.

- **Open Authentication** – the sender and receiver do not share secret Key for communication. Instead, each party generates its own key-pairs and asks 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 **Encryption** is enabled.

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

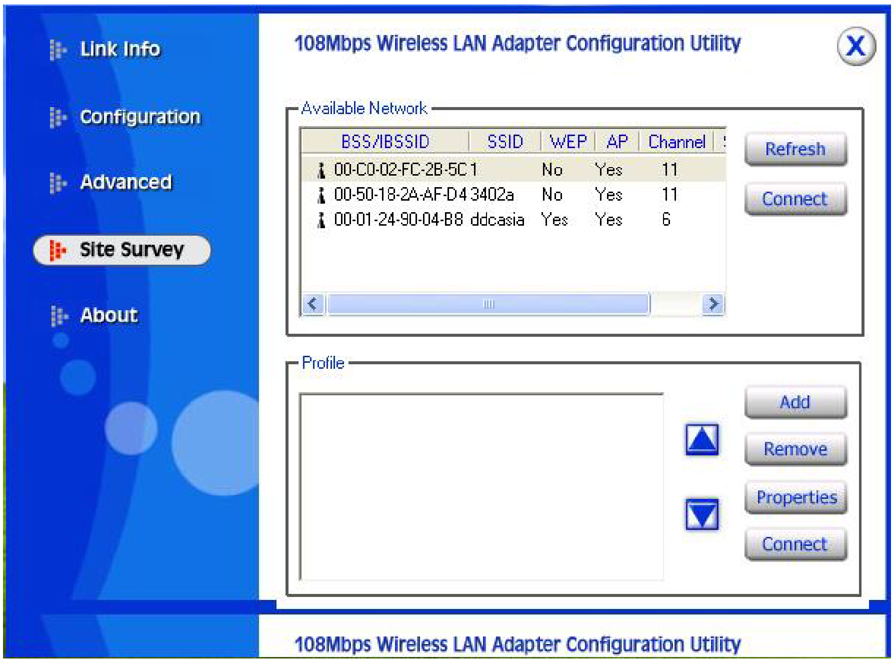
Network Key: enter values to these fields, either in HEX or ASCII formats. You only have to enter the key that you will use

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

Key Format: ASCII or **HEX**

3.4 Site Survey

This page allows you to enable the Site Survey function to scan for the available wireless network (wireless clients and Access Points) and establish wireless communications with one.



BSS/IBSSID	SSID	WEP	AP	Channel
00-C0-02-FC-2B-5C	1	No	Yes	11
00-50-18-2A-AF-D4	3402a	No	Yes	11
00-01-24-90-04-B8	ddcasia	Yes	Yes	6

Available Network – displays the wireless networks (wireless clients and Access Points) that are in your signal range.

Select any one of them to establish communications by simply mouse **double-click** or click on the "**Connect**" button.

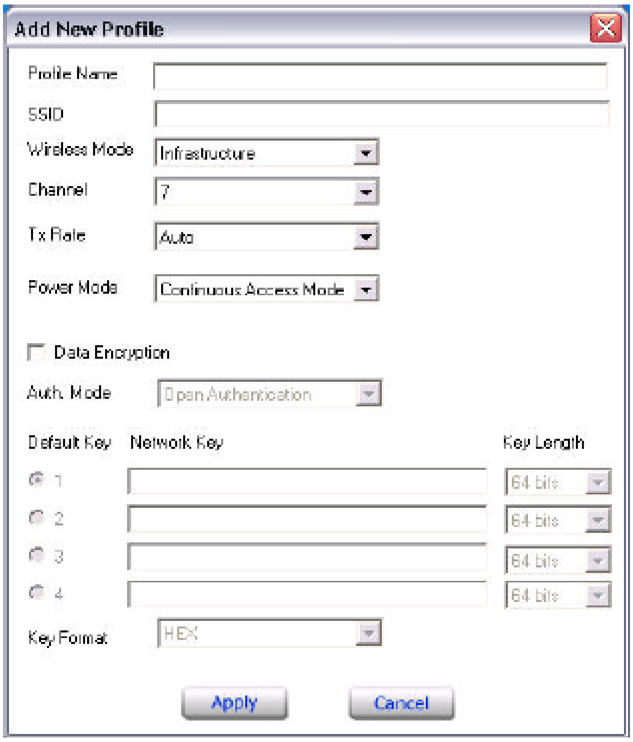
Click "**Refresh**" button to start scanning for available network again.

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.

Remove: To remove the selected the profile

Properties: To view and change its settings of the profile.

Add: To add a profile. Then, the following screen would appear.



Add New Profile

Profile Name

SSID

Wireless Mode: Infrastructure

Channel: 7

Tx Rate: Auto

Power Mode: Continuous Access Mode

□ Data Encryption

Auth. Mode: Open Authentication

Default Key	Network Key	Key Length
● 1		64 bits
○ 2		64 bits
○ 3		64 bits
○ 4		64 bits

Key Format: HEX

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.

Wireless Mode: 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 and 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain

Tx Rate: Select the data rate for data transmission.

Power Mode: There are 3 modes to choose.

●Continuous Access Mode (default) – the device is constantly operating with full power and it consumes the most power.

●Maximum Power Save – the device consumes the least power and only operates when there is wireless network activity.

●Power Save – the device consumes the moderate level of power

●Data Encryption –for WEP data encryption feature. If one of the two options is selected, it is required to select the **Authentication mode** from the next dropping list.

Auth. Mode: There are three modes available to choose.

- **Open Authentication** – the sender and receiver do not share secret Key for communication. Instead, each party generates its own key-pairs and asks 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 **Encryption** is enabled.

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

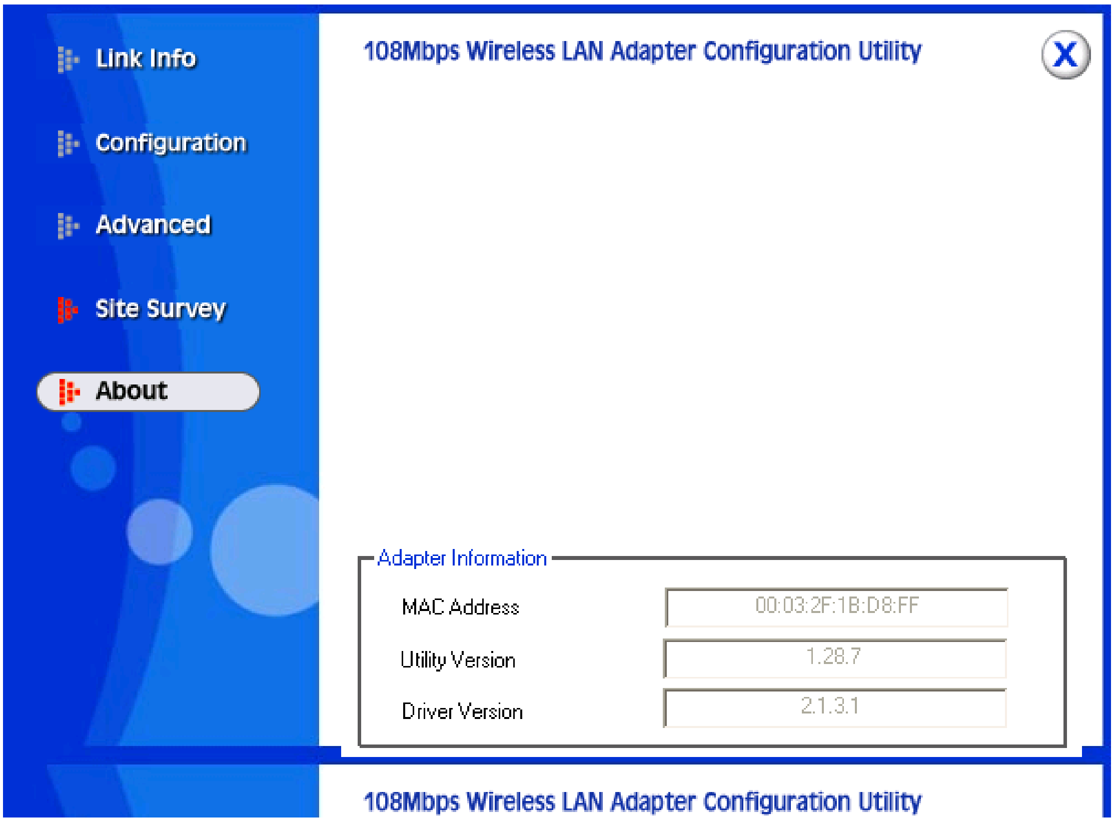
Network Key: enter values to these fields, either in HEX or ASCII formats. You only have to enter the key that you will use

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

Key Format: ASCII or **HEX**

3.5 About US

This page displays some information about the 108Mpbs wireless LAN 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.



Link Info
Configuration
Advanced
Site Survey
About
108Mbps Wireless LAN Adapter Configuration Utility
X

Adapter Information

MAC Address 00:03:2F:1B:D8:FF

Utility Version 1.28.7

Driver Version 2.1.3.1

108Mbps Wireless LAN Adapter Configuration Utility

4. 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 a network adapter.

AP Client: One of the additional AP operating modes offered by 108Mbps 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).

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 administrators 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 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 setups 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: Request **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 54mpbs Access Point, which allows a pair of APs to act as the bridge that connects two Ethernet networks or Ethernet enabled clients together.

WNC-0300

Appendix

APPENDIX A: NETWORKING BASIS

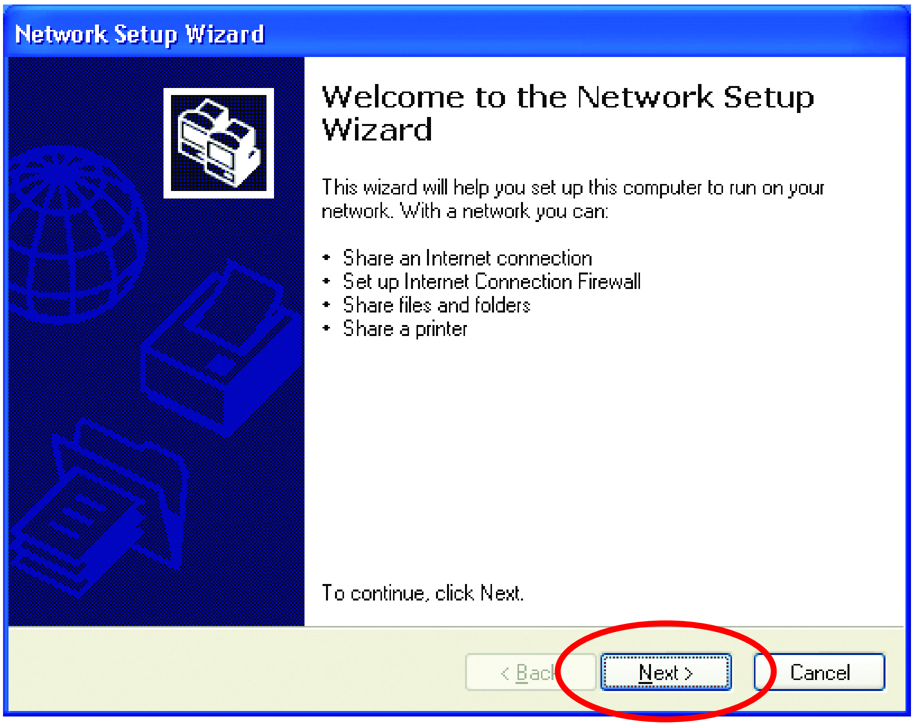
This chapter will help you learn the basics of home networking.

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

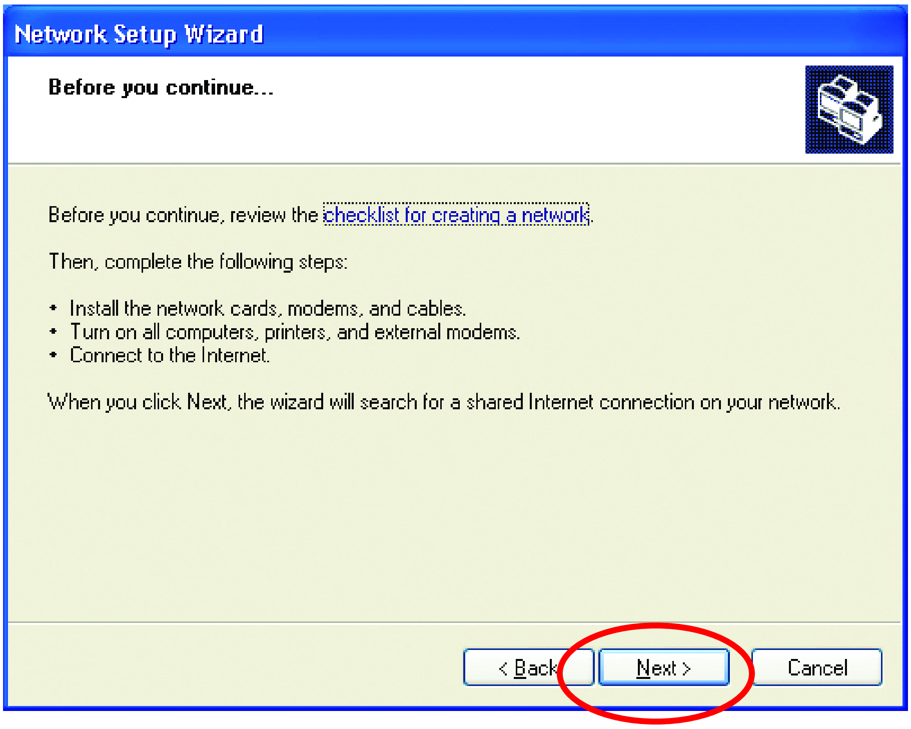
Welcome to the Network Setup Wizard

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:

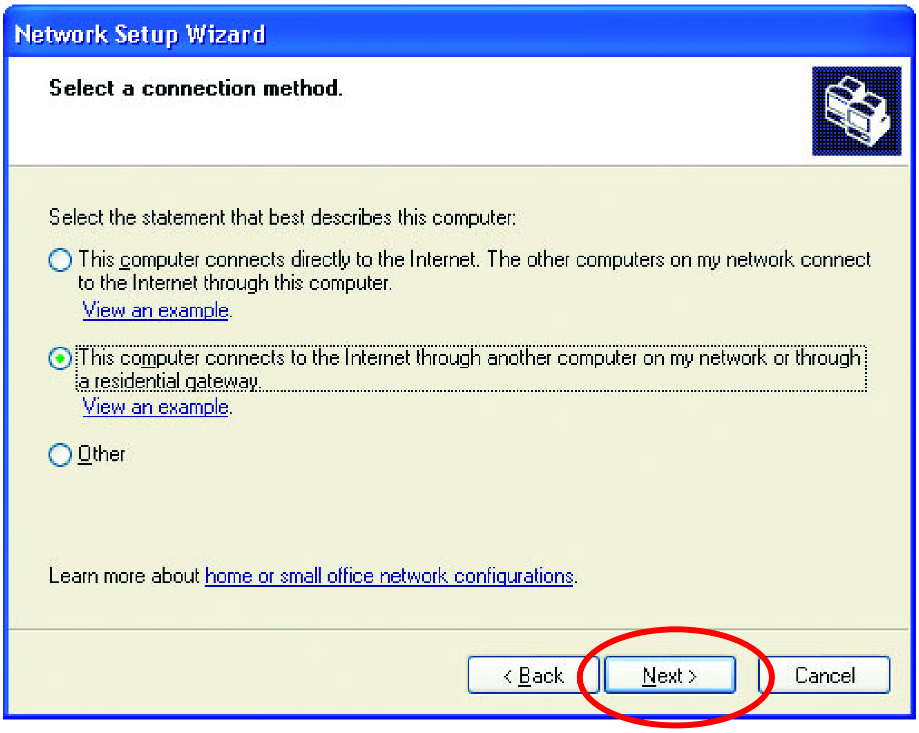
- Install the network cards, modems, and cables.
- Turn on all computers, printers, and external modems.
- Connect to the Internet.

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:

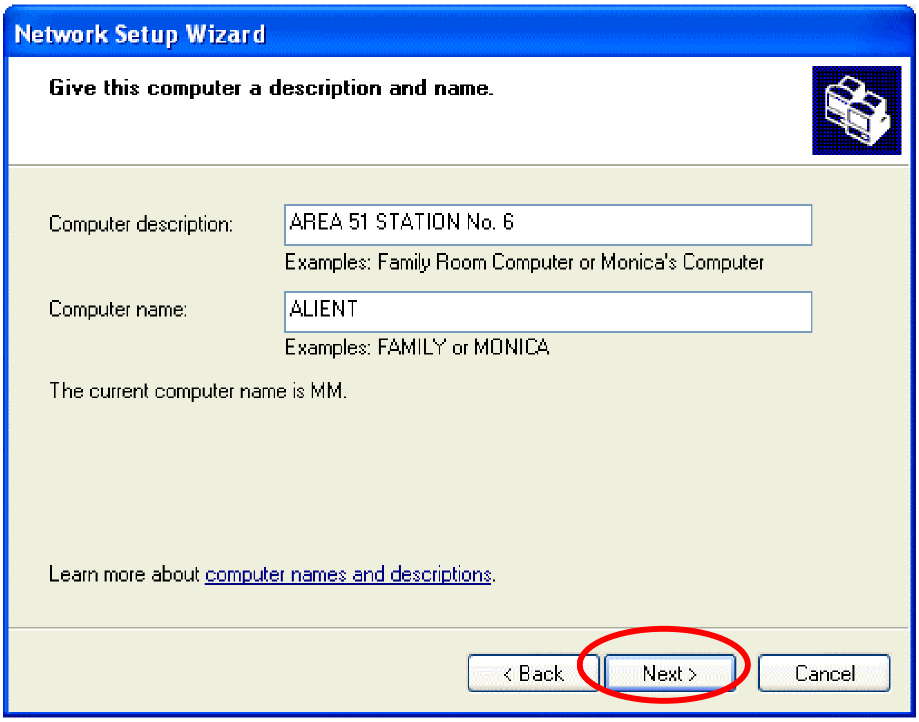
○ This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.

● 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

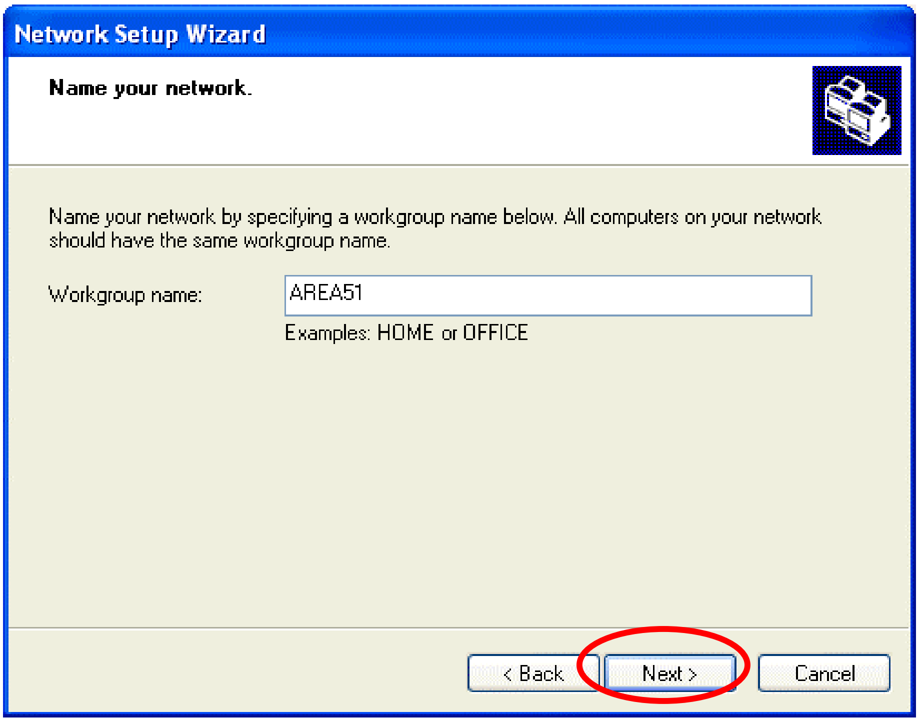
Computer name: ALIENT

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

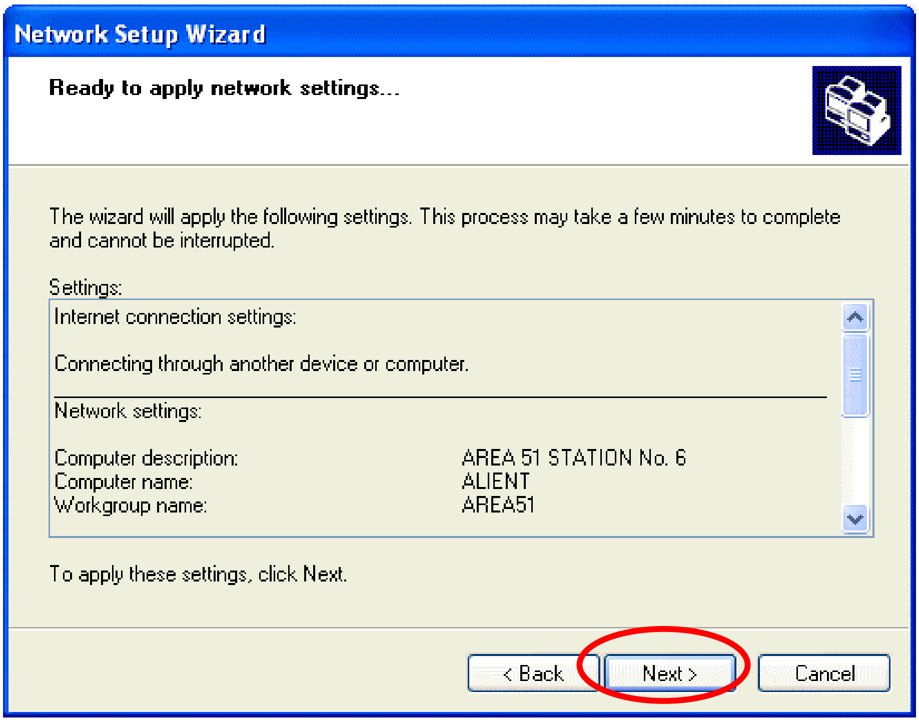
Name your network.

