22Mbps Wireless Network Access Point User Manual

V 3.0

Manufacturer's Disclaimer Statement

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

FCC STATEMENT

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Radiation Exposure Statement

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

TABLE OF CONTENTS

INTRODUCTION

The Wireless Access Point delivers enhanced IEEE 802.1b high performance for up to 22mbps, which is double of that offered by most of the Access Points in the current market.

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

The 22mbps Wireless Access Point is fully compatible with other 11mbps wireless devices. The easy-to-use web based configuration utility is independent of operation systems, and can be accessed through most of the web browsers that are Javascript enabled.

The enhanced functions offered by the Wireless Access Point, e.g., DHCP server and 4 different operation modes, allow the users to share resources and information, e.g., files and printers, and enjoy the freedom of networking wirelessly.

The 22mbps Wireless Access Point is an ideal wireless device for SOHO and small office, which can also be integrated to large networks as well. Please take a moment to read through this manual and get acquainted with our 22mpbs Wireless Access Point.

Product Features

- Fully compatible with IEEE 802.11b standard for wireless and 802.3 for LAN connection.
- Interoperable with existing IEEE 802.11b standard devices.
- Supports new data modulation PBCC technology from Text Instrument, which allows high data with double speed of right up to 22mbps.
- 20% more transmitting and receiving coverage supported by PBCC modulation.
- 4X mode achieving real throughput of over 12Mbps is available.
- Supports auto data rate fallback under noisy environment or longer distance.
- Enhanced security on WEP encryption from 64, 128 to a maximum of 256 bits.
- Supports 802.1x to further ensure wireless network security.
- Built-in DHCP server
- 4 AP operating modes available to fulfill your needs:
  1. AP
  2. AP Client
  3. AP Bridge (Point-to-Point and Multi-Point)

4. Repeater

- Easy setup and installation with web-based configuration utility.
- AP management utility running on PC to make it easy to manage and configure all the AP in the same network.

System Requirements

- Windows 95, 98, 98SE, Millennium, NT, 2000 and XP computers
- Internet Explorer 5.5 or higher
- One CD-ROM drive
- At least one RJ-45 Ethernet network adapter installed

GETTING STARTED

Getting To Know The Wireless Network Access Point

WIRELESS NETWORK ACCESS POINT'S PORTS

- Power Receptor
- Reset Button
- MDII RJ-45 Ethernet Port
  - Straight-Through cable is required to connect with router or switch.
  - Cross-Over cable is required to connect to computer directly

WIRELESS NETWORK ACCESS POINT'S LEDS

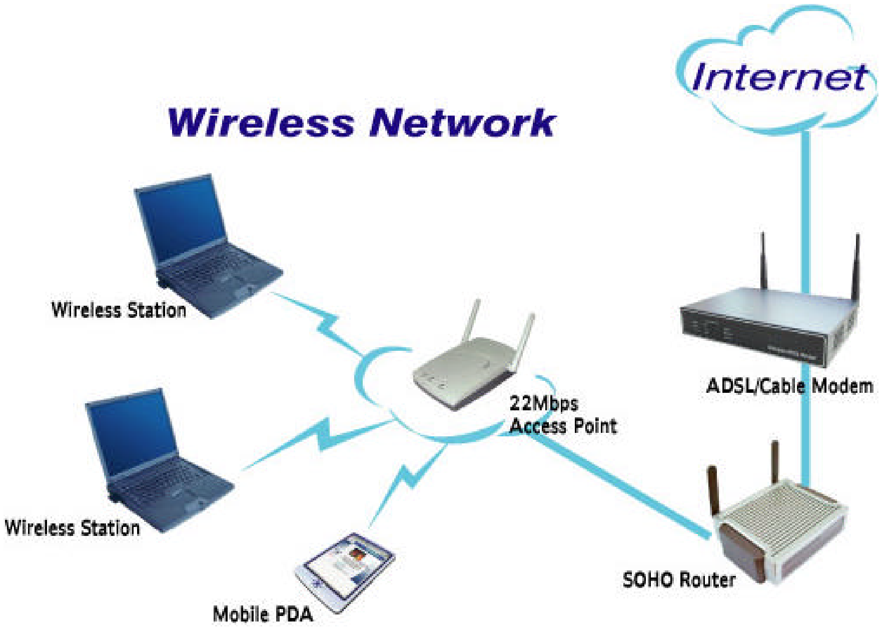
- Power LED

  ON when the unit is powered up
- LAN LED

  ON indicates LAN connection; blink indicates LAN activity
- WLAN LED

  ON indicates WLAN is working; blink indicates wireless activity

Connecting The Wireless Network Access Point



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

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

Setting Up The Wireless Network Access Point

The 22mbps Access Point is designed to be working right out of the box. Any changes of the default settings can be easily made through the web-based configuration menu using web browser, such as Internet Explorer. Please go through this chapter carefully for the Access Point setup.

CONFIGURING YOUR WIRELESS ACCESS POINT

The web-based configuration menu provides user friendly graphic design for easy configuration. Please go through the following check list before you consider using the configuration menu.

1. You will need a JavaScript enabled web browser such as Internet Explorer v5.5 or higher and Netscape v4.0 or higher.
2. The Ethernet network adapter must be working properly. Please refer to Troubleshooting section for details.
3. If you are connecting the Access Point through a router or a local area network, which has DHCP server enabled, you will not need to assign a static IP address to the computer that you are using to configure the Access Point. Please go to check item no. 6
4. If you are not connecting the Access Point through a router or a local area network, which has DHCP server enabled, you will need to assign a static IP address to the computer that you are using to configure the Access Point.
5. The IP address assigned to the computer that you are using to configure the Access Point must be in the same IP address range as Access Point ’s. Please refer to Networking Basis section to learn more about assigning IP address.
6. The power jack must be properly inserted to make sure that the Access Point is powered.