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:

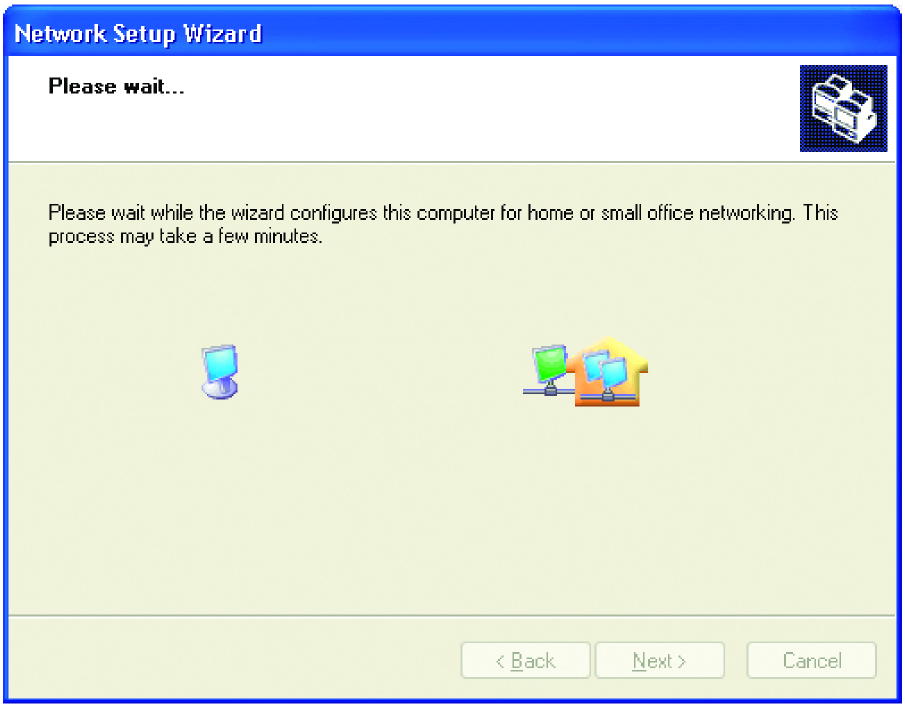
Internet connection settings:

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

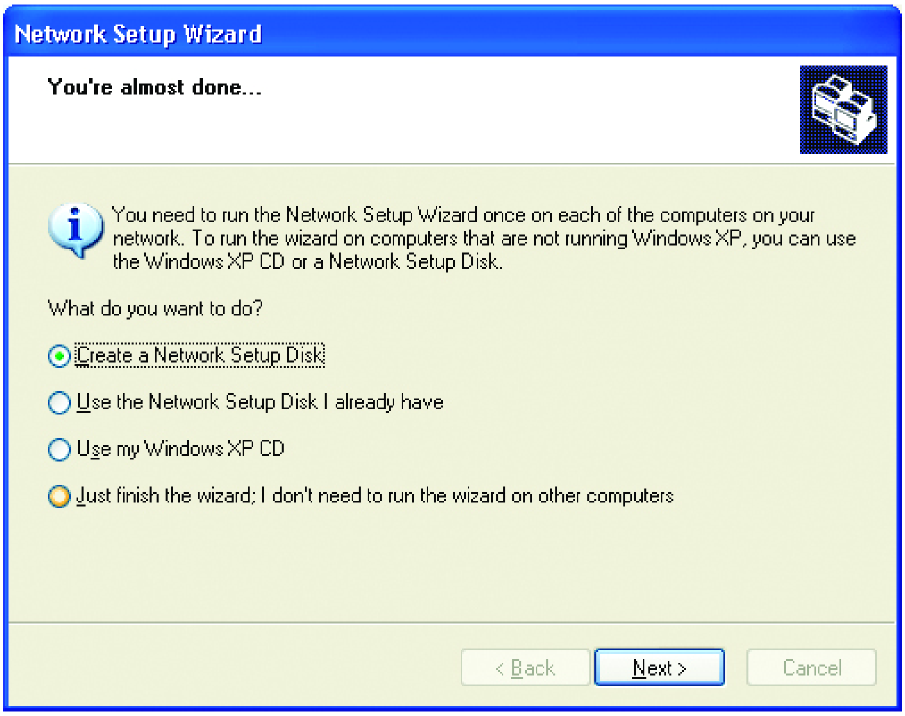
Please wait...

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...

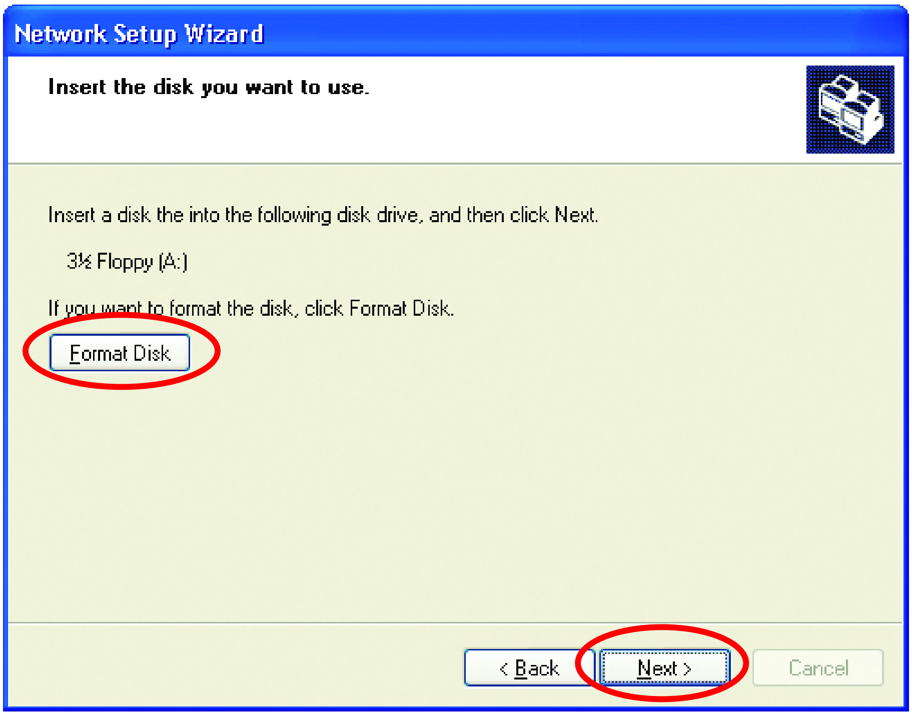
You need to run the Network Setup Wizard once on each of the computers on your network. To run the wizard on computers that are not running Windows XP, you can use the Windows XP CD or a Network Setup Disk.

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.



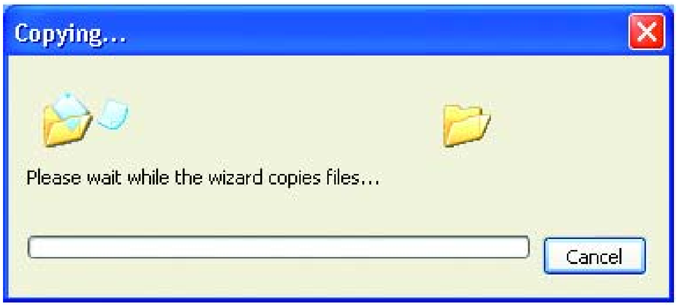
Network Setup Wizard

Insert the disk you want to use.

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

3½ Floppy (A:)

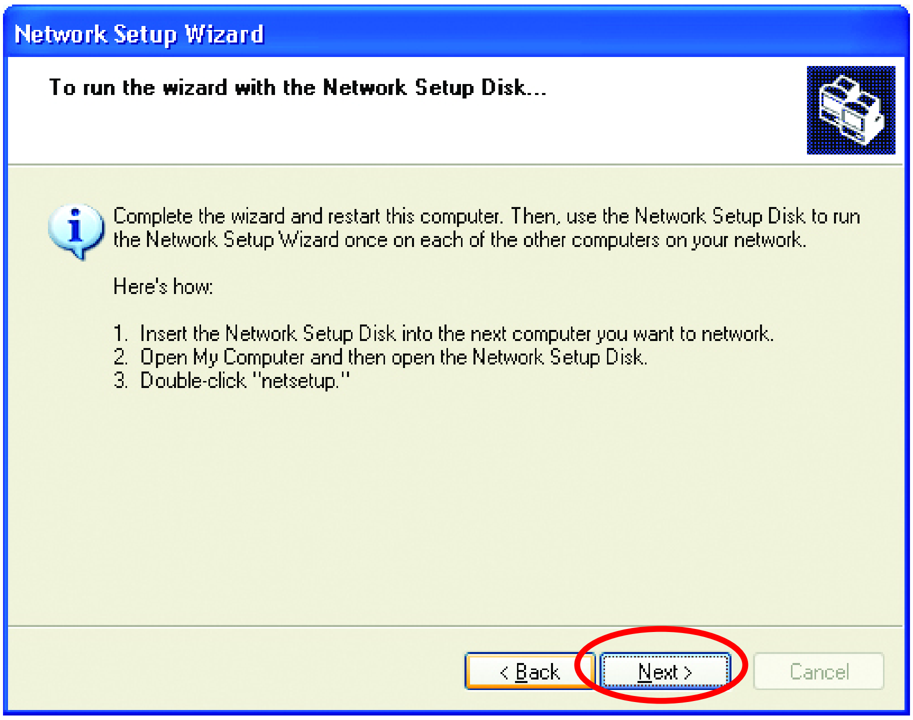
If you want to format the disk, click Format Disk.



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.

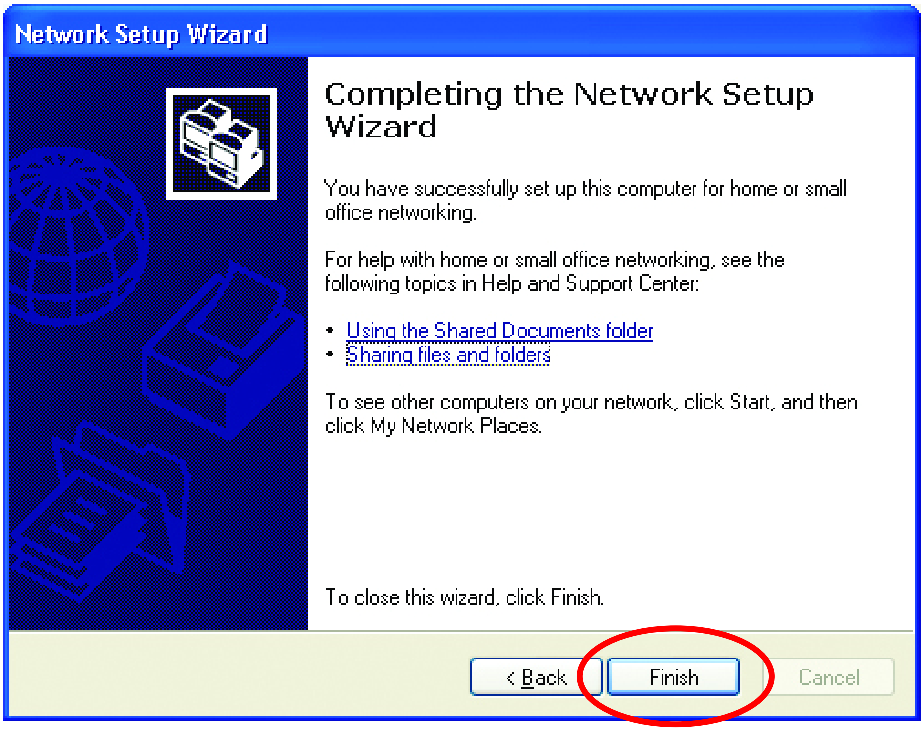
Here's how:

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.



Network Setup Wizard

Completing the Network Setup Wizard

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

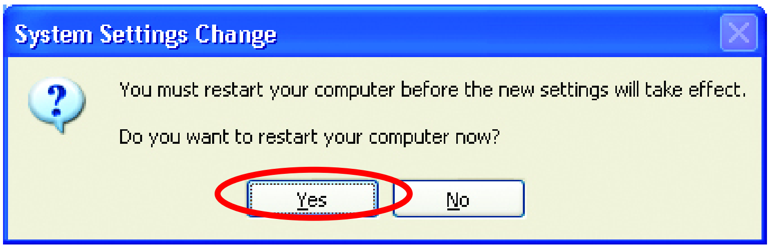
For help with home or small office networking, see the following topics in Help and Support Center:

- 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



System Settings Change

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

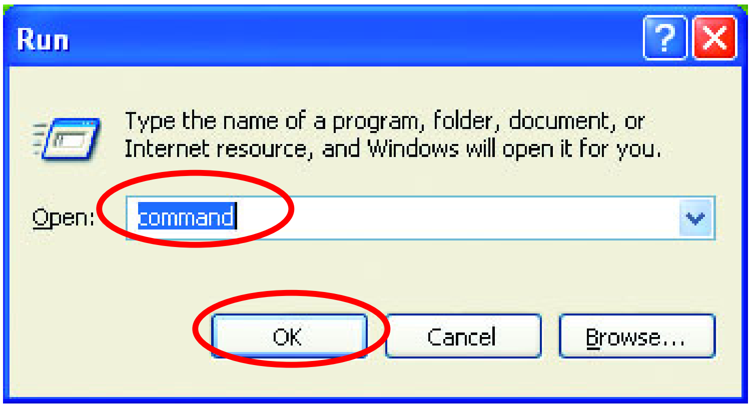
Do you want to restart your computer now?

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**"

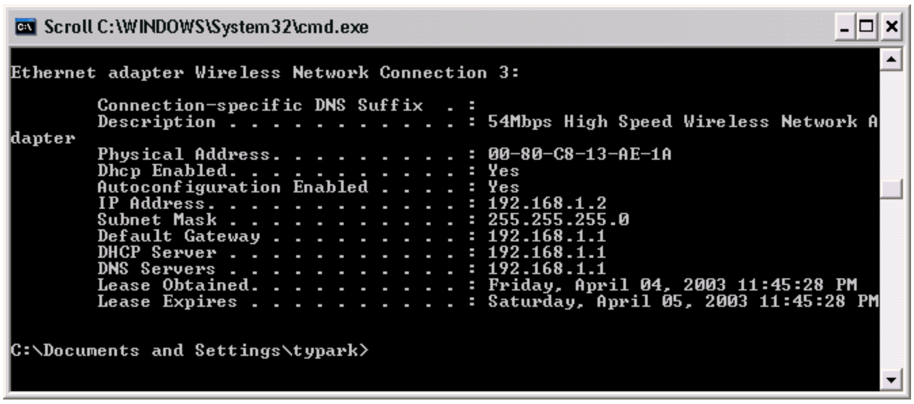
Click "**OK**"



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: command

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.



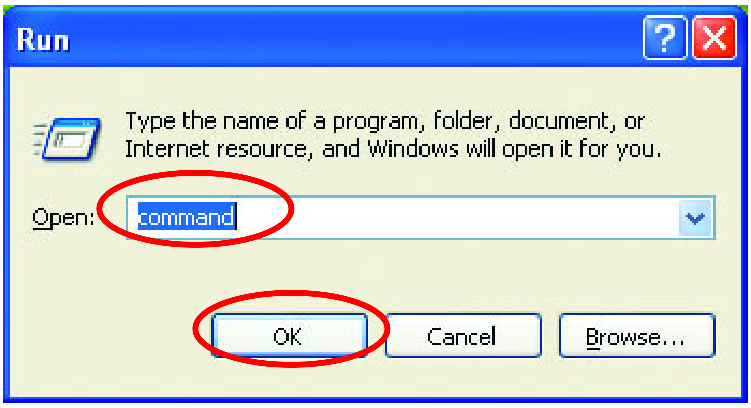
```
Ethernet adapter Wireless Network Connection 3:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 54Mbps High Speed Wireless Network A
dapter
        Physical Address. . . . . . . . . : 00-80-C8-13-AE-1A
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1
        Lease Obtained. . . . . . . . . . : Friday, April 04, 2003 11:45:28 PM
        Lease Expires . . . . . . . . . . : Saturday, April 05, 2003 11:45:28 PM

C:\Documents and Settings\typark>
```

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**"

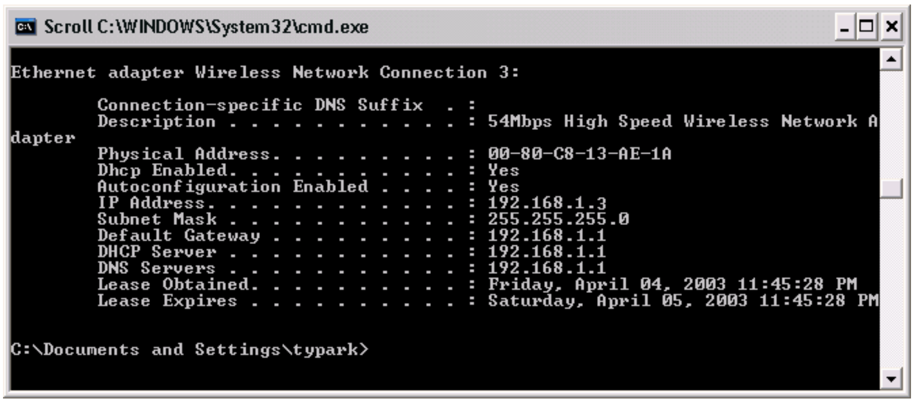
Click "**OK**"



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: command

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.



```
Ethernet adapter Wireless Network Connection 3:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 54Mbps High Speed Wireless Network A
dapter
        Physical Address. . . . . . . . . : 00-80-C8-13-AE-1A
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1
        Lease Obtained. . . . . . . . . . : Friday, April 04, 2003 11:45:28 PM
        Lease Expires . . . . . . . . . . : Saturday, April 05, 2003 11:45:28 PM

C:\Documents and Settings\typark>
```

In this case, the IP address that we acquired is 192.168.1.3. However, it's often that the acquired IP address of the network adapter might would not be the same.

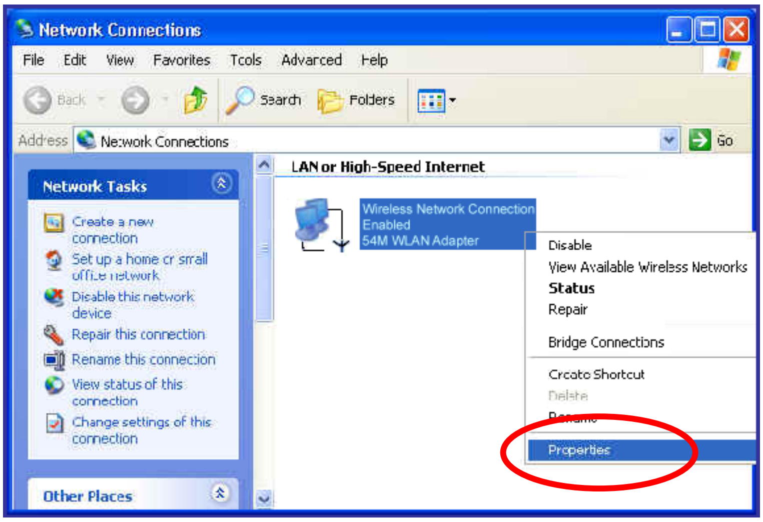
NOTE:

To renew IP under Windows 98SE 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**"



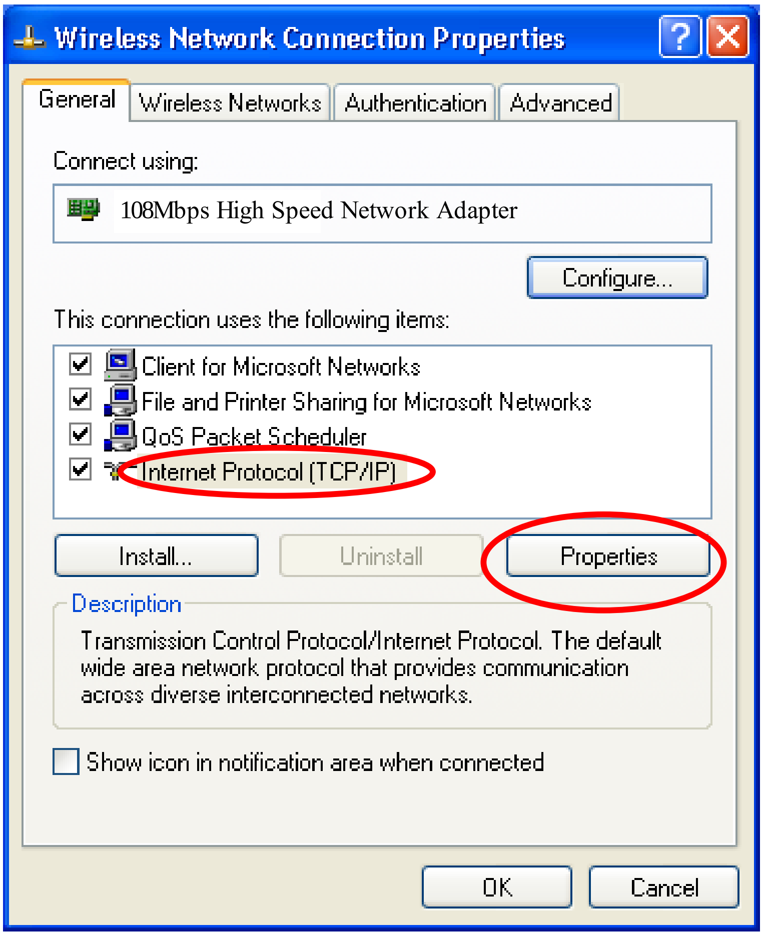
Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
Other Places
LAN or High-Speed Internet
Wireless Network Connection
Enabled
54M WLAN Adapter
Disable
View Available Wireless Networks
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
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.