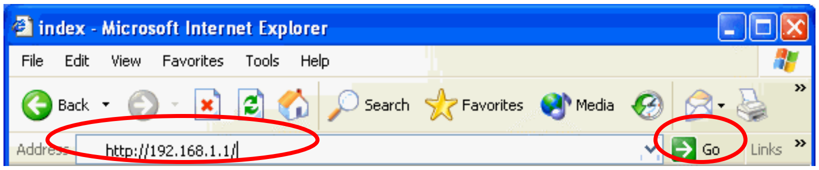
The Default Settings of the 22mbps Access Point:

IP Address	192.168.1.1
User Name	admin
Password	admin
ESSID	wireless
Channel	6
WEP	disabled

Configuration Menu

You can access the configuration menu anytime by opening up an web browser window, and type in the IP address of the Access Point. The default IP address of the Access Point is shown below.

Open web browser window
Type in IP address
Press "Enter" or "Go"

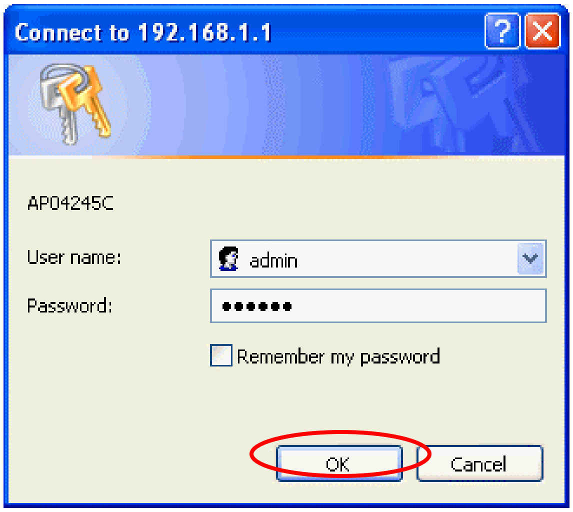

index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links

Address: http://192.168.1.1/

Note! The IP address shown above is the default IP address for the Access Point. Use this IP address when connecting to a network consisting of Access Points set to default settings. If the IP address of the Access Point is being changed to comply with the network, then type in the IP address in the Address field of the web browser, instead of the default IP address.

Type in "user name"
Type in "password"

Click "**OK**"



Connect to 192.168.1.1

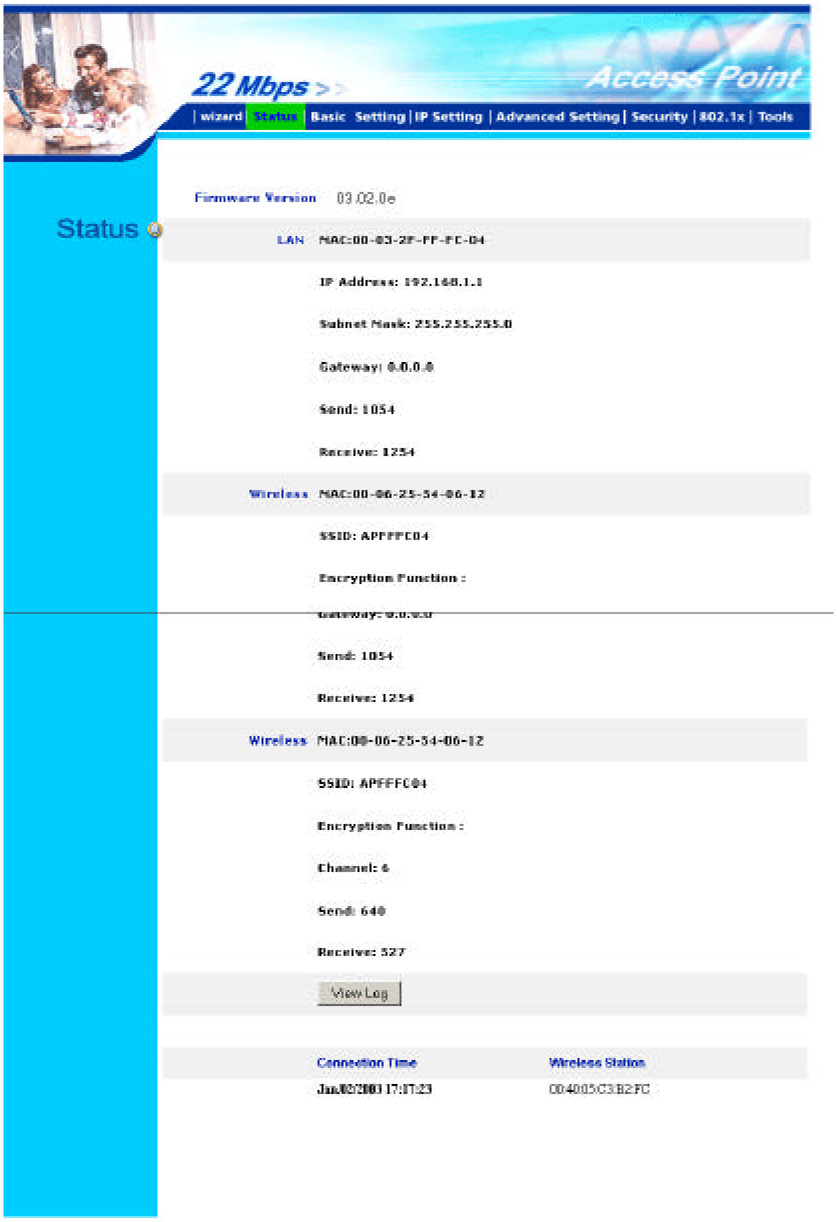
AP04245C

User name: admin

Password: ••••••

□ Remember my password

Note! The default username is “admin” and the default password is also “admin”. The configuration menu will appear. You can configure and get information about the Access Point by going through each tab. Here **Status** page is displayed.



Firmware Version 03.02.0e

LAN MAC:00-03-2F-FF-FC-04

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Send: 1054

Receive: 1254

Wireless MAC:00-06-25-54-06-12

SSID: APFFFC04

Encryption Function :

Gateway: 0.0.0.0

Send: 1054

Receive: 1254

Wireless MAC:00-06-25-54-06-12

SSID: APFFFC04

Encryption Function :

Channel: 6

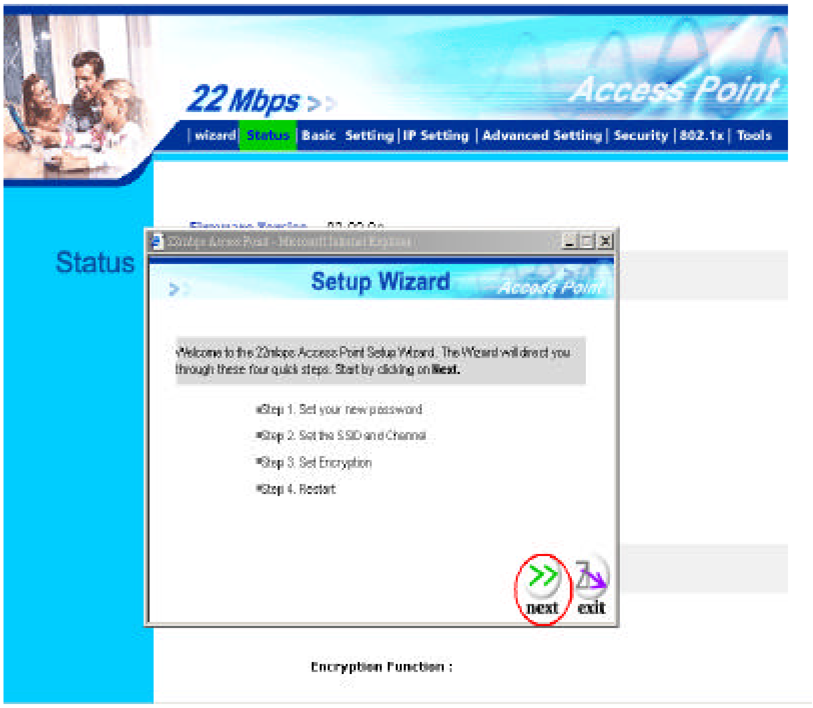
Send: 640

Receive: 527

Connection Time	Wireless Station
Jan/02/2003 17:17:23	00:40:05:C3:B2:FC

Getting Started With Setup Wizard

Setup wizard is provided as part of the web configuration utility. You can simply follow the step-by-step process to get your Access Point configured and ready for running in 4 easy steps by clicking on the "**Wizard**" button on the function menu. The following screen w ill appear. Please click "**Next**" to continue.


22 Mbps
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
Status
Setup Wizard
Access Point
next
exit
Encryption Function :

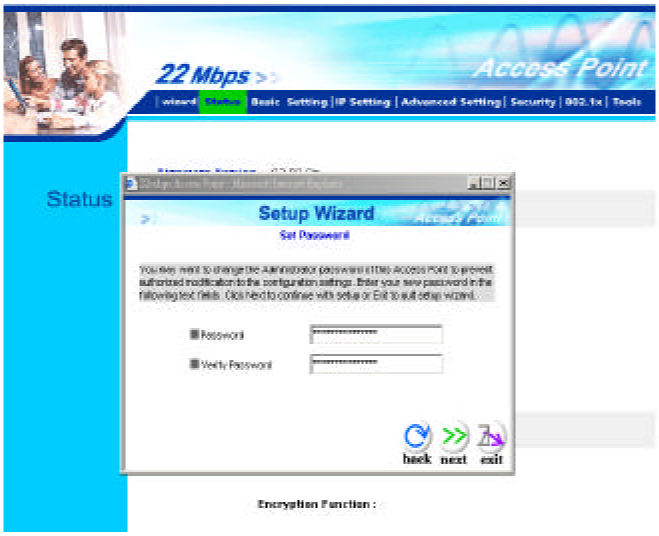
Welcome to the 22mbps Access Point Setup Wizard. The Wizard will direct you through these four quick steps. Start by clicking on **Next.**

- Step 1. Set your new password
- Step 2. Set the SSID and Channel
- Step 3. Set Encryption
- Step 4. Restart

Step 1: Set Password

The Access Point is password protected to prevent unauthorized modification to your configuration. You can change to new password if you wish, otherwise simply click "**Next**" to continue.

After entering the new password in both text boxes, click "**Next**" to continue.


22 Mbps
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
Status
Setup Wizard
Access Point
back
next
exit
Encryption Function :

Set Password

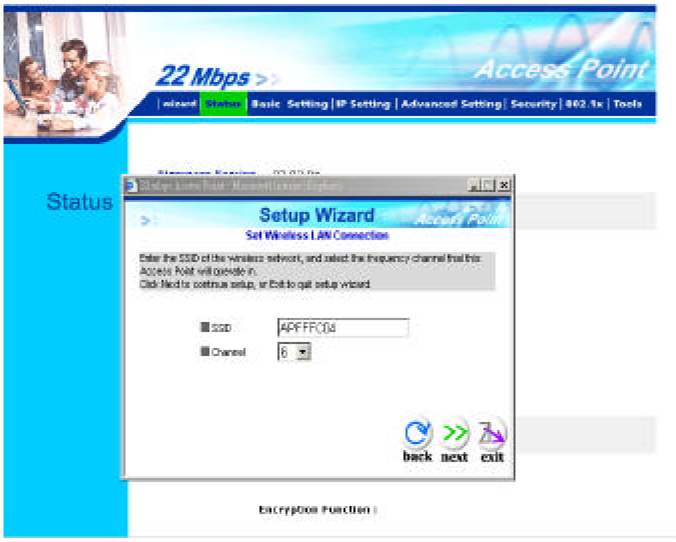
You may want to change the Administrator password of this Access Point to prevent authorized modification to the configuration settings. Enter your new password in the following text fields. Click Next to continue with setup or Exit to quit setup wizard.

Password: ****************

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

Step 2: Set WLAN Connection

Enter the SSID that you would like to use and select the channel of operation, then click “**Next**” to continue.