Connect using:

108Mbps High Speed Network 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

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

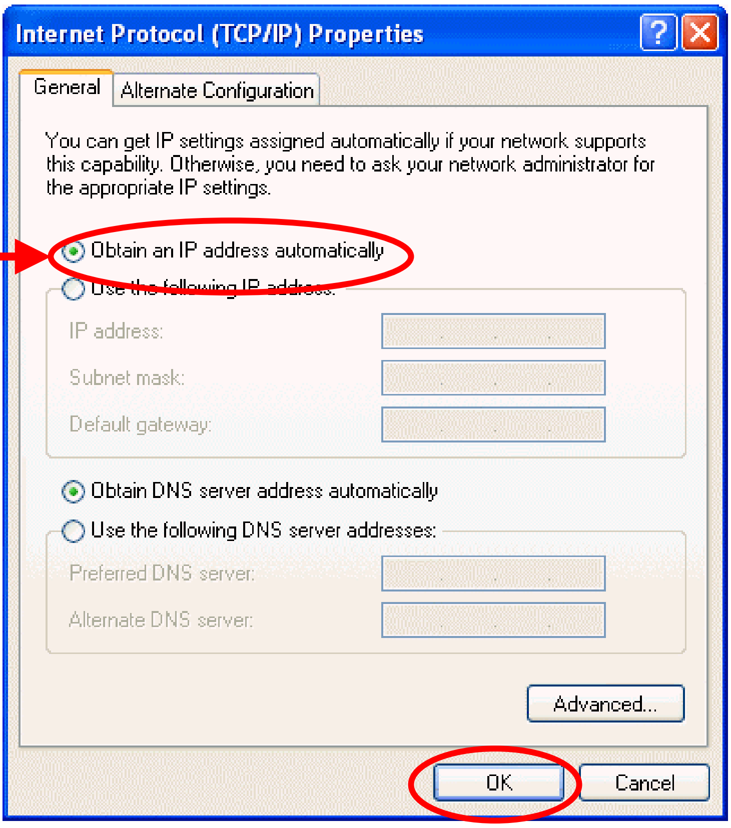
□ Show icon in notification area when connected

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



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: . . .

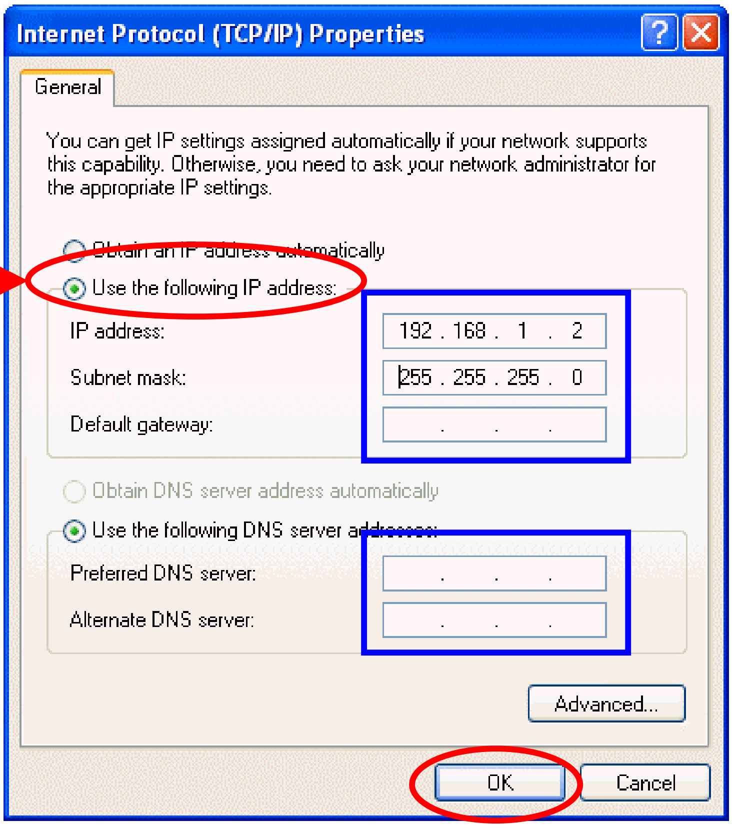
Static IP Address

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



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: . . .

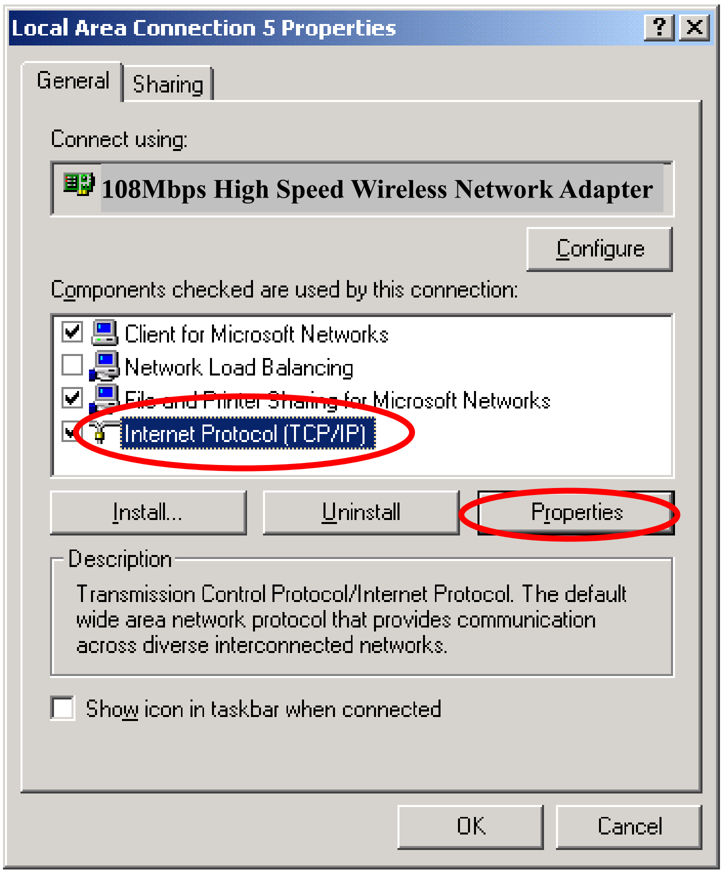
NOTE:

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

Connect using:

108Mbps High Speed Wireless Network Adapter

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

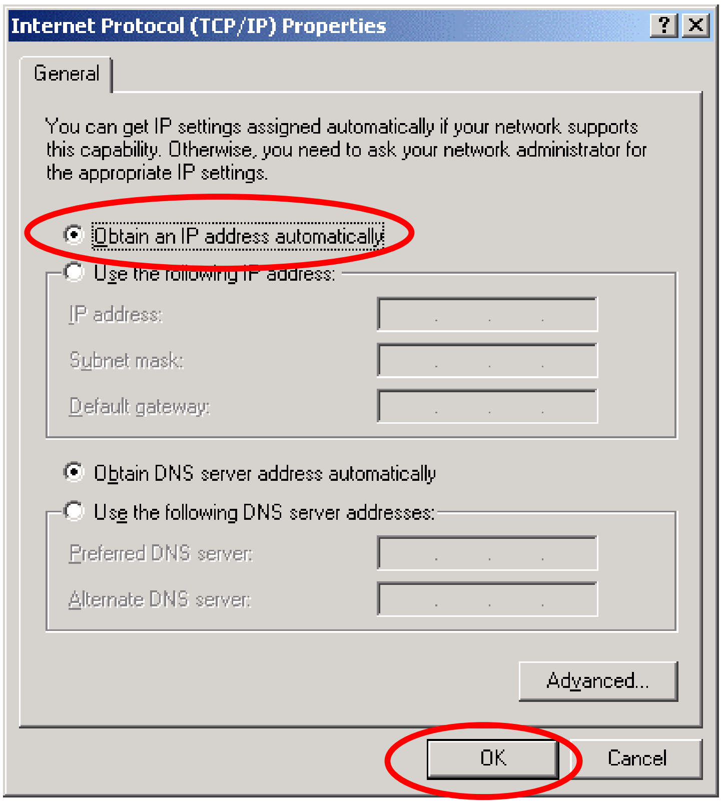
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ 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: . . .

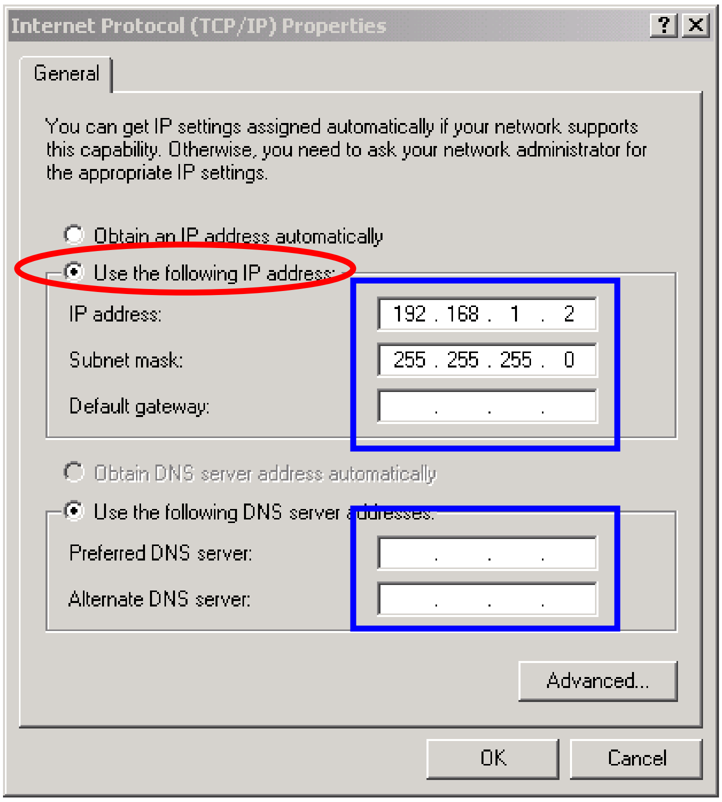
Alternate DNS server: . . .

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

Enter the **IP address** and **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



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: . . .

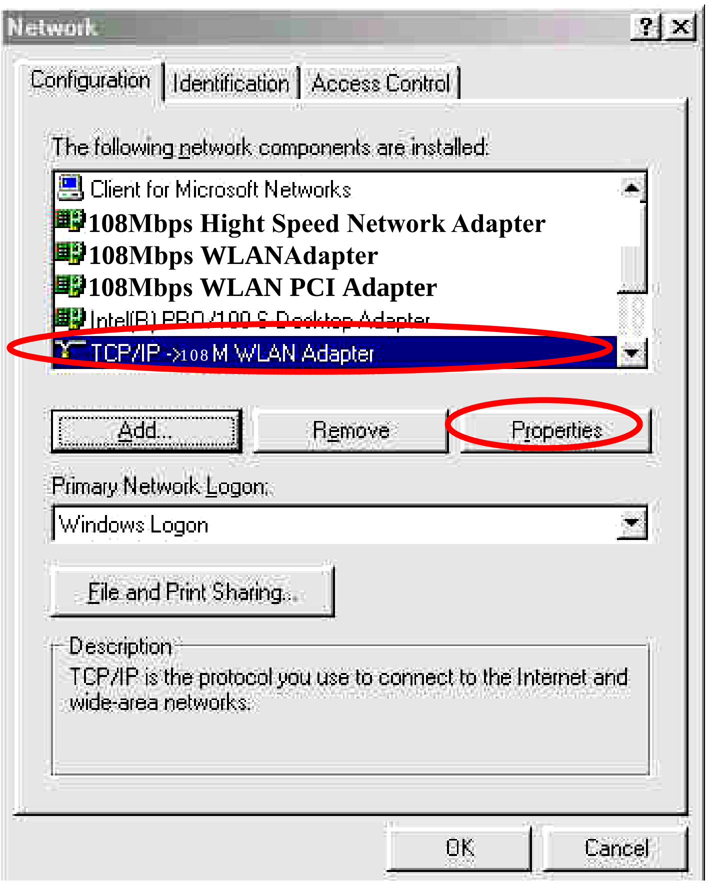
Alternate DNS server: . . .

Wireless Network In Windows 98SE 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:

- Client for Microsoft Networks
- 108Mbps Hight Speed Network Adapter
- 108Mbps WLANAdapter
- 108Mbps WLAN PCI Adapter
- Intel(R) PRO/100 S Desktop Adapter
- TCP/IP ->108 M WLAN Adapter

Primary Network Logon:

Windows Logon

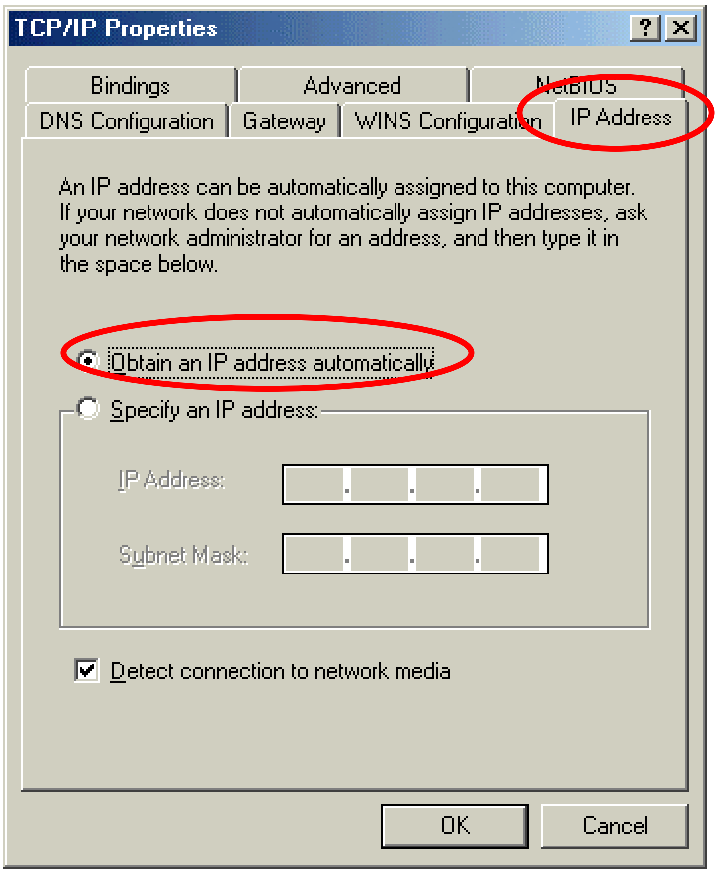
Description

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: . . .

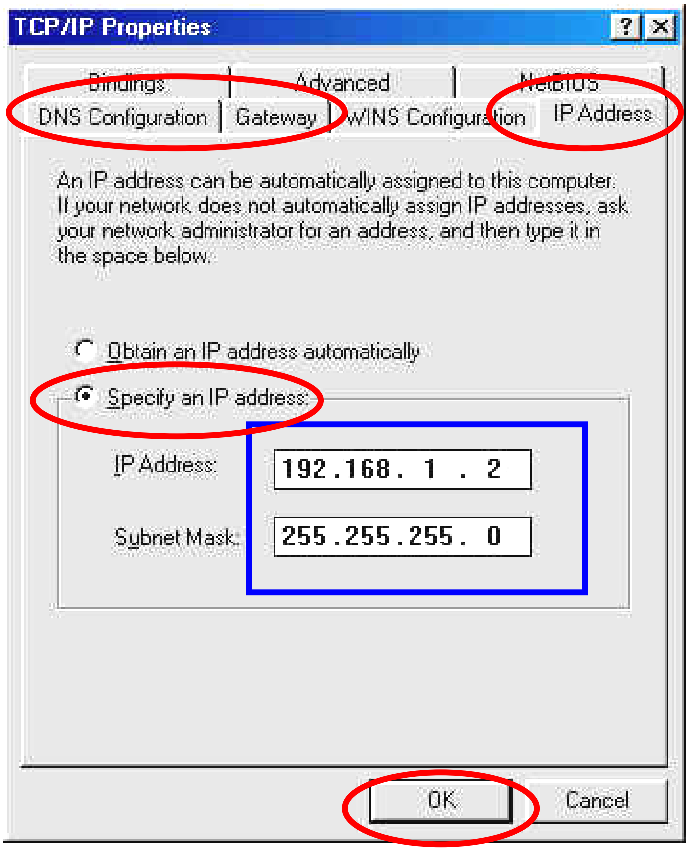
☑ Detect connection to network media

Select "**Specify an 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



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:

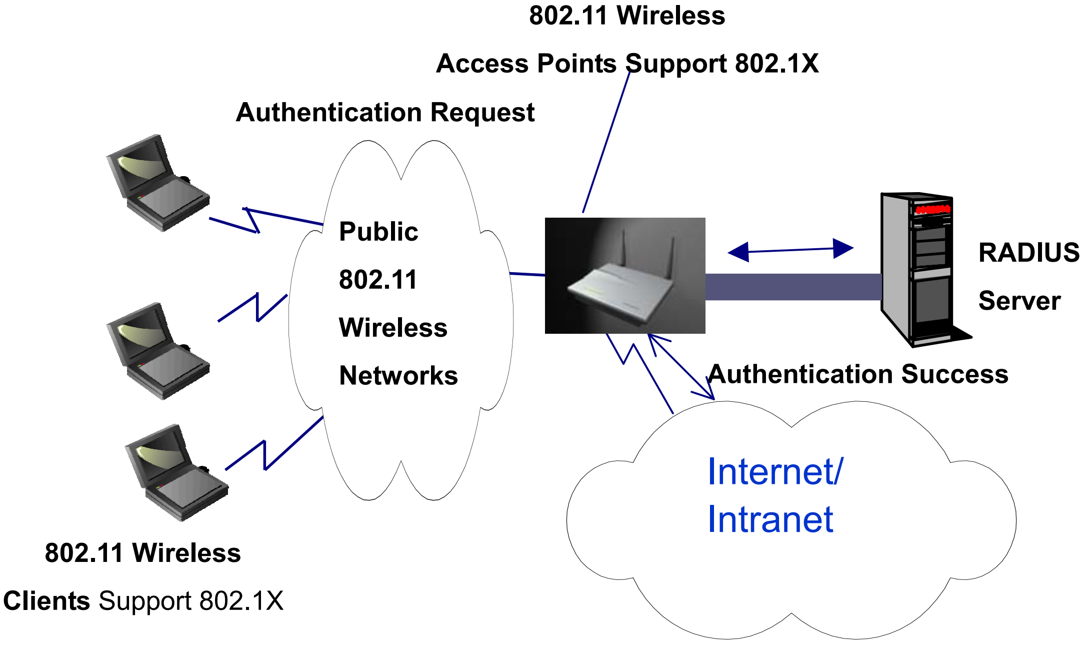
IP Address: 192.168. 1 . 2

Subnet Mask: 255.255.255. 0

APPENDIX B: 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:

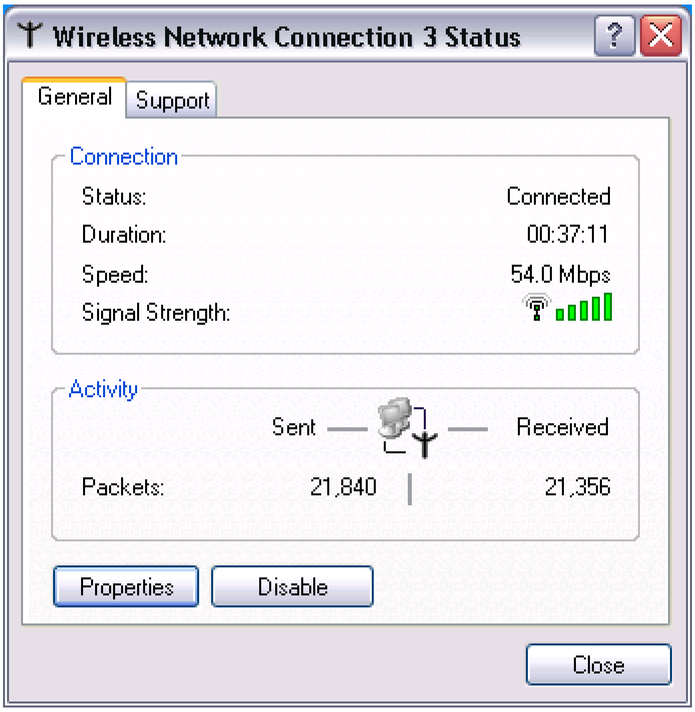
1. The client sends an EAP start message to the Access Point
2. The Access Point replies with an EAP Request ID message
3. The client sends its Network Access Identifier (NAI) – its user name – to the Access Point in an EAP Respond message.
4. The Access Point forwards the NAI to the RADIUS server with 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 108Mbps 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 108Mbps wireless PC Card.
4. Click "**Properties**" to open up the Properties setting window.



Connection

Status: Connected

Duration: 00:37:11

Speed: 54.0 Mbps

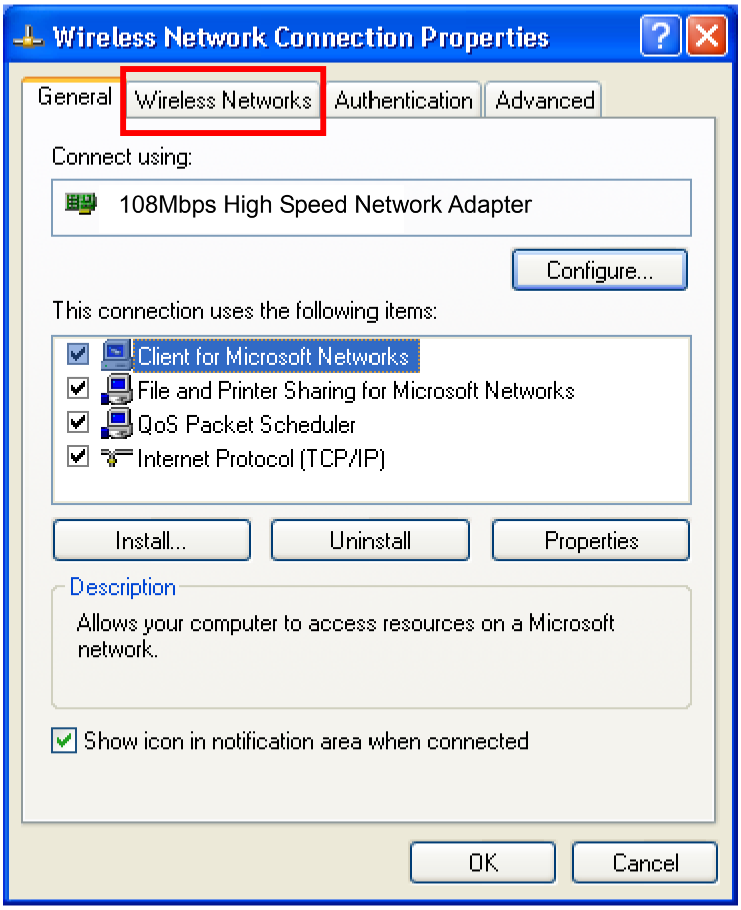
Signal Strength:

Activity

Sent — Received

Packets: 21,840 | 21,356

5. Click on the “**Wireless Network**” tab.


Wireless Network Connection Properties

Connect using:

108Mbps High Speed Network 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)

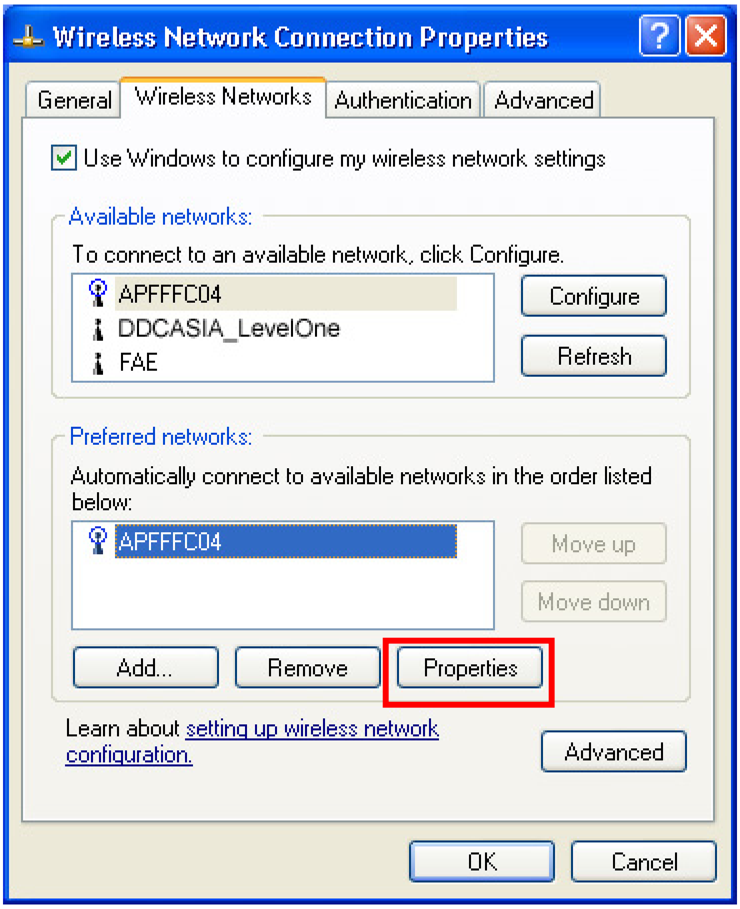
Description

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

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

APFFFC04
DDCASIA_LevelOne
FAE

Preferred networks:

Automatically connect to available networks in the order listed below:

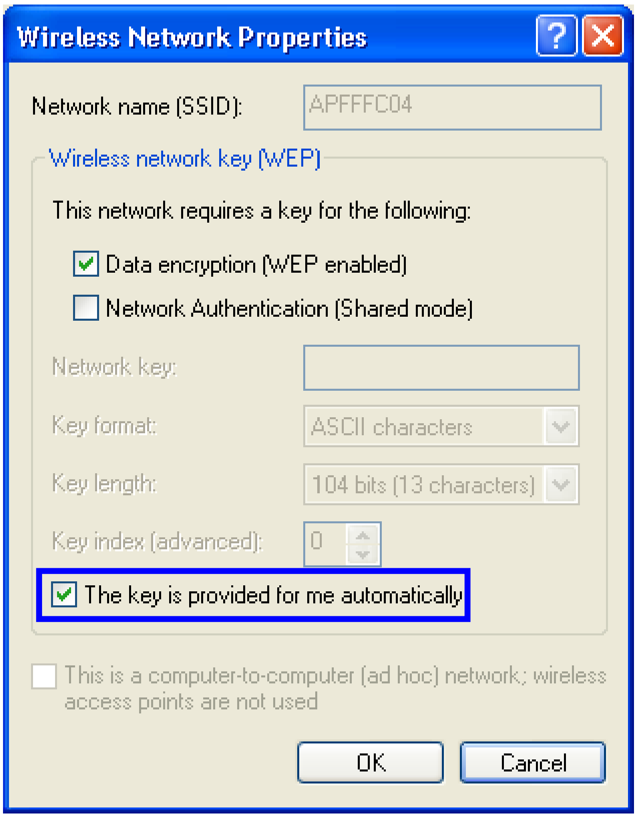
APFFFC04

Learn about setting up wireless network configuration.

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

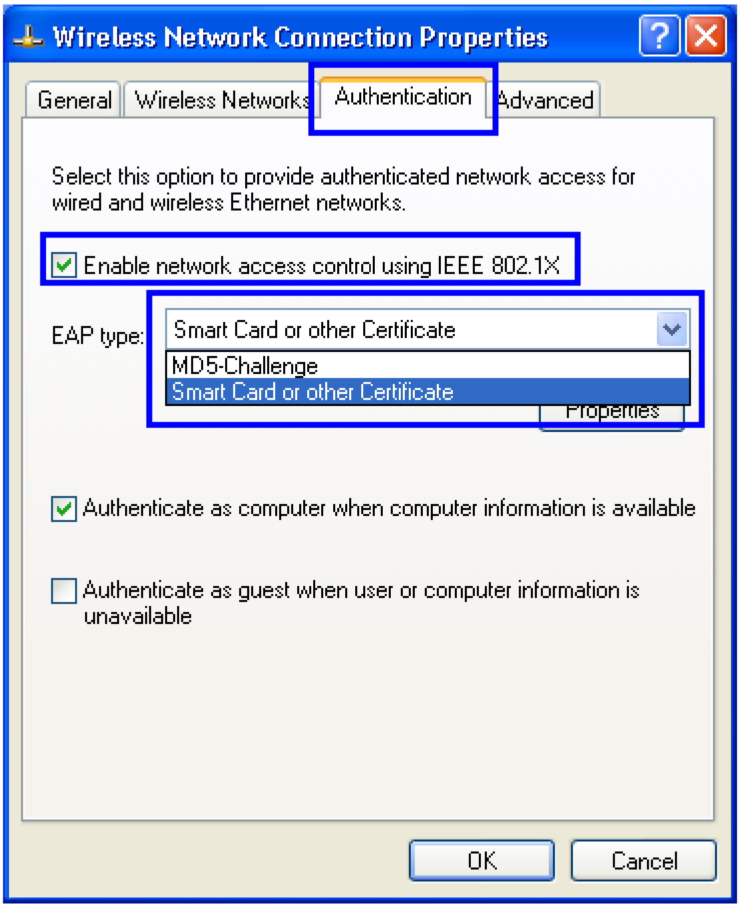
□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

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

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

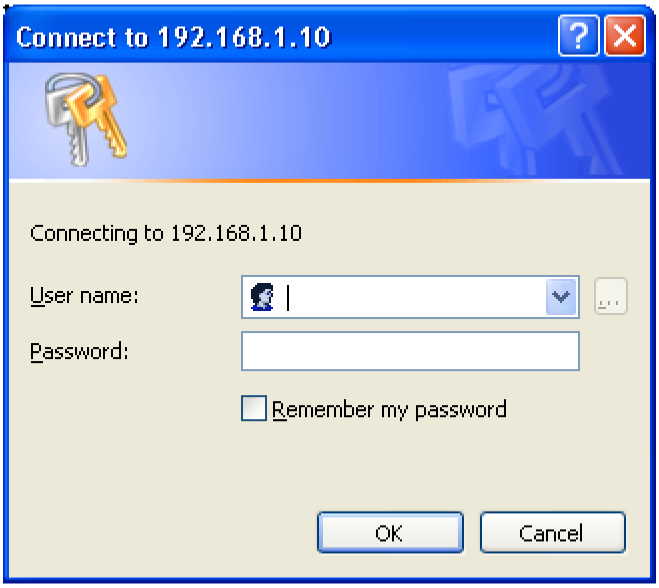
12. Click "**OK**" to close the Wireless Network Connection Properties window, thus make the changes effective.

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:

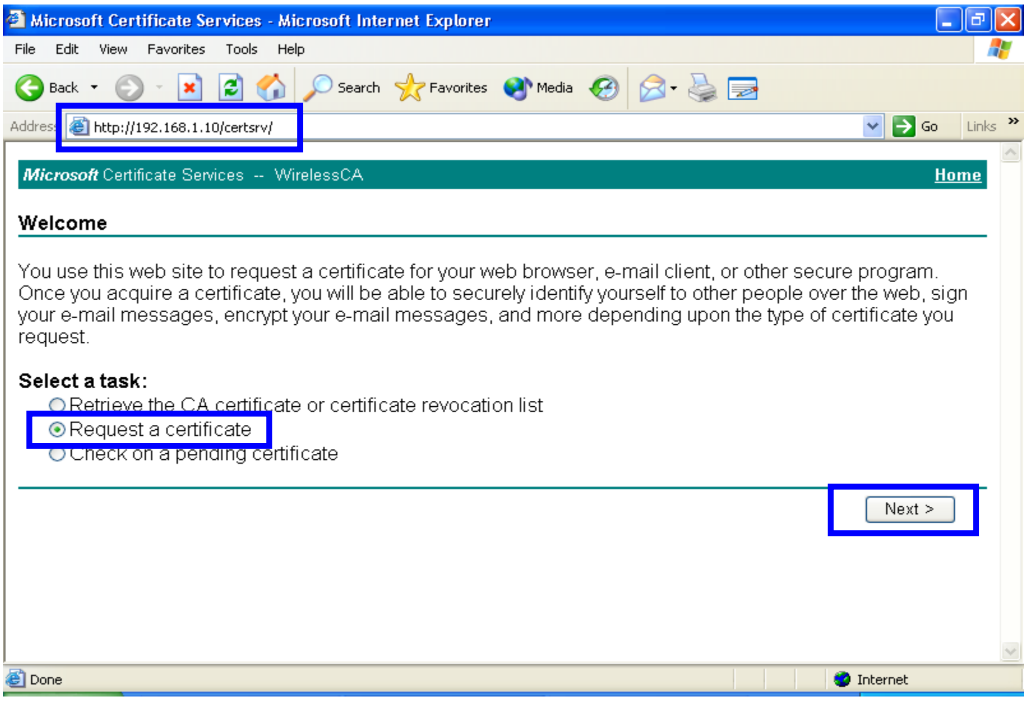
□ Remember my password

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

Address: http://192.168.1.10/certsrv/

Microsoft Certificate Services -- WirelessCA

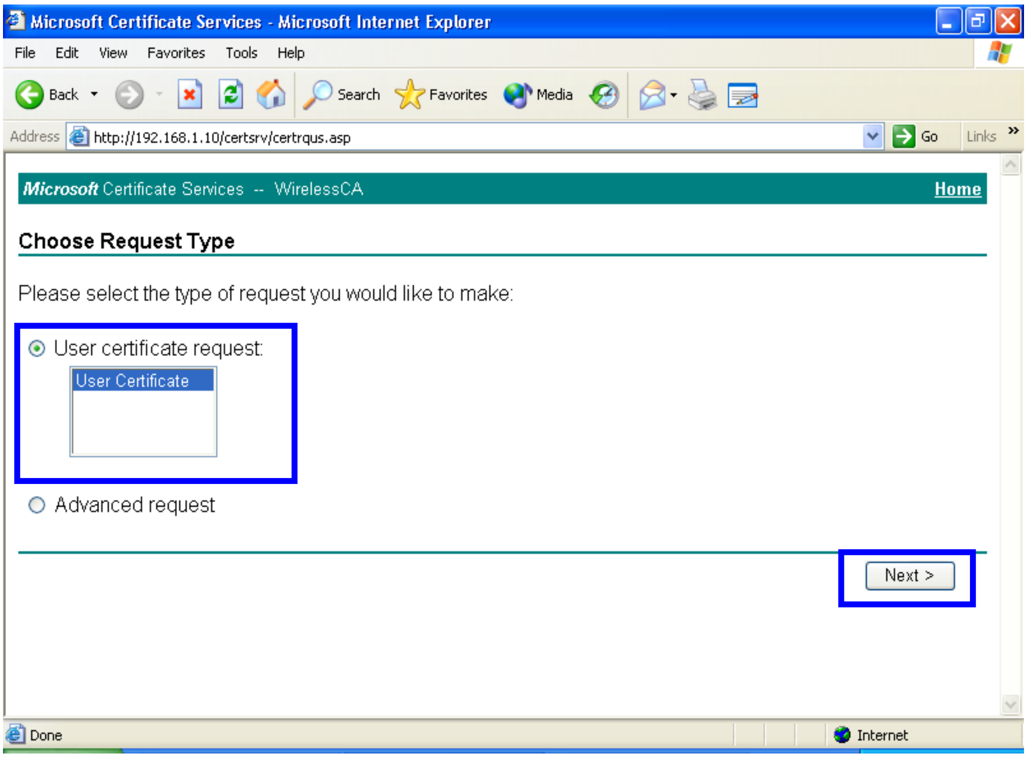
Welcome

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

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



Microsoft Certificate Services - Microsoft Internet Explorer

Address: http://192.168.1.10/certsrv/certrqus.asp

Microsoft Certificate Services -- WirelessCA

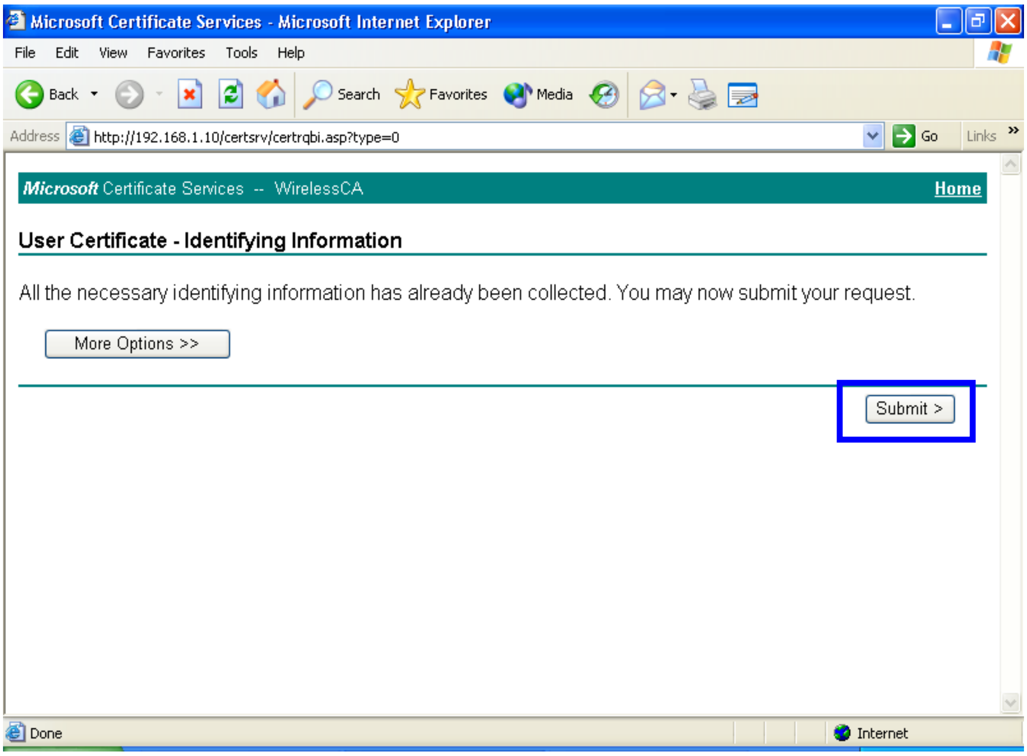
Choose Request Type

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

● User certificate request:
User Certificate

○ Advanced request

18. Click “**Submit** >” to continue.



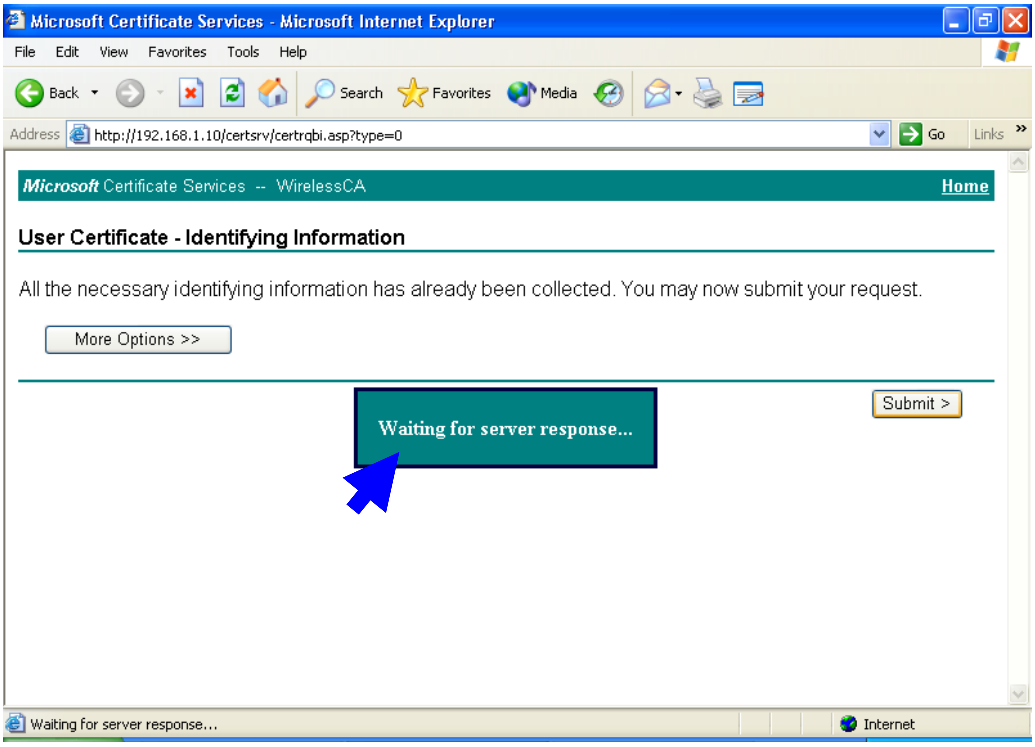
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrqbi.asp?type=0
Go Links
Microsoft Certificate Services -- WirelessCA
Home

User Certificate - Identifying Information

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

More Options >>
Submit >
Done
Internet

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



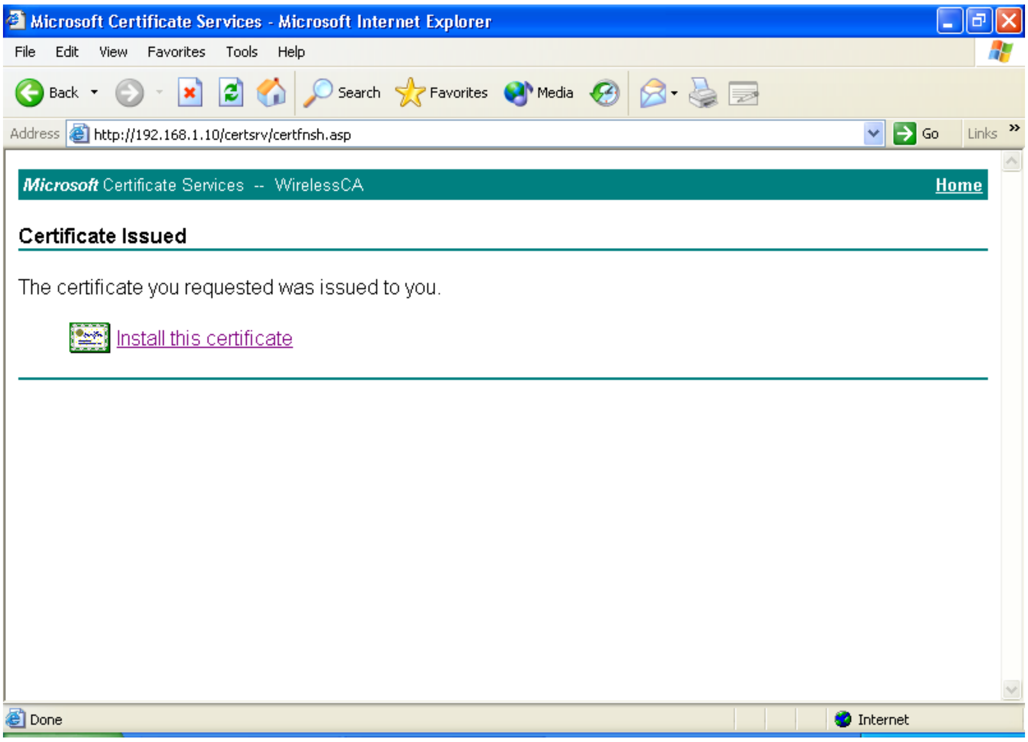
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrqbi.asp?type=0
Go Links
Microsoft Certificate Services -- WirelessCA
Home