22 Mbps
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
Status
back
next
exit
Encryption Function :

Setup Wizard

Set Wireless LAN Connection

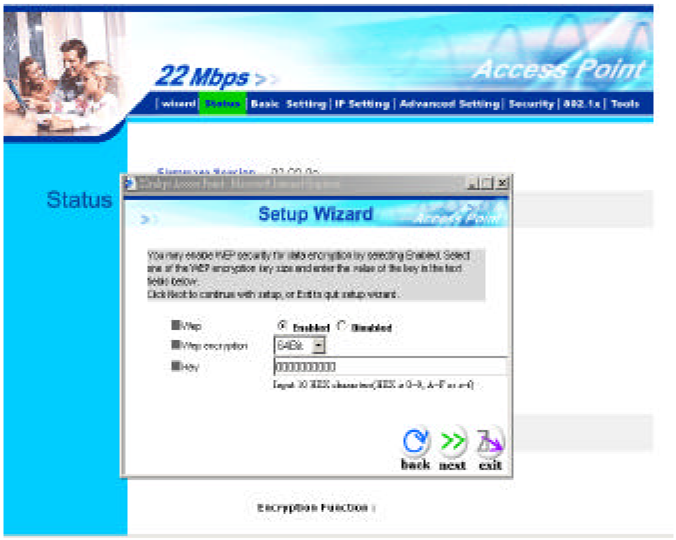
Enter the SSID of the wireless network, and select the frequency channel that this Access Point will operate in.
Click Next to continue setup, or Exit to quit setup wizard.

SSID: APFFFC04

Channel: 6

Step 3: Set WEP Encryption

You may enable the WEP security by selecting “**Enabled**”, otherwise, simply click “**Next**” to continue Select one of the WEP encryption key size and enter the value of the key in the Key text box, then click “**Next**” to continue.


22 Mbps
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
Status
back
next
exit
Encryption Function :

Setup Wizard

You may enable WEP security for data encryption by selecting Enabled. Select one of the WEP encryption key size and enter the value of the key in the text fields below.
Click Next to continue with setup, or Exit to quit setup wizard.

Wep: ● Enabled ○ Disabled

Wep encryption: 64Bit

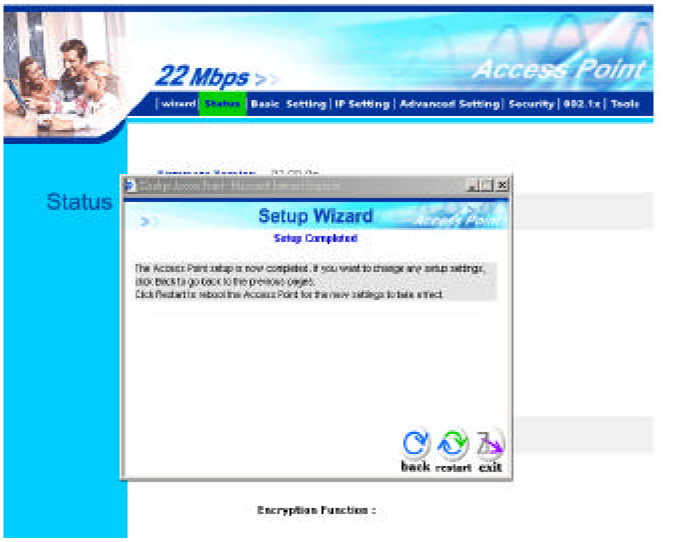
Key: 0000000000

Input 10 HEX characters(HEX is 0-9, A-F or a-f)

Note! There are 3 key sizes to choose from, 64, 128 and 256 Bit, however 256 Bit will only be supported with 22Mbps series products.

Step 4: Restart

The Setup wizard is now completed. The new settings will be effective after the Access Point restarts. Click “**Restart**” to reboot the Access Point.

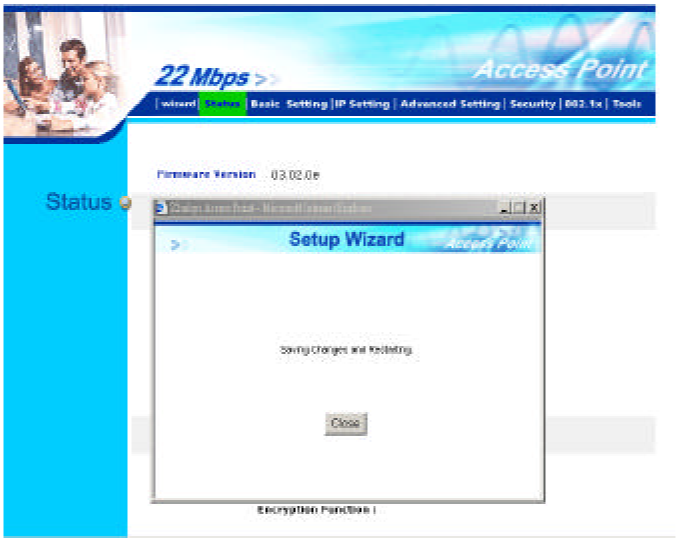

22 Mbps
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
Status
back
restart
exit
Encryption Function :

Setup Wizard

Setup Completed

The Access Point setup is now completed. If you want to change any setup settings, click Back to go back to the previous pages.
Click Restart to reboot the Access Point for the new settings to take effect.

The Access Point is now rebooting, click “**Close**” to close the Setup wizard window and go back to the main menu.