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

Address http://192.168.1.10/certsrv/certfnsh.asp

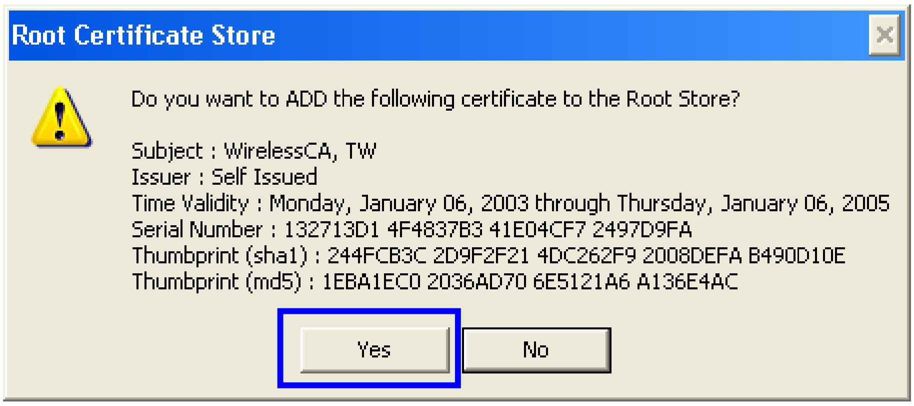
Microsoft Certificate Services -- WirelessCA **Home**

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

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

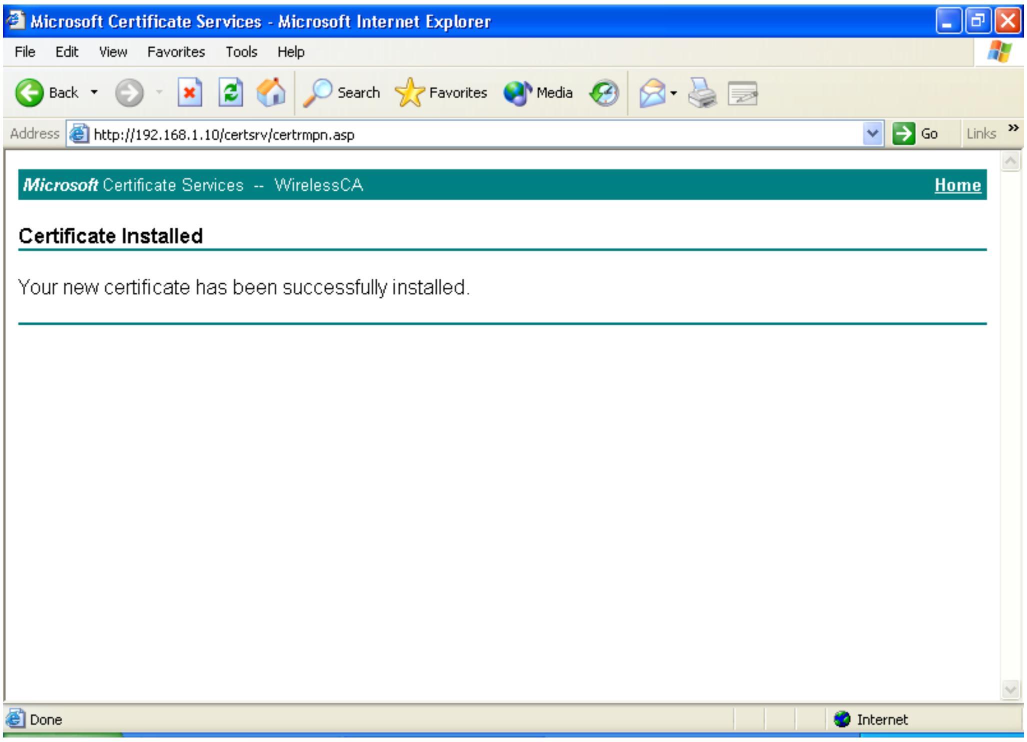


Root Certificate Store

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.

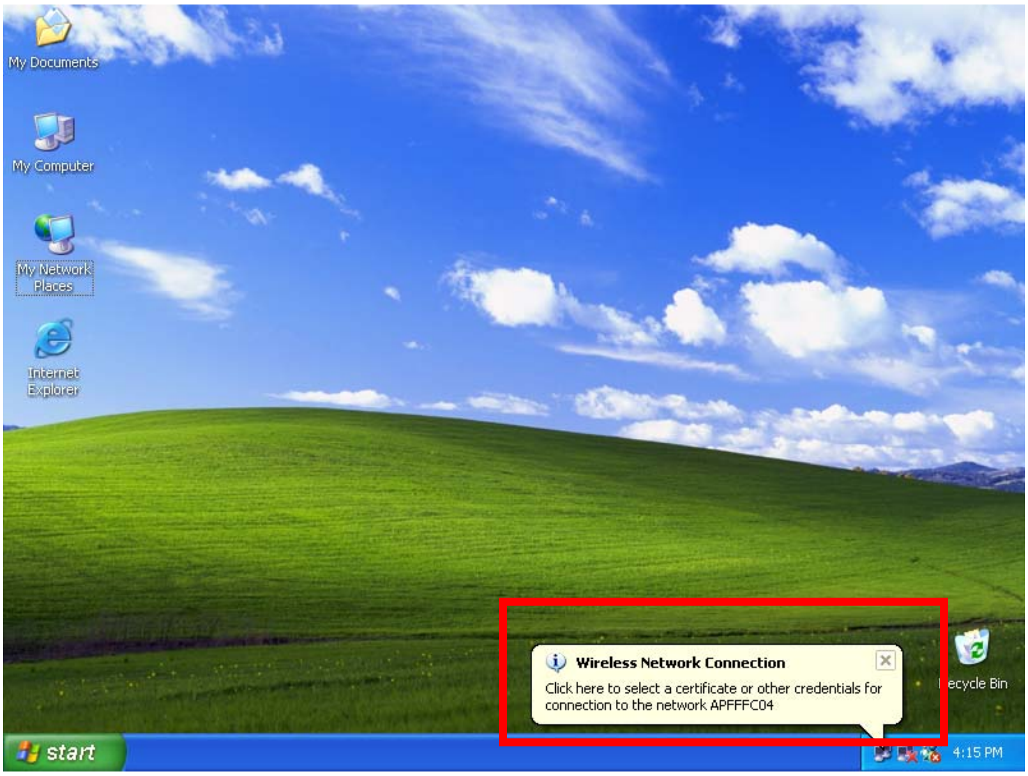

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrmpn.asp
Go Links
Microsoft Certificate Services -- WirelessCA
Home

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.

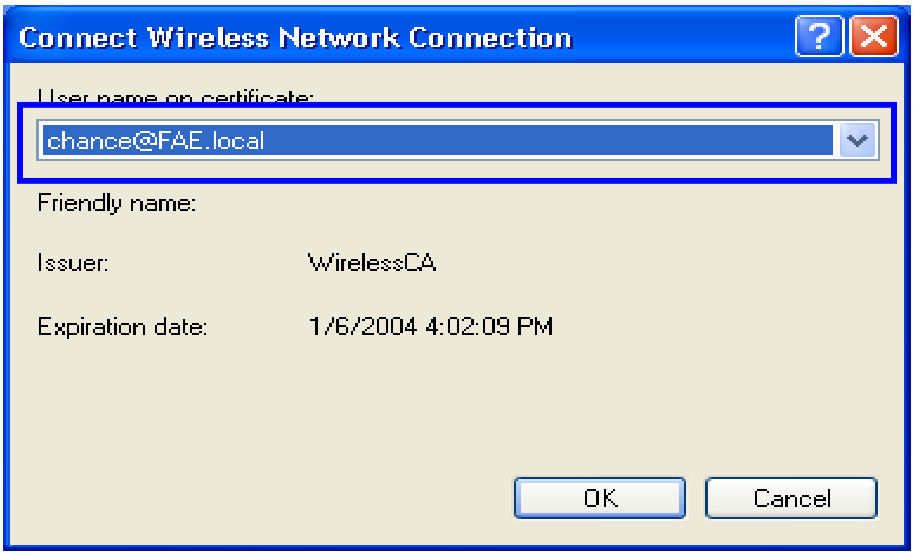
23. Windows XP will prompt you to select a certificate for wireless network connection. Click on the network connection icon in the system tray to continue.



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

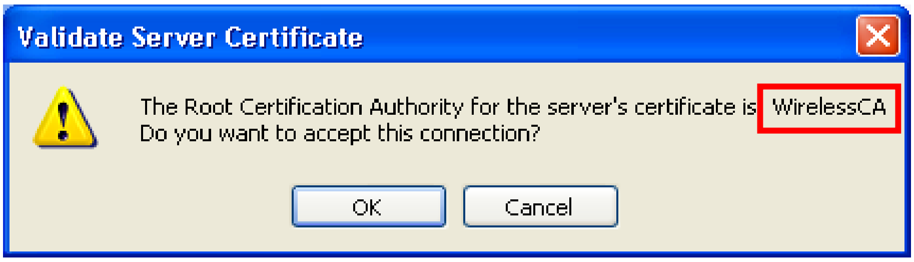
User name on certificate: chance@FAE.local

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?

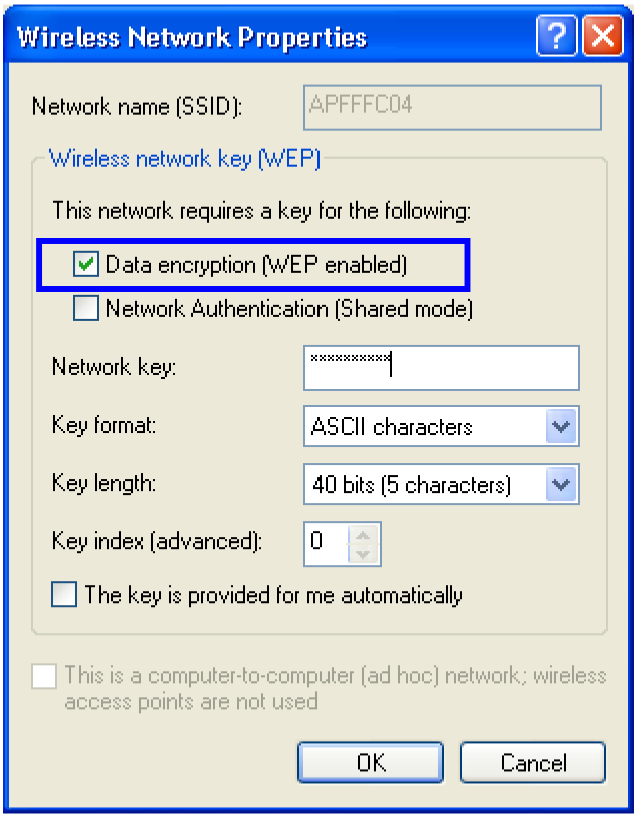
MD5 Authentication

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

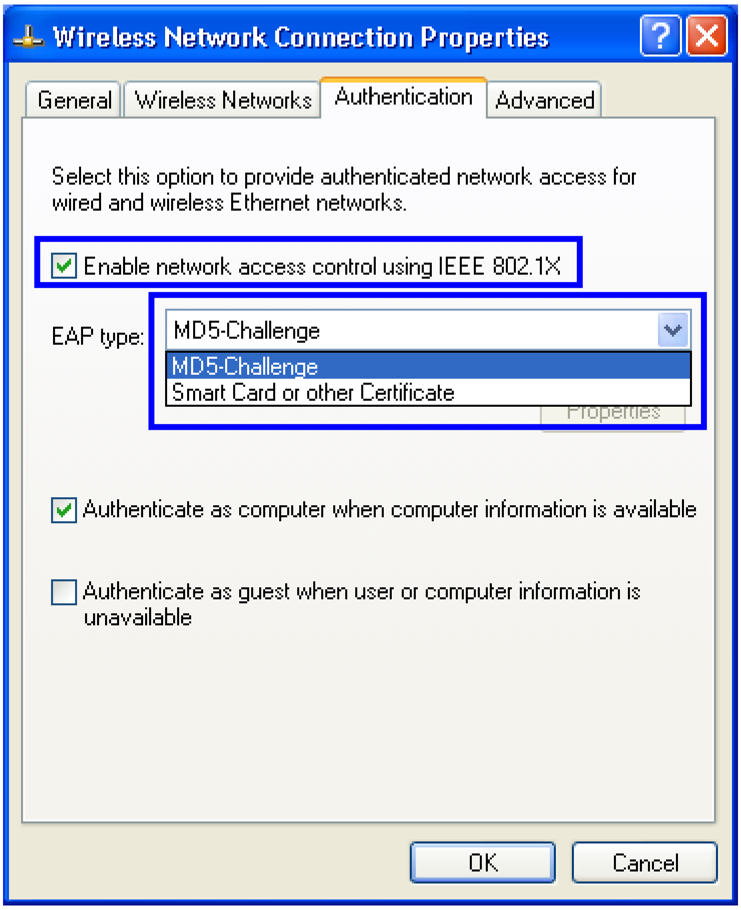
Please note that that value of Network key entered, and key format/length used, must be the same as that used in the Access Point. Although there are 4 set of keys can be set in the Access Point WEP configuration, it's the ***first set*** of key that must be the same as that we used by the supplicant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



Wireless Network Connection Properties

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

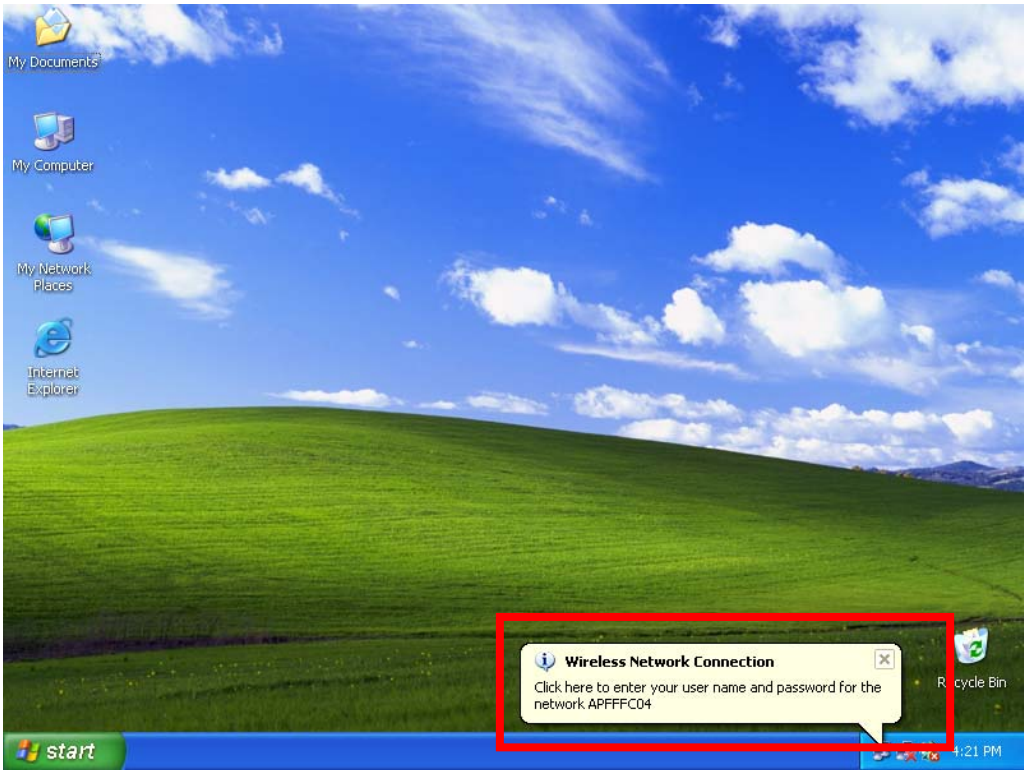
☑ Authenticate as computer when computer information is available

□ 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.

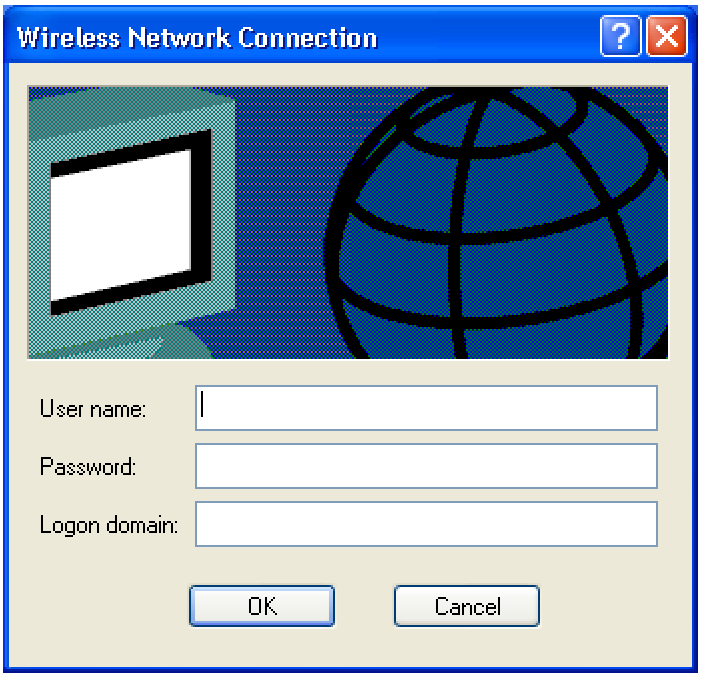


Wireless Network Connection

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.



Wireless Network Connection

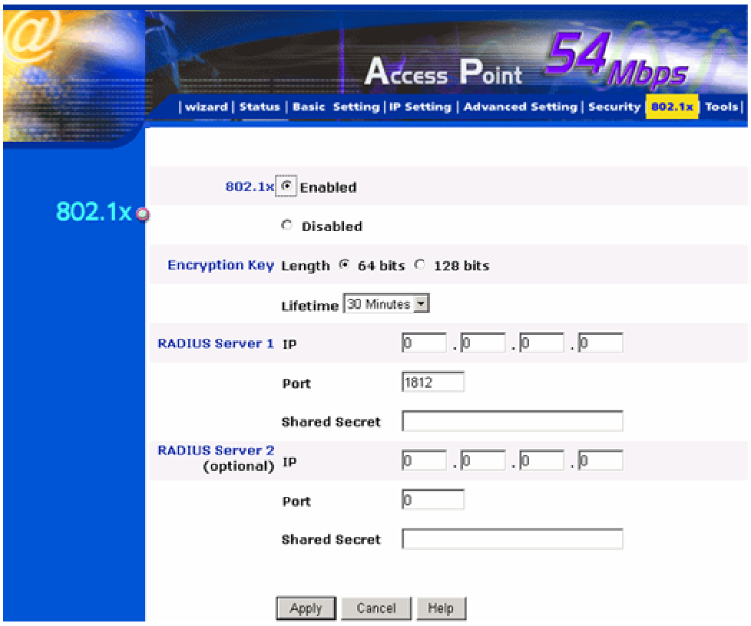
User name:

Password:

Logon domain:

Authenticator: Wireless Network Access Point

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


Access Point
54Mbps
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security
802.1x
Tools |
802.1x
Apply
Cancel
Help

802.1x ● Enabled
○ Disabled

Encryption Key Length ● 64 bits ○ 128 bits

Lifetime 30 Minutes

RADIUS Server 1 IP 0 . 0 . 0 . 0

Port 1812

Shared Secret

RADIUS Server 2 (optional) IP 0 . 0 . 0 . 0

Port 0

Shared Secret

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.

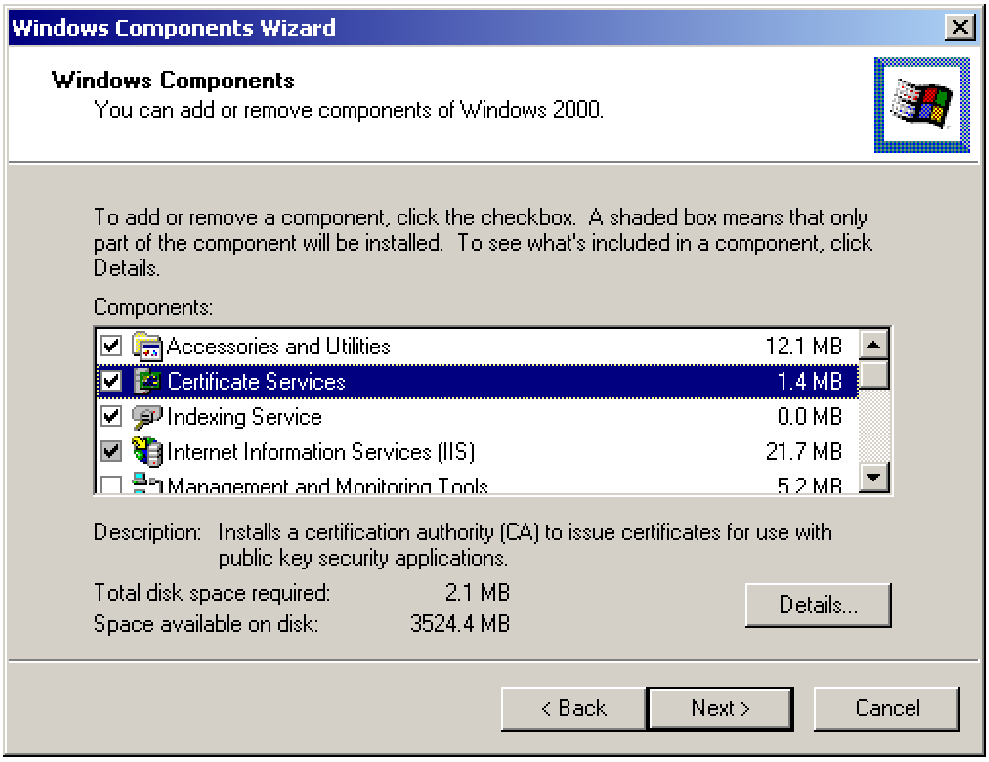
NOTE:

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.