22 Mbps
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
Status
Setup Wizard
Access Point
Close

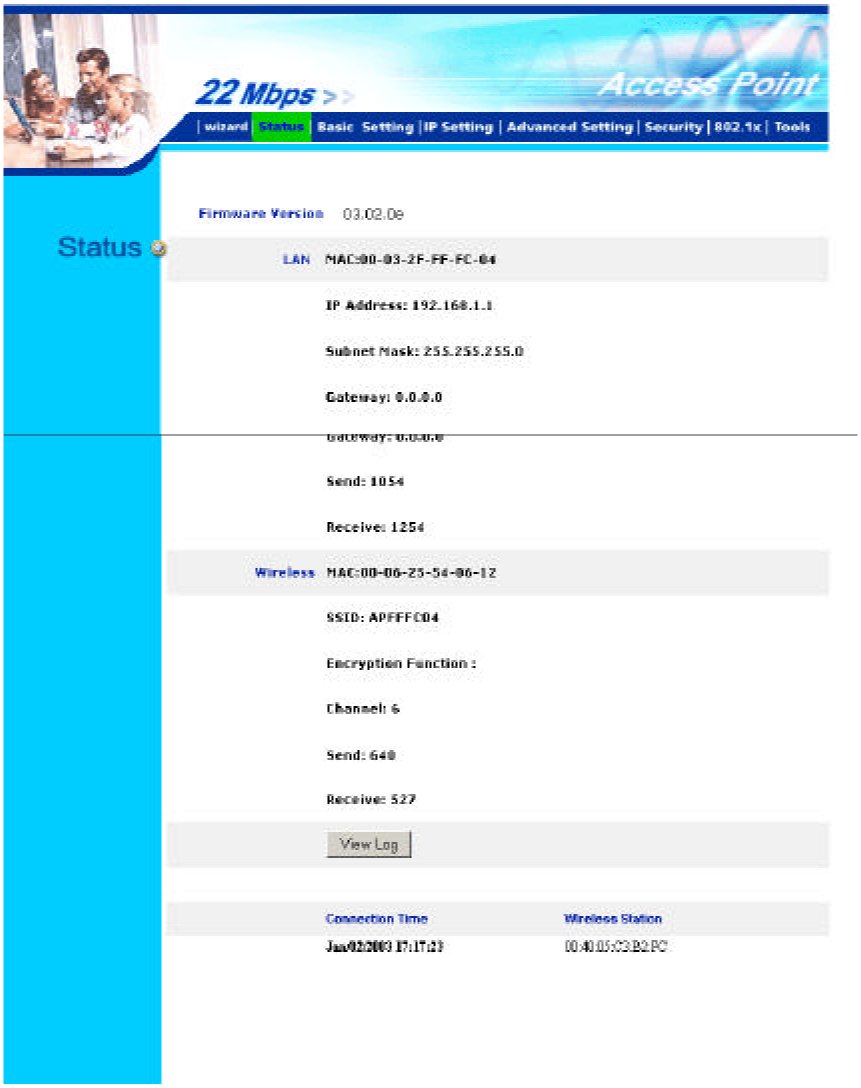
Firmware Version 03.02.0e

Saving Changes and Restarting

Encryption Function :

Status Page

This page displays the following information.


22 Mbps
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
Status
View Log

Firmware Version 03.02.0e

LAN MAC:00-03-2F-FF-FC-04

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Gateway: 0.0.0.0

Send: 1054

Receive: 1254

Wireless MAC:00-06-25-54-06-12

SSID: APFFFC04

Encryption Function :

Channel: 6

Send: 640

Receive: 527

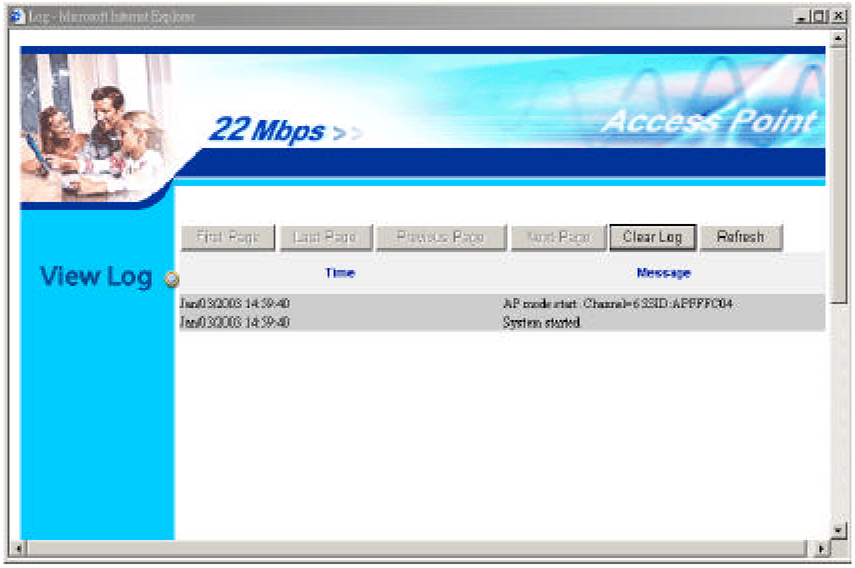
Connection Time	Wireless Station
Jan/02/2003 17:17:23	00:40:05:C3:B2:FC

Firmware Version: Shows the current firmware version

LAN: Shows the Mac address, IP address (default: 192.168.1.1), Subnet Mask, Gateway Address. The current LAN traffic calculated in terms of number of packets sent and received by AP through wired connection is also displayed.

Wireless: Shows the Mac address, current ESSID, the status of Encryption Function (Enable or Disable), the current using channel. The current wireless traffic calculated in terms of number of packets sent and received by AP through wireless communication is also displayed.

View Log: Upon clicked, the page will change to log page. The log page records every event and the time that it happens.