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:

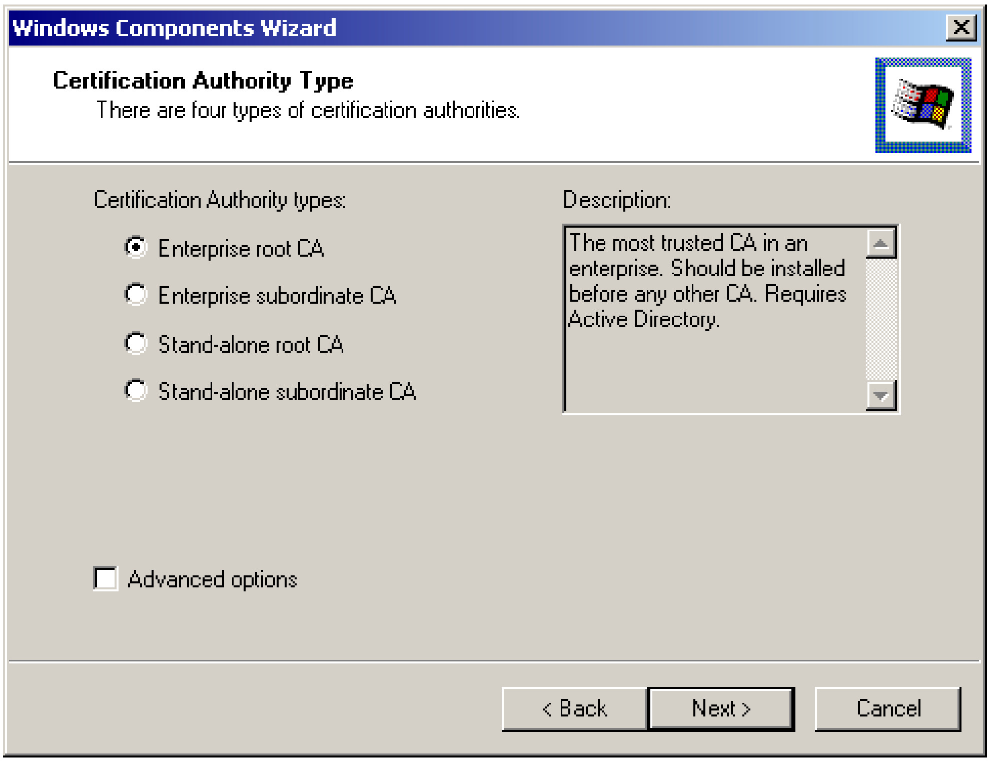
☑	Accessories and Utilities	12.1 MB
☑	Certificate Services	1.4 MB
☑	Indexing Service	0.0 MB
☑	Internet Information Services (IIS)	21.7 MB
□	Management and Monitoring Tools	5.2 MB

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.



Windows Components Wizard

Certification Authority Type

There are four types of certification authorities.

Certification Authority types:

● Enterprise root CA

○ Enterprise subordinate CA

○ Stand-alone root CA

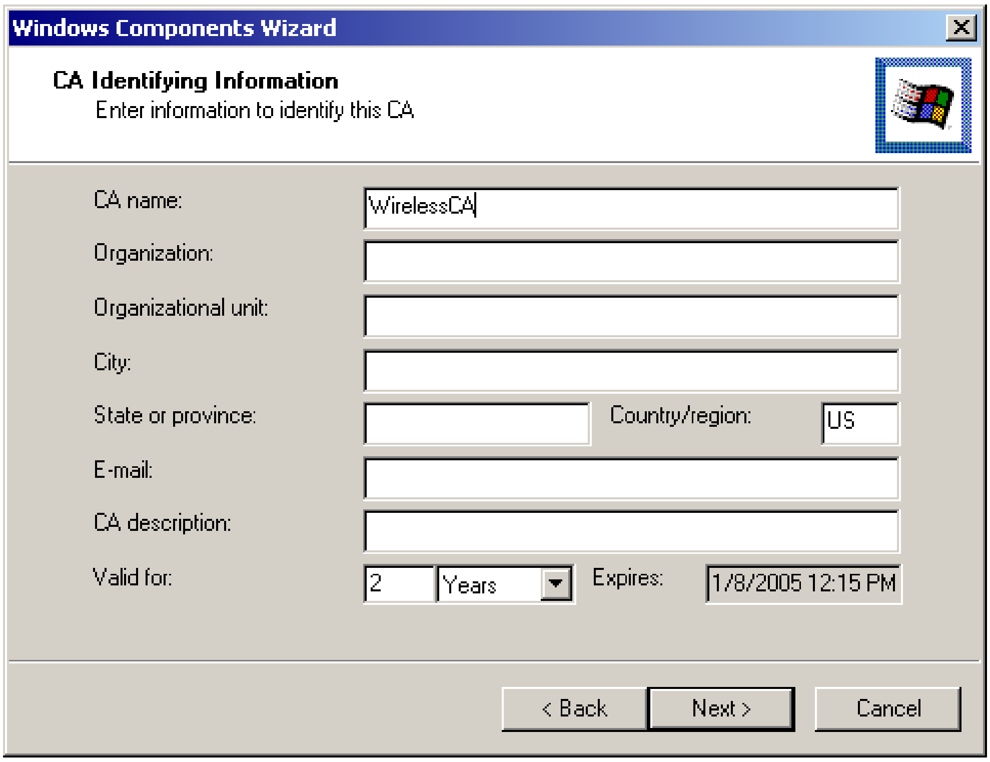
○ Stand-alone subordinate CA

Description:

The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.

□ Advanced options

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



Windows Components Wizard

CA Identifying Information

Enter information to identify this CA

CA name: WirelessCA

Organization:

Organizational unit:

City:

State or province: Country/region: US

E-mail:

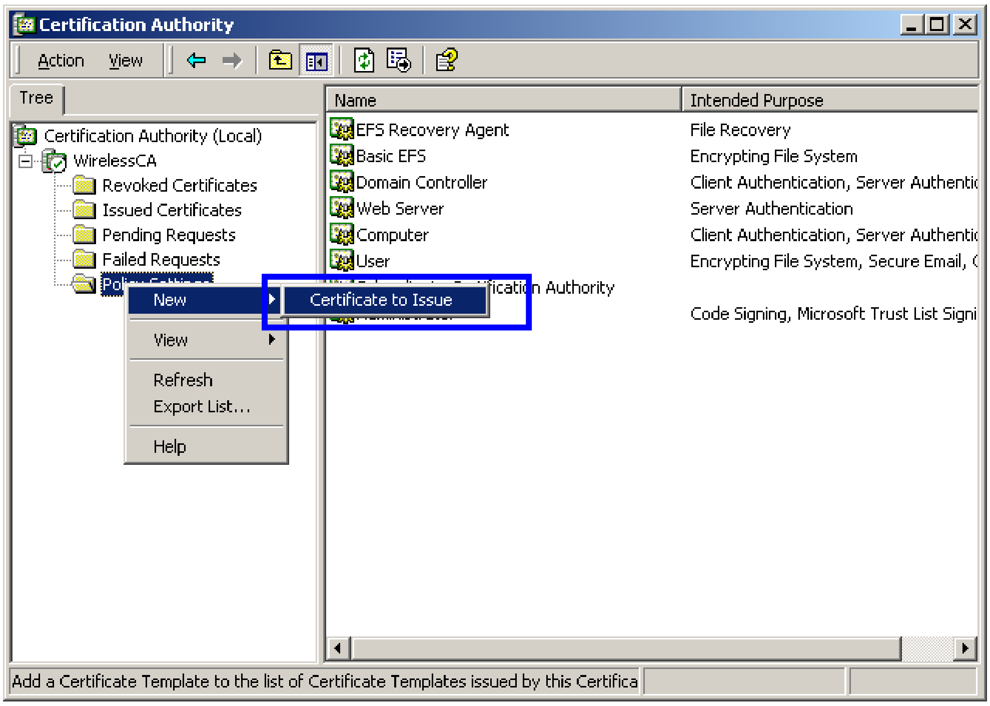
CA description:

Valid for: 2 Years Expires: 1/8/2005 12:15 PM

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

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

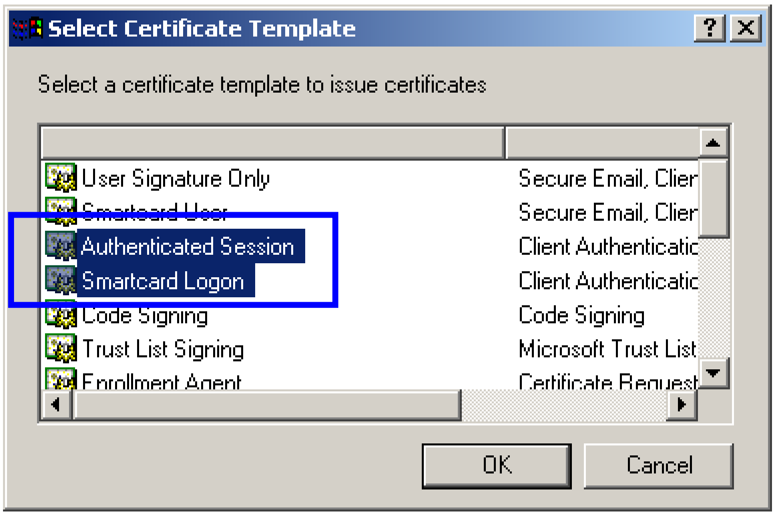
9. Select "**Certificate to Issue**"



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, (
ication 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.

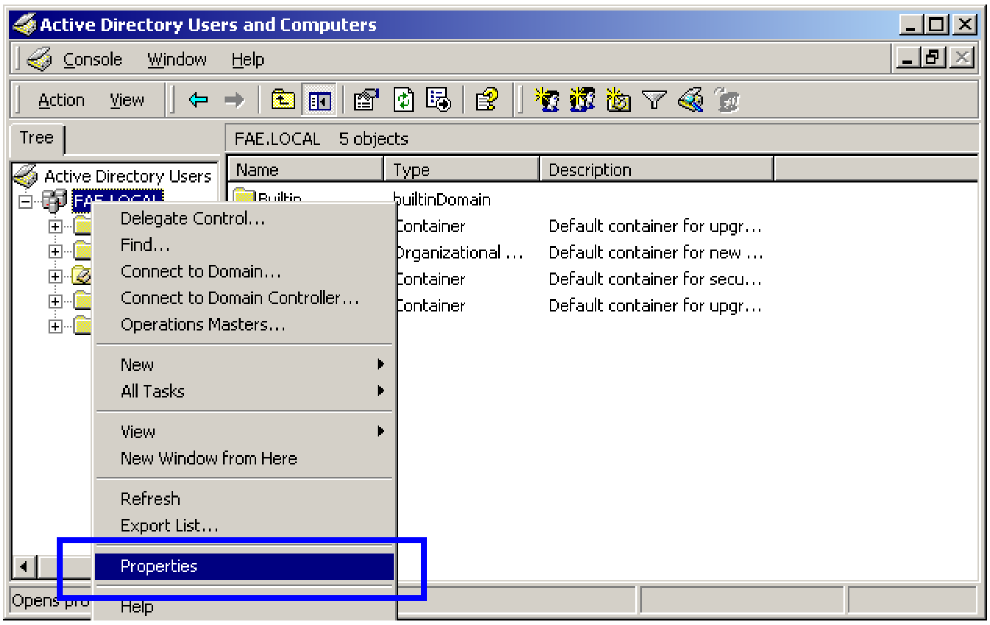


Select a certificate template to issue certificates

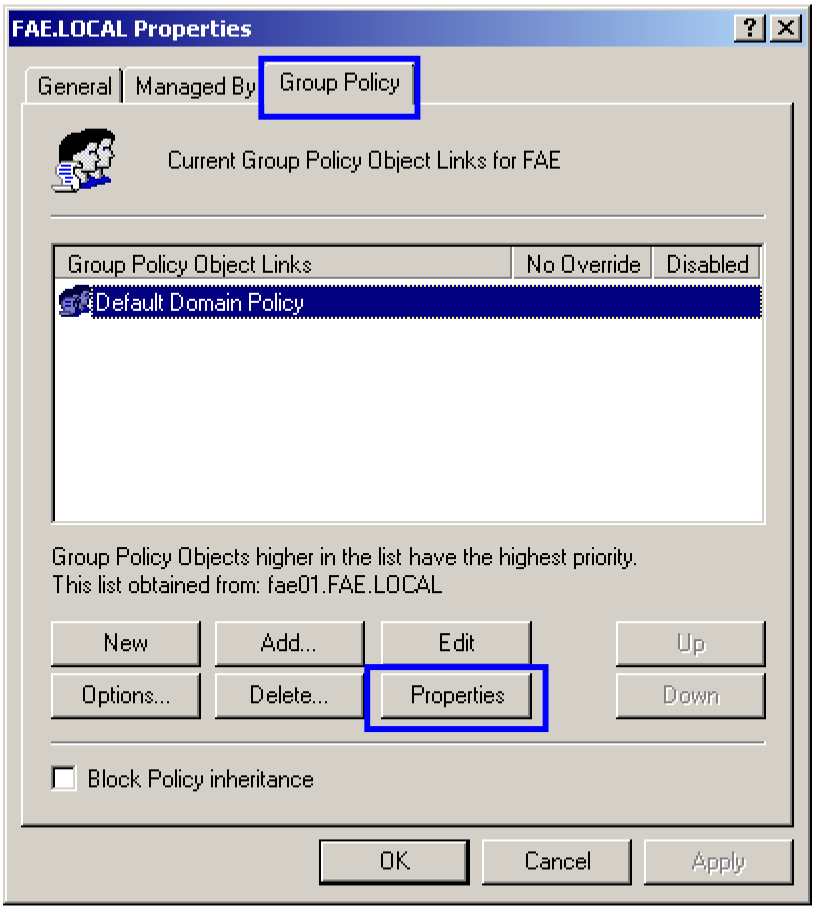
User Signature Only	Secure Email, Clier
Smartcard User	Secure Email, Clier
Authenticated Session	Client Authenticatic
Smartcard Logon	Client Authenticatic
Code Signing	Code Signing
Trust List Signing	Microsoft Trust List
Enrollment Agent	Certificate Request

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

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



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		

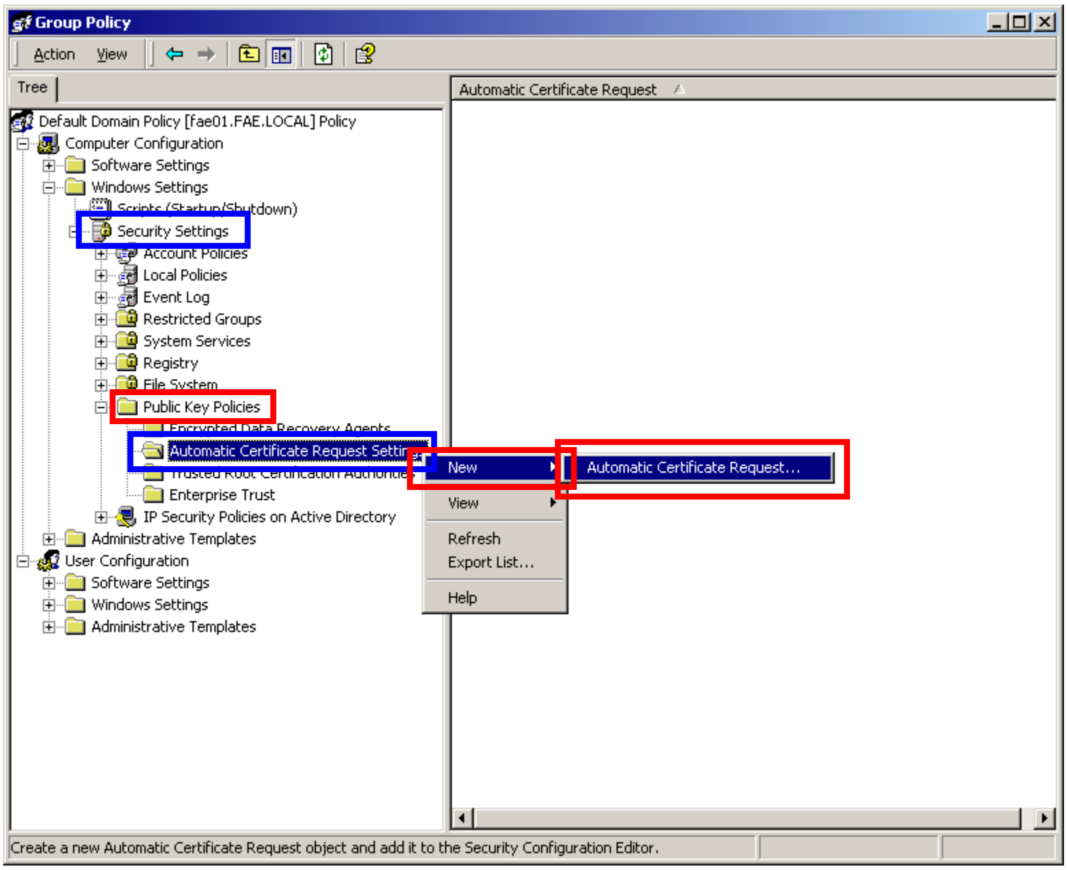
Group Policy Objects higher in the list have the highest priority.
This list obtained from: fae01.FAE.LOCAL

□ Block Policy inheritance

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

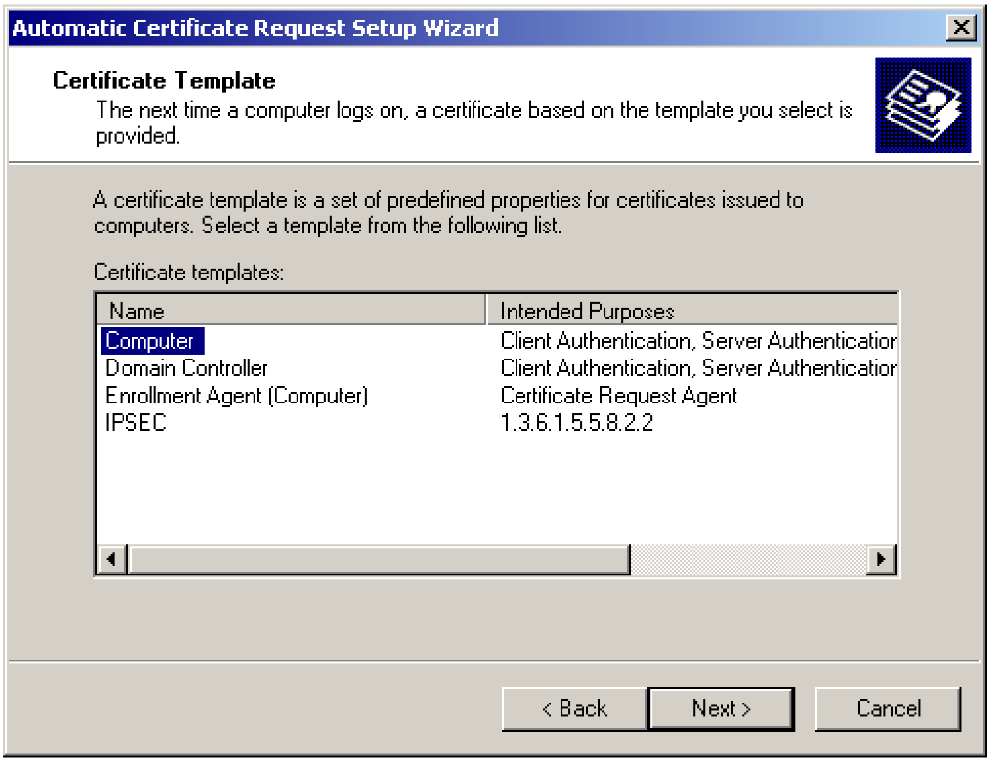
15. Right-click "**Automatic Certificate Request Setting**", and select "**New**"

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.



Certificate Template

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.