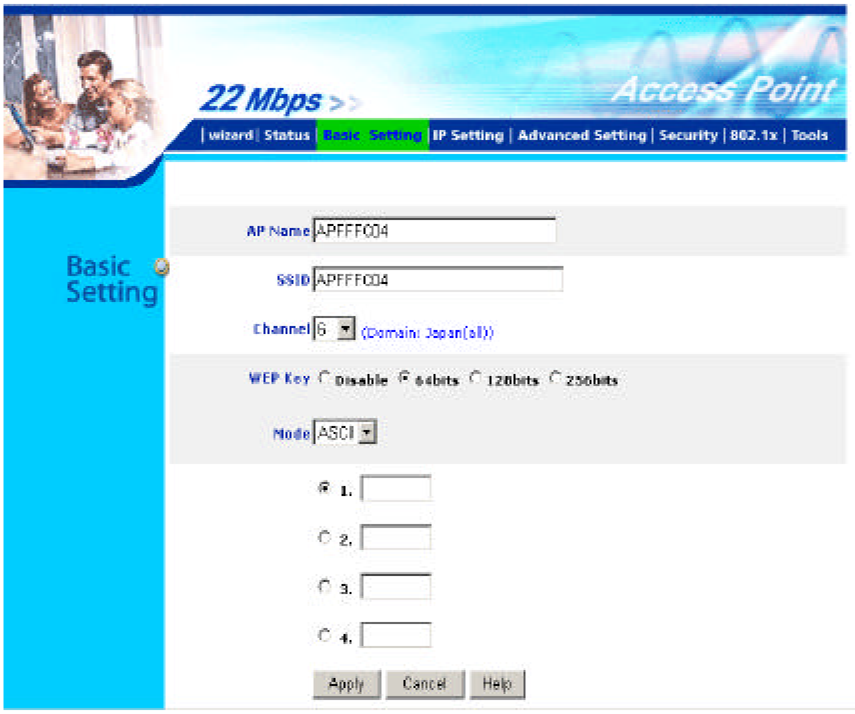


Time	Message
Jan/03/2003 14:59:40	AP mode start : Channel=6 SSID:APFFFC04
Jan/03/2003 14:59:40	System started

You may clear the entries recorded in the log by clicking the "**Clear Log**" button, and refresh the screen to show the latest log entries by clicking the "**Refresh**" button.

Basic Setting

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


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

AP Name APFFFC04

SSID APFFFC04

Channel 6 (Domain: Japan(all))

WEP Key ○ Disable ● 64bits ○ 128bits ○ 256bits

Mode ASCI

● 1.

○ 2.

○ 3.

○ 4.

AP Name: Name of the AP, which can be used to identify the Access Point among the all the Access Points in the wireless network.

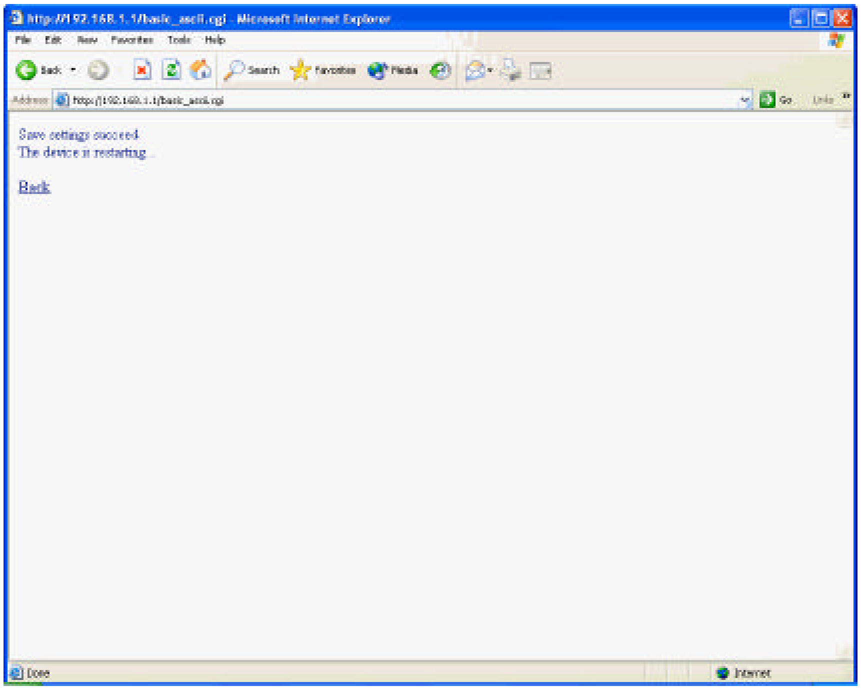
SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless networ k. The SSID must be identical for each clients and nodes in the wireless network.

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

WEP Key: To disable WEP security, click on the "Disable" option. To enable WEP security, there are 3 type of WEP keys to choose from, 64bits, 128bits and 256bits. When one of the 3 WEP key options is selected, you must enter the va lue of one of the four Keys in ASCII or HEX format. You can also enter the values for all four WEP keys, and select one to use.

Note! When AP's WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.

For the changes made to any of the items above to be effective, click "Apply".


http://192.168.1.1/basic_ascii.cgi - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://192.168.1.1/basic_ascii.cgi
Go
Links
Done
Internet

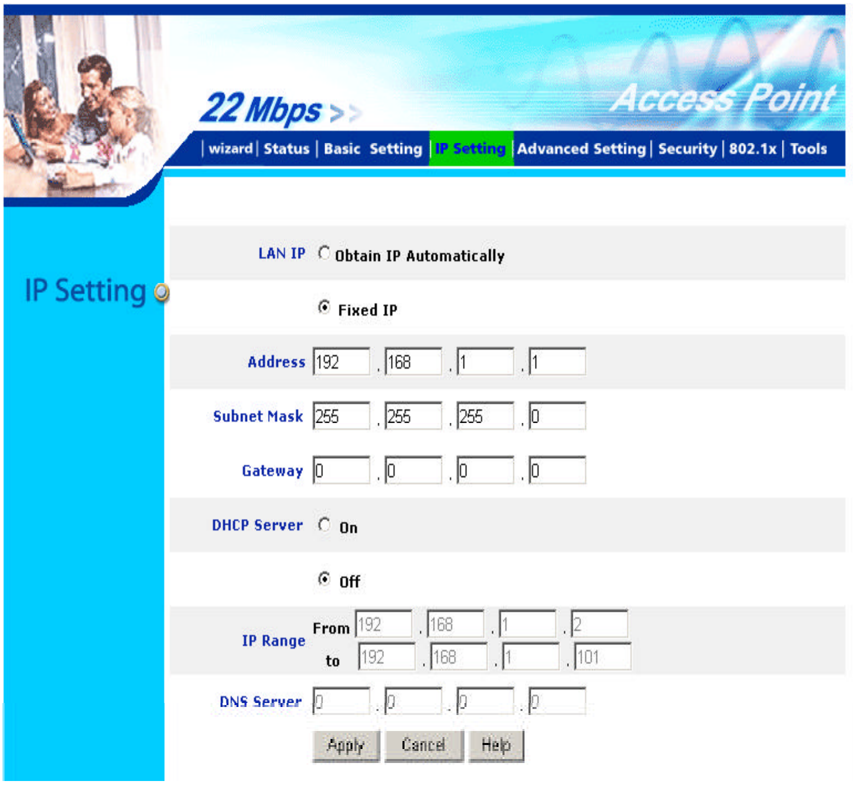
Save settings succeed.
The device is restarting...