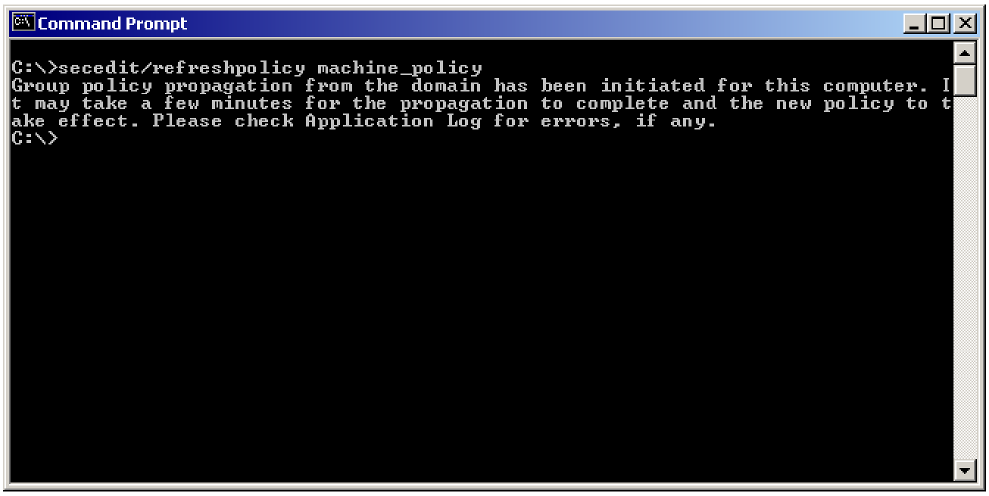
Certificate templates:

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

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

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



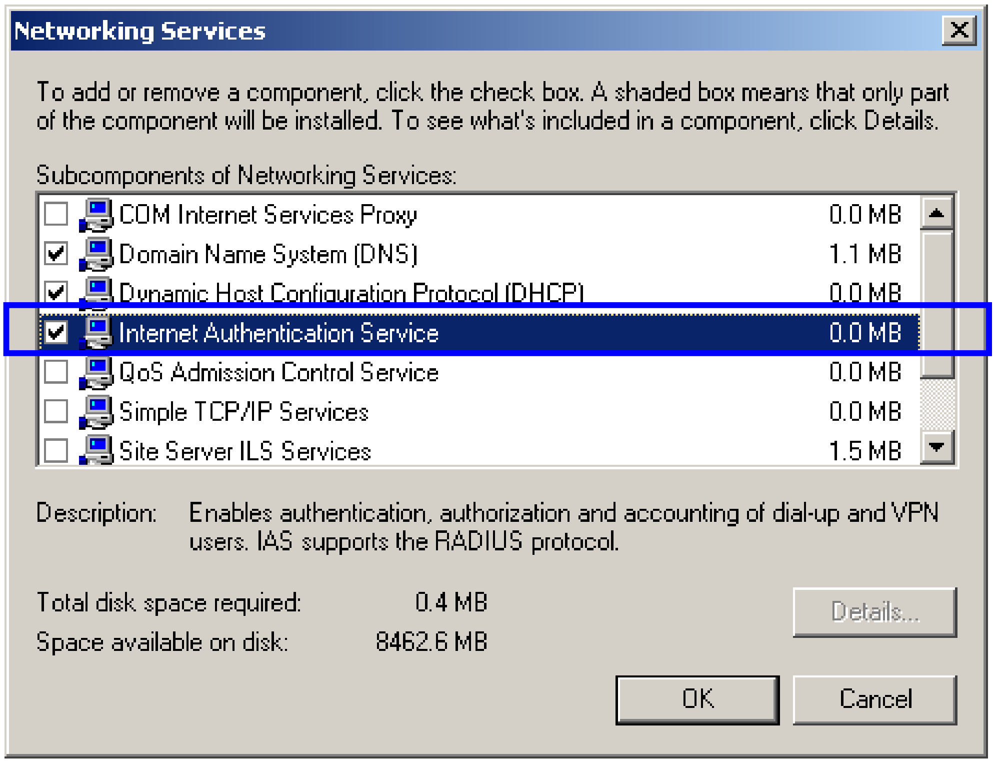
```
C:\>secedit/refreshpolicy machine_policy
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>
```

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.

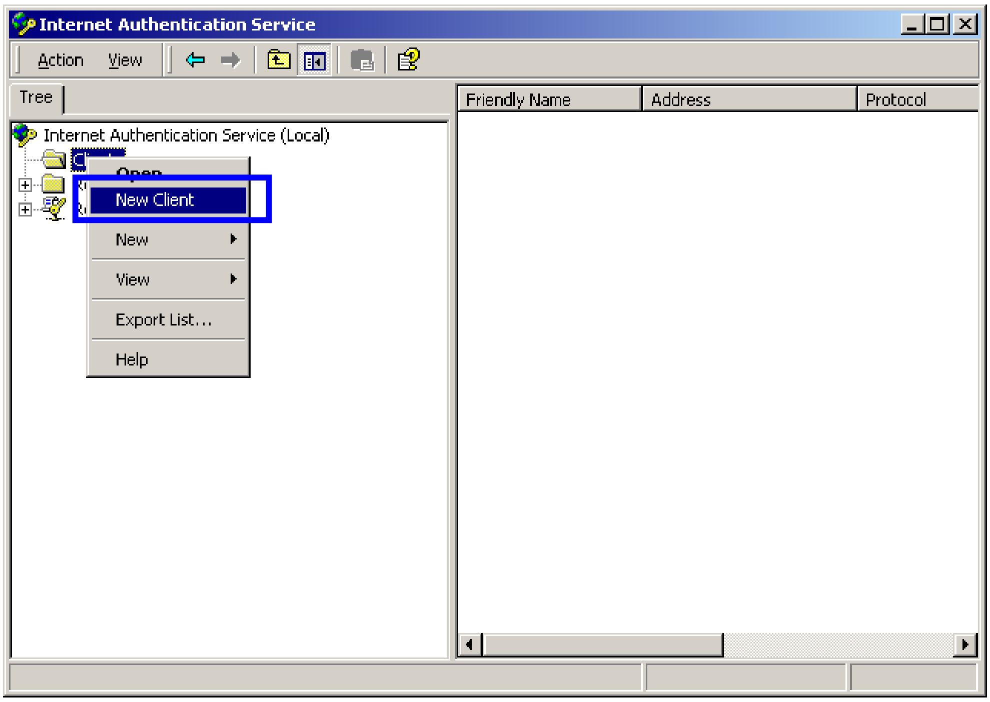
Total disk space required: 0.4 MB

Space available on disk: 8462.6 MB

Setting Internet Authentication Service

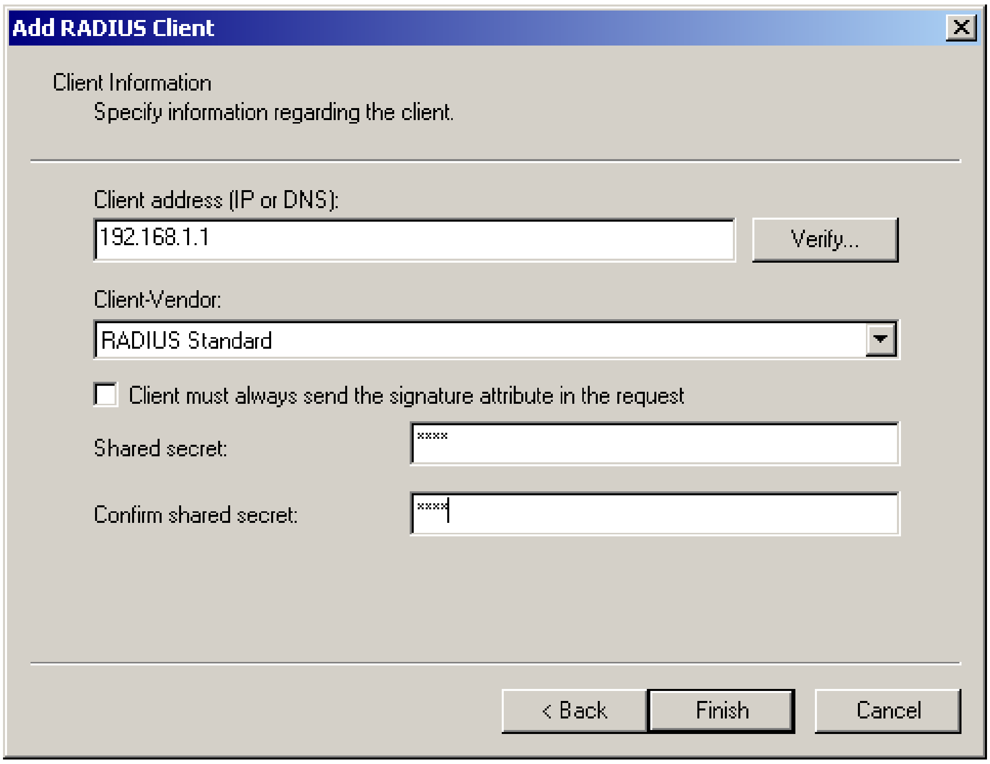
24. Go to Start > Program > Administrative Tools > **Internet Authentication Service**

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

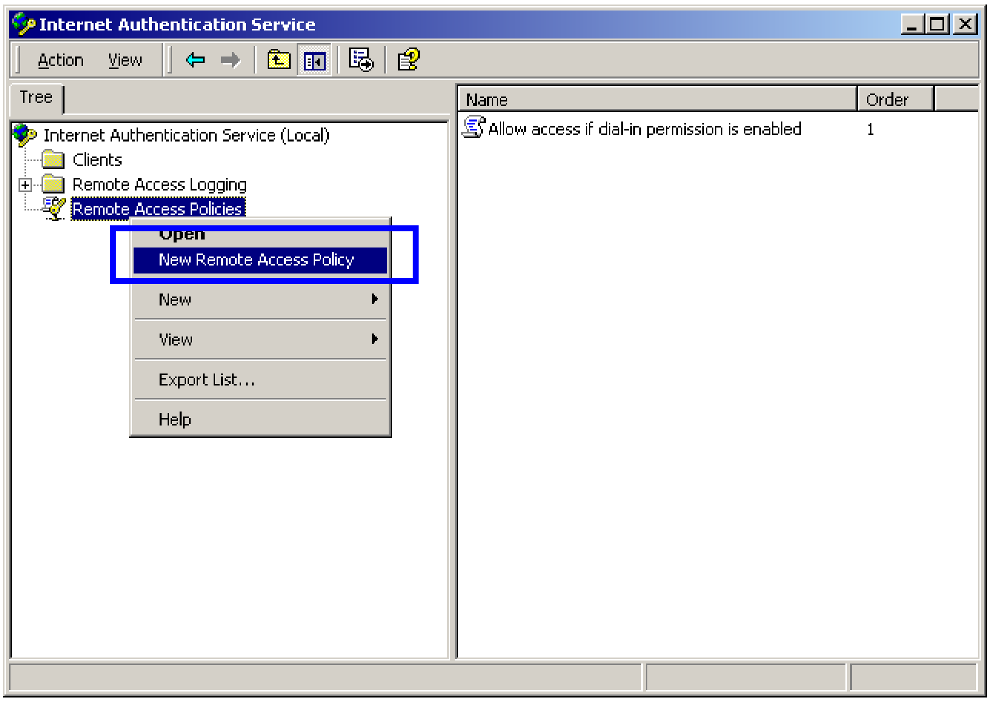
□ Client must always send the signature attribute in the request

Shared secret: ****

Confirm shared secret: ****

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

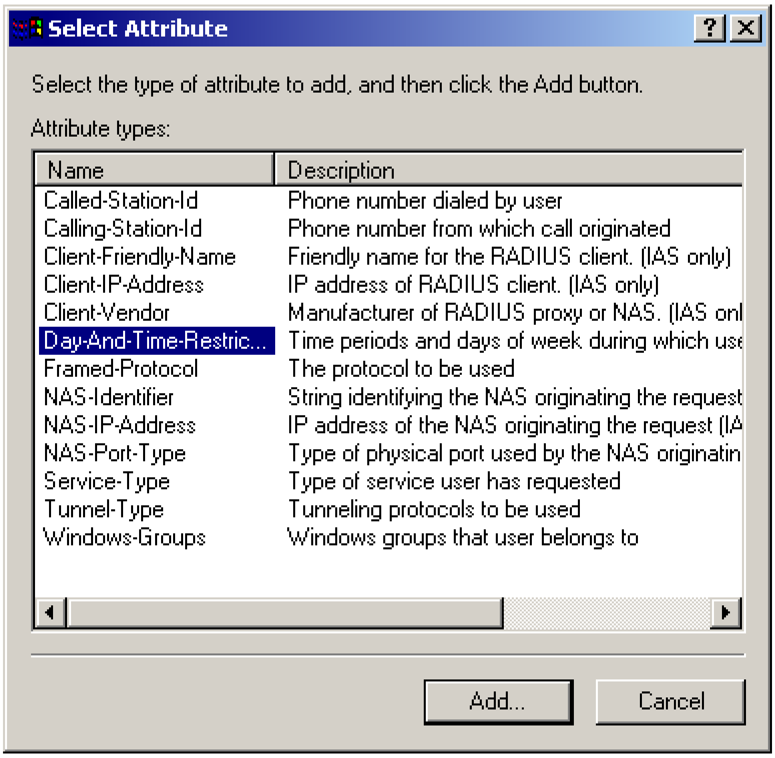
29. Select "New Remote Access Policy".



Internet Authentication Service

Name	Order
Allow access if dial-in permission is enabled	1

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



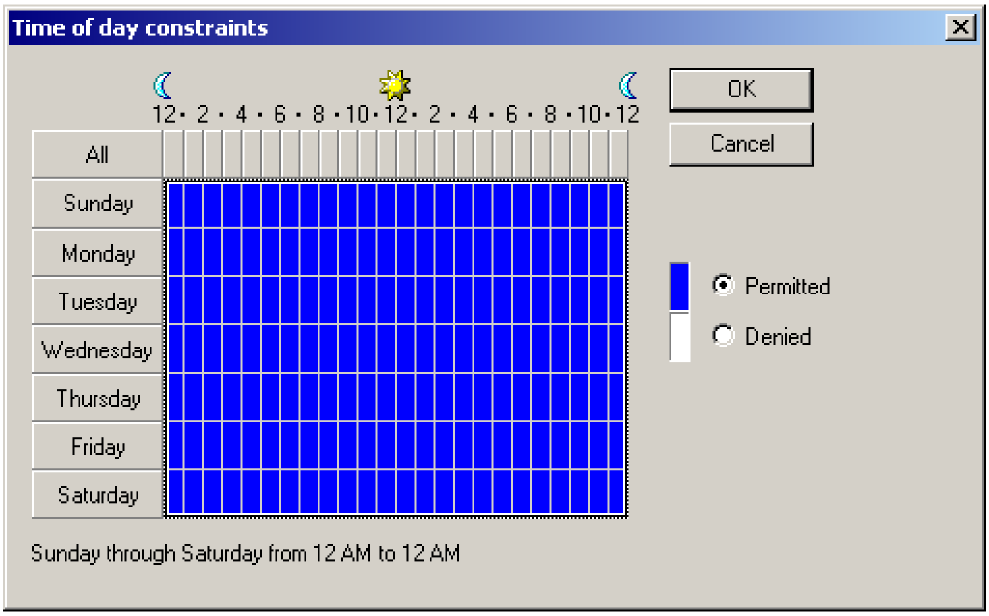
Select Attribute

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.



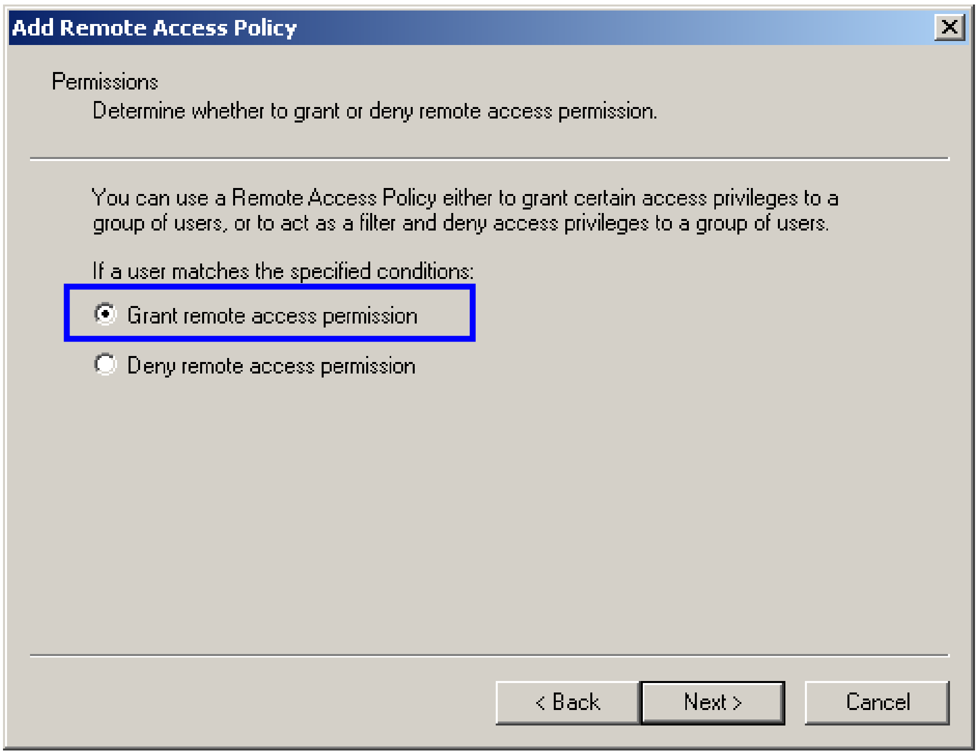
Time of day constraints

● Permitted

○ Denied

Sunday through Saturday from 12 AM to 12 AM

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


Add Remote Access Policy

Permissions

Determine whether to grant or deny remote access permission.

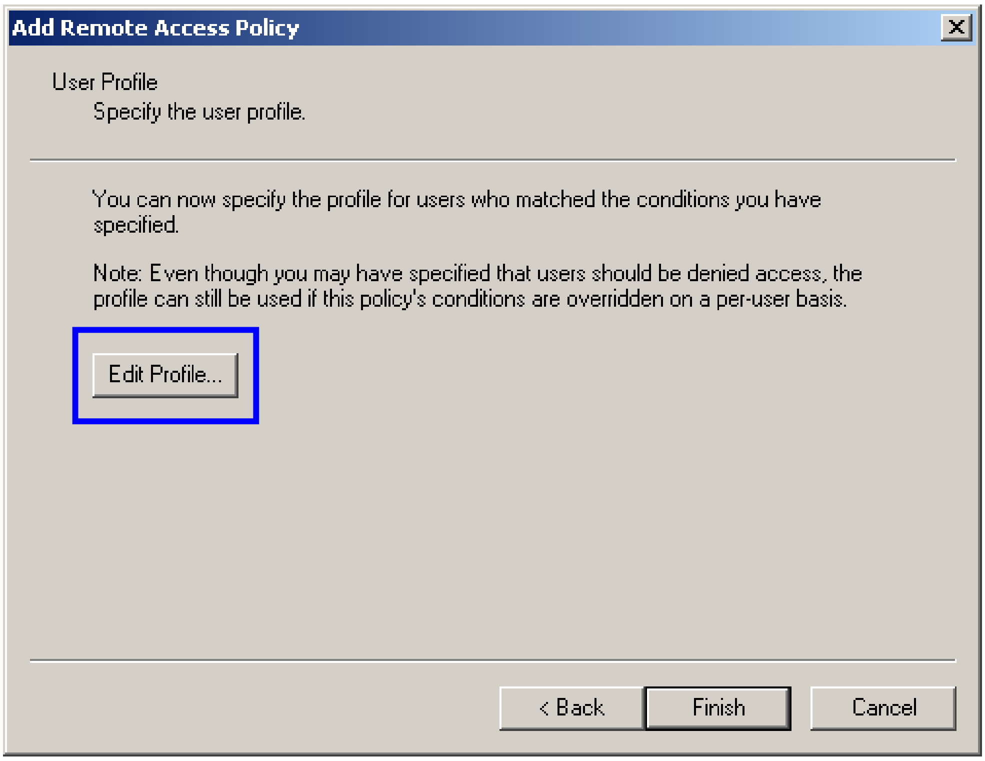
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.

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.

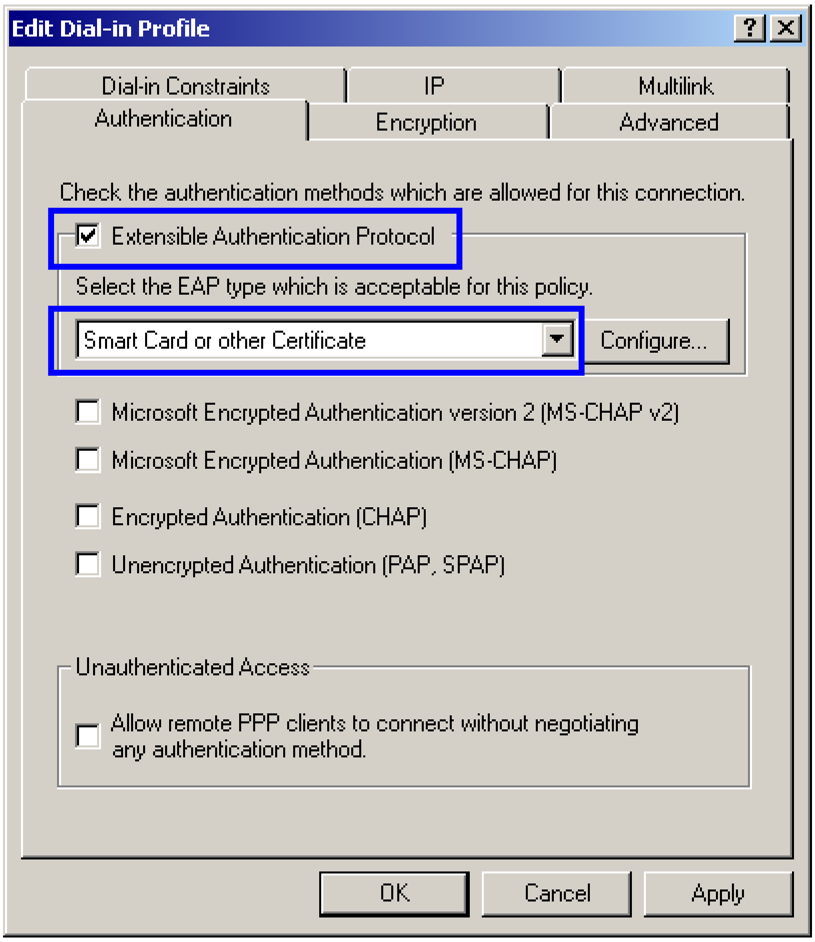
You can now specify the profile for users who matched the conditions you have specified.