Back

The new settings are now been saved to Access Point and will be effective once the Access Point restarts.
Click "**Back**" to go back to Basic Setting page.

IP Setting

This is the page where you configure the IP and DHCP settings of the Access Point.


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

LAN IP ○ Obtain IP Automatically

● Fixed IP

Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

Gateway 0 . 0 . 0 . 0

DHCP Server ○ On

● Off

IP Range From 192 . 168 . 1 . 2

to 192 . 168 . 1 . 101

DNS Server 0 . 0 . 0 . 0

The default IP address of the Access Point is 192.168.1.1 with the Subnet Mask of 255.255.255.0. You can type in other values for IP Address, Subnet Mask and Gateway and click “**Apply**” button for the changes to be effective.

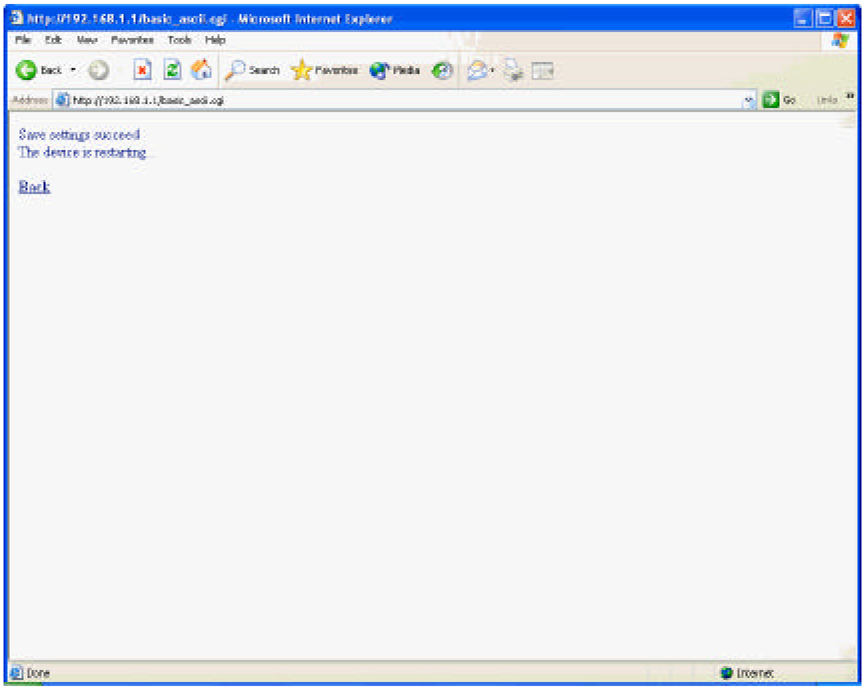
You can also set the Access Point to obtain the IP from a DHCP server, but it is not recommended. Once set, it will be difficult to determine the dynamic IP assigned to the Access Point. Select the option “Obtain IP Automatically” and click “**Apply**” button for the changes to be effective.

DHCP Server:

It’s not recommended to enable the DHCP Server if you have a DHCP server running in your LAN network, for it will cause possible IP assignment conflict.

Enable the DHCP server function by selecting the option “On”, and enter the IP range.

Click “**OK**” to close pop-up box. Click “**Apply**” for the changes to be effective.


http://192.168.1.1/basic_ascii.cgi - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.1.1/basic_ascii.cgi
Go
Links
Done
Internet

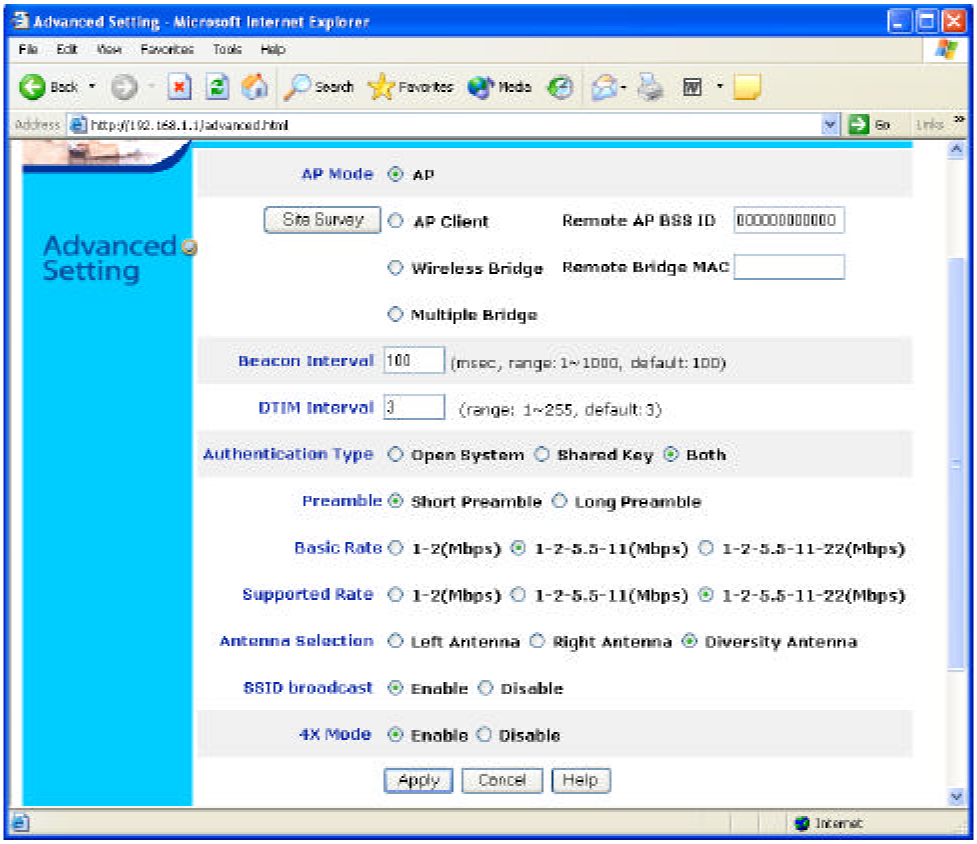
Save settings succeed
The device is restarting

Back

The new settings are now been saved to Access Point and will be effective once the Access Point restarts. Click “**Back**” to go back to Basic Setting page.