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



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)

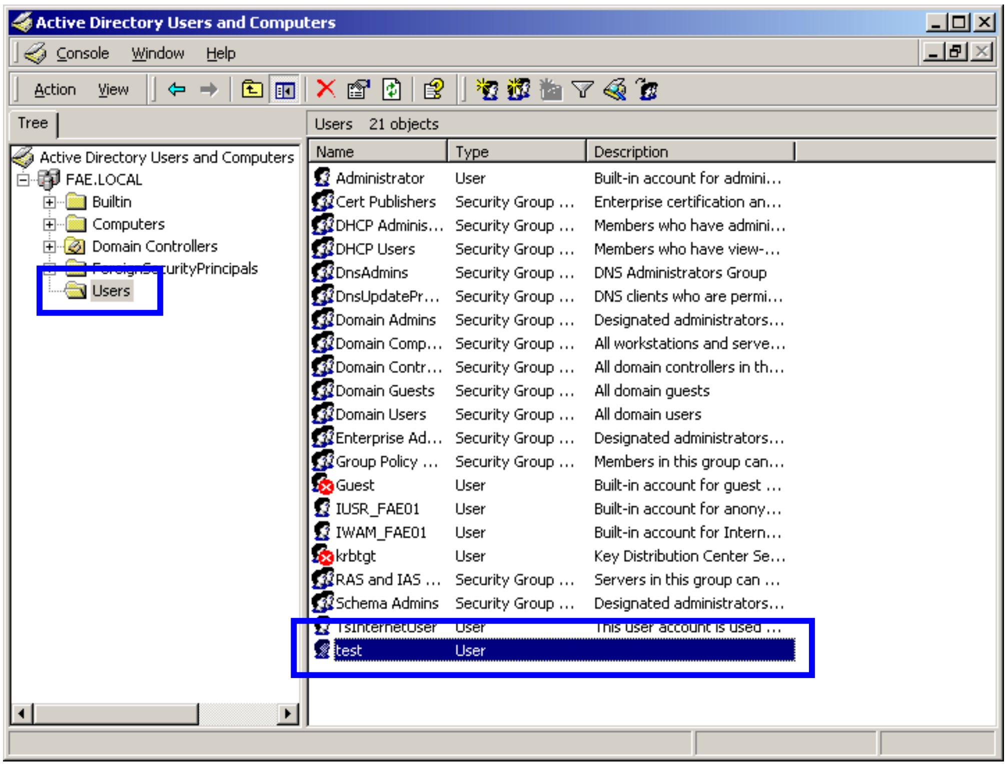
□ Unencrypted Authentication (PAP, SPAP)

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 rights to obtain digital certificate remotely.



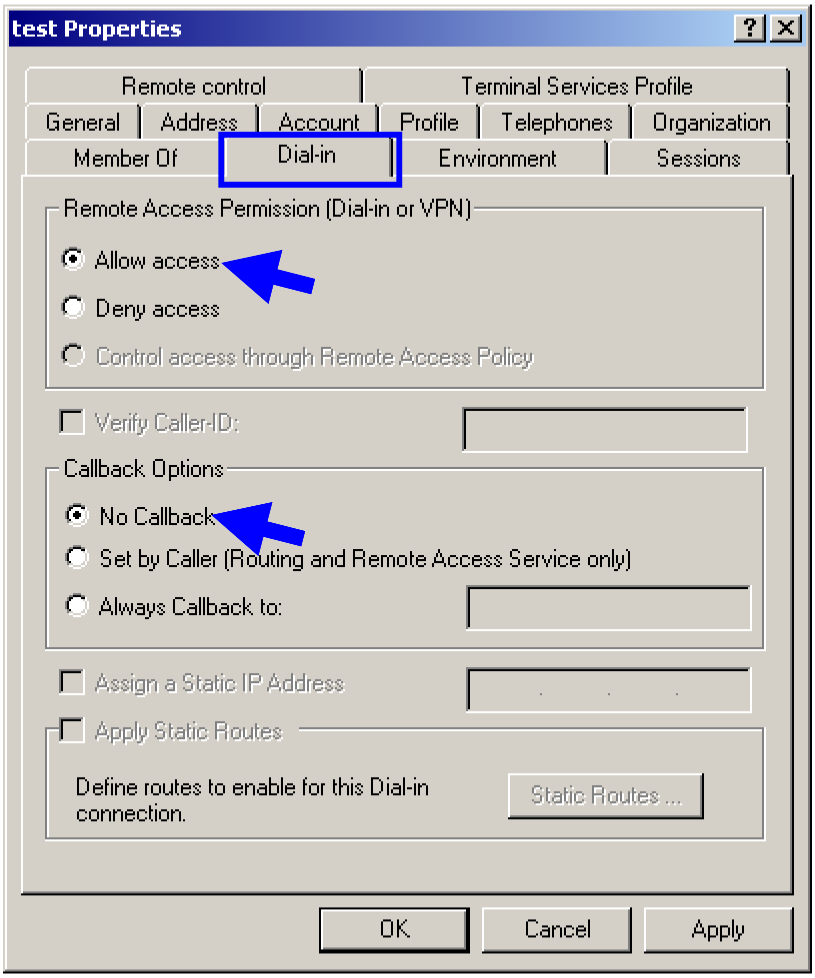
Active Directory Users and Computers
Console Window Help
Action View
Tree
Active Directory Users and Computers
FAE.LOCAL
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

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 Callback**” for Callback Options.



test Properties

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

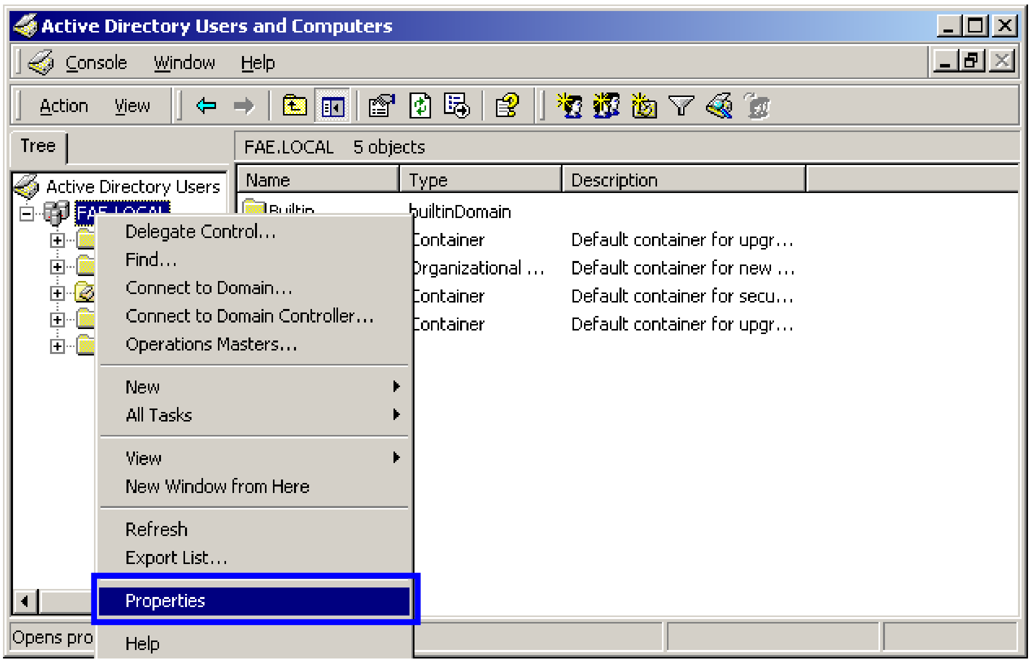
□ Apply Static Routes

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.**

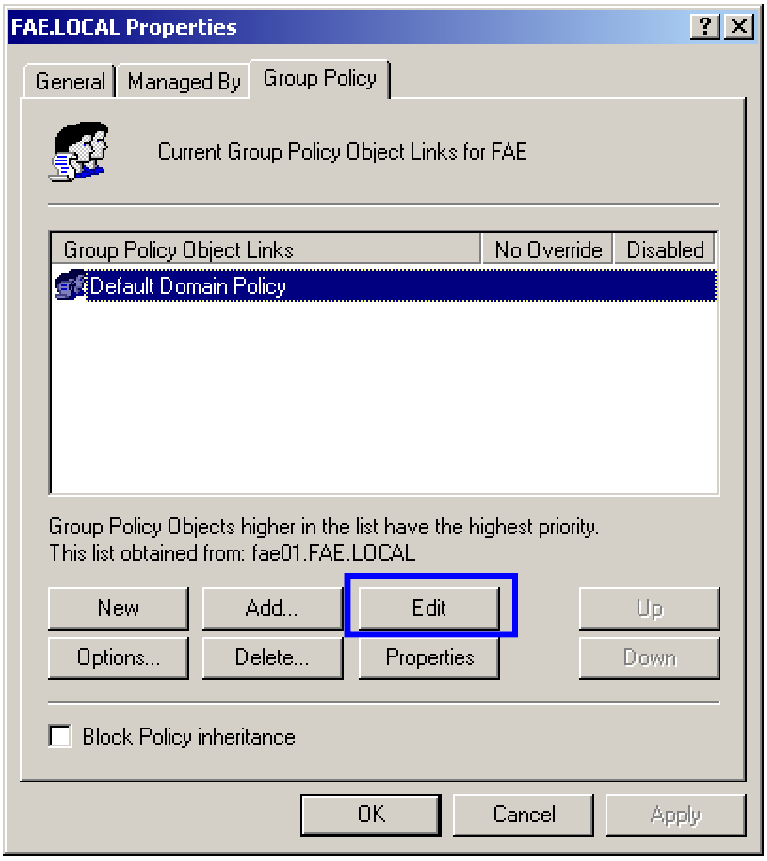
40. Right-click on the domain, and select "**Properties**"



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...

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



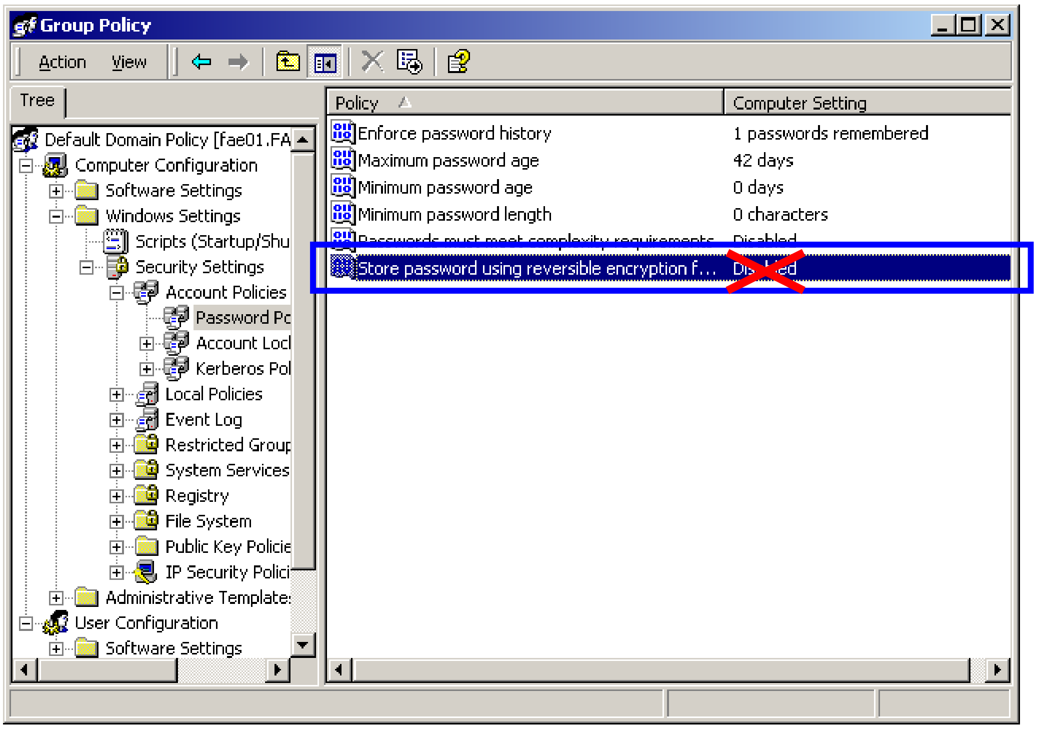
Current Group Policy Object Links for FAE

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

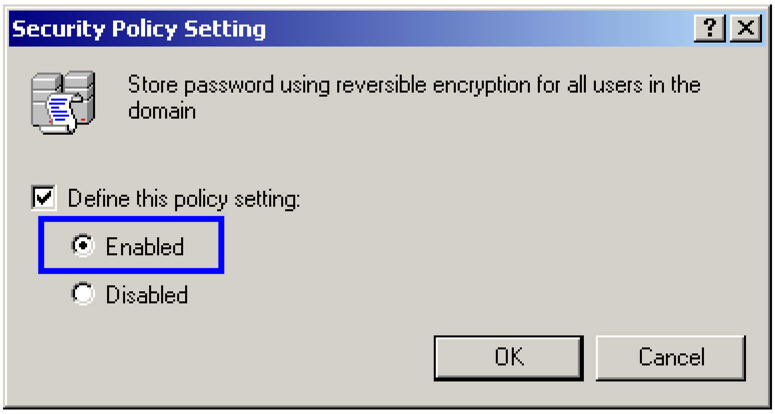
□ Block Policy inheritance

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.


Security Policy Setting

Store password using reversible encryption for all users in the domain

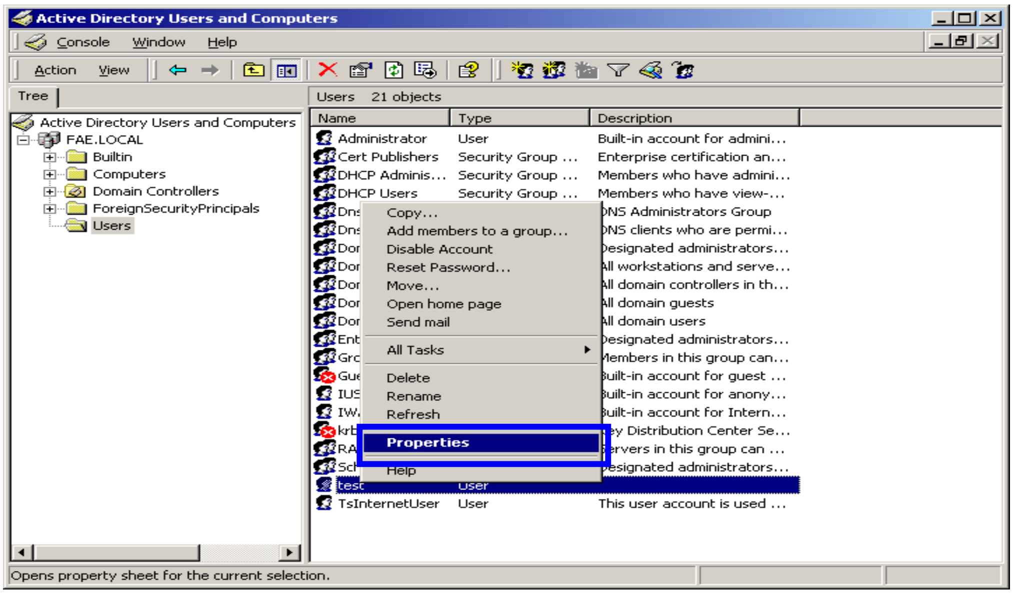
☑ Define this policy setting:

● 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**"

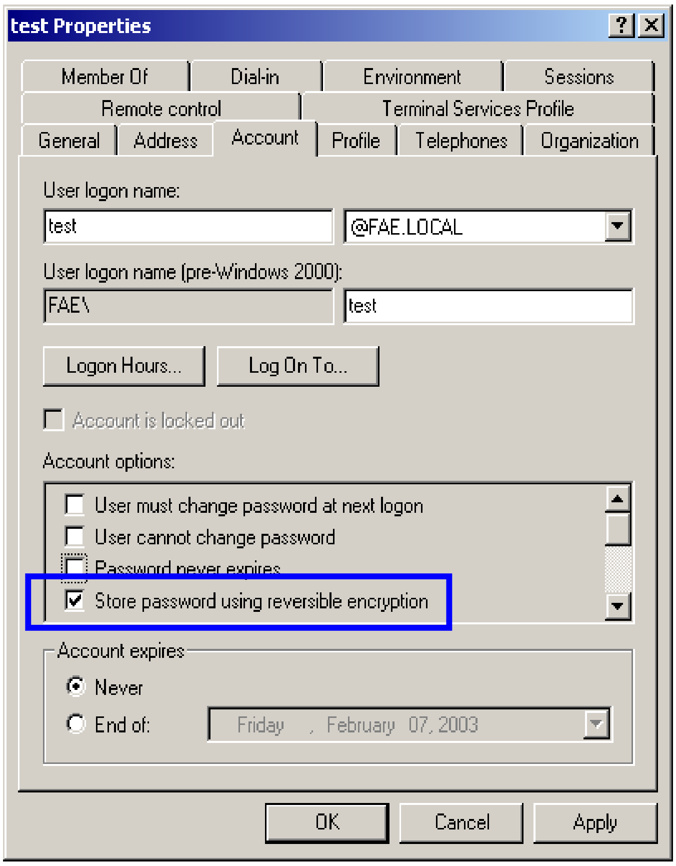


Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Enterprise certification an...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
Dns		NS Administrators Group
Dns		NS clients 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		y Distribution Center Se...
RA		rvers in this group can ...
Scl		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

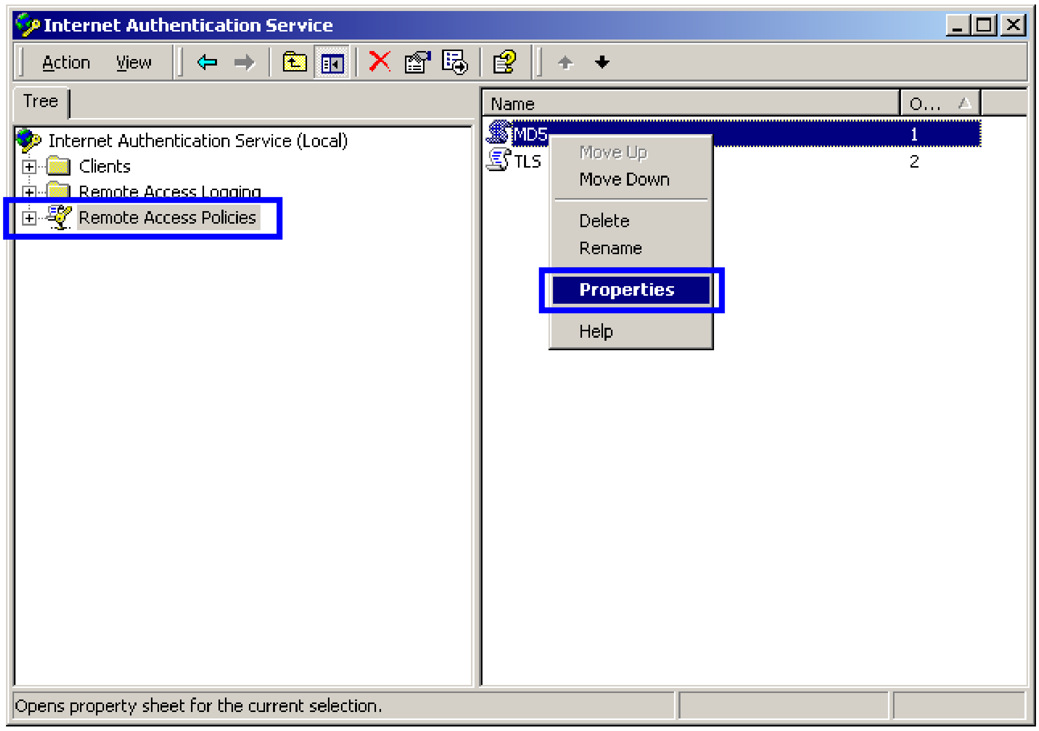
Account expires
● Never
○ End of: Friday , February 07, 2003

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

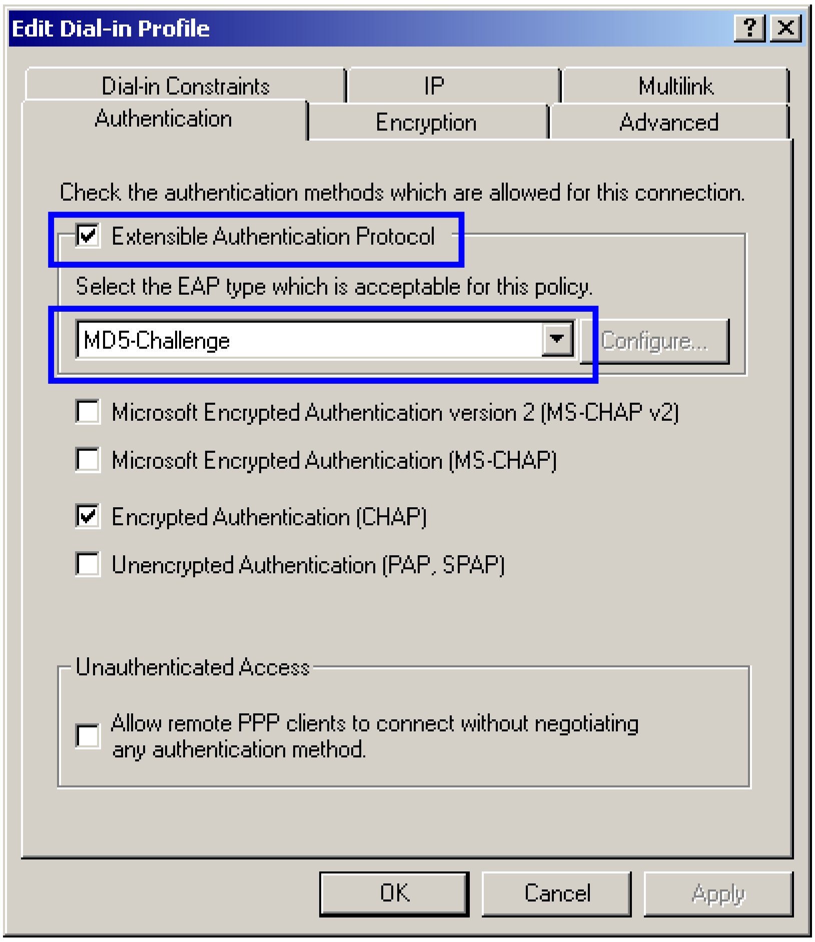
51. Right-click "**MD5**", and select "Properties"



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

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

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



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.

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.