Advanced Setting

This page contains configurations for advanced users, which the change will reflect the wireless performance and operating modes.


Advanced Setting - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/advanced.html
Go Links
Advanced Setting
Site Survey
Apply Cancel Help
Internet

AP Mode ● AP
○ AP Client Remote AP BSS ID 000000000000
○ Wireless Bridge Remote Bridge MAC
○ Multiple Bridge

Beacon Interval 100 (msec, range: 1~1000, default: 100)

DTIM Interval 3 (range: 1~255, default: 3)

Authentication Type ○ Open System ○ Shared Key ● Both

Preamble ● Short Preamble ○ Long Preamble

Basic Rate ○ 1-2(Mbps) ● 1-2-5.5-11(Mbps) ○ 1-2-5.5-11-22(Mbps)

Supported Rate ○ 1-2(Mbps) ○ 1-2-5.5-11(Mbps) ● 1-2-5.5-11-22(Mbps)

Antenna Selection ○ Left Antenna ○ Right Antenna ● Diversity Antenna

SSID broadcast ● Enable ○ Disable

4X Mode ● Enable ○ Disable

AP Mode:

Select one of the AP operating modes for different application of Access Point.

1. AP – The normal Access Point operating mode which forms a wireless ESS network with its wireless clients.
2. AP Client – Acts as an **Ethernet-to-Wireless Bridge**, which allows a LAN or a single computer station to join a wireless ESS network through it. You must make sure that the SSID and Channel is set to the same as that used by the AP you wish to connect.

    Remote AP BSS ID: key in the LAN Mac address (NOT wireless Mac address) of the AP that you wish to get connected.

    Please note that if you leave Mac address as 000000000000, then you will get connected by the SSID that is set in you AP.

3. Wireless Bridge – A pair of APs operating under Bridge mode to act as the bridge that connects two Ethernet networks or Ethernet enabled clients together. You must make sure that the SSID and Channel is set to the same as that used by the AP you wish to connect. The "Remote Bridge MAC" is where you enter the MAC address of the other AP that you connect to setup the wireless bridge.

   Remote Bridge MAC filed: key in the **LAN Mac address** (NOT wireless Mac address) of the AP that you wish to get connected.
4. Multiple Bridge – A group of APs which consists of two or more APs operating under Multiple Bridge mode, that can connect two or more Ethernet networks or Ethernet enabled clients together. The way that multiple bridge setup is based on the topology of Ad-Hoc mode.

Note**!** All APs have to use the same **Channel** and **SSID** in order to form a Multiple Bridge network.

Beacon Interval: To set the period of time in milliseconds that AP sends out a beacon. Default is 100 milliseconds.

RTS Threshold: To set the size of RTS/CTS packet size. Default is 2432 bytes.

Fragmentation Threshold: To set the number of bytes used for the fragmentation boundary for directed messages. Default is 2436 bytes.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.

Authentication Type: The Authentication Type default is set to Open System, and you may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type. It's recommend that you use the default setting.

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.

Basic Rate: The basic transfer rate is set depending on the speed of your wireless network. For example, you set 1-2 (Mbps) if you have older 802.11 compliant device in your network, which supports 1 ~ 2 Mbps data rate. This setting does not limit the basic transfer rates of the faster 802.11 compliant network devices.

Antenna Selection: To set the antenna for transmitting data. The default setting is Diversity Antenna, which is better for reception.

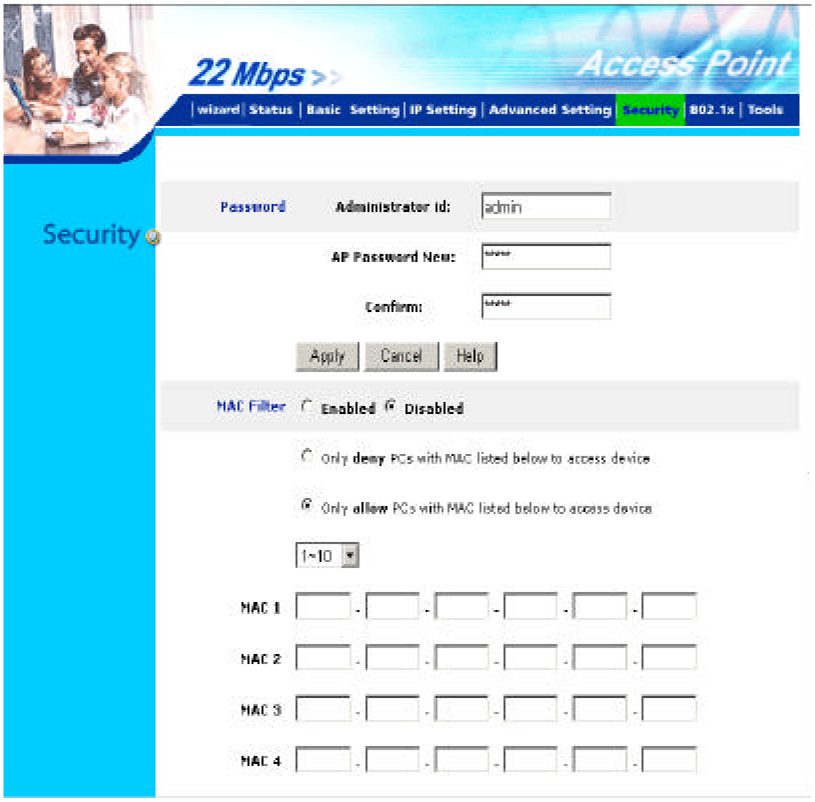
SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to communicate with the Access Point. For security purpose, you may want to disable SSID Broadcast to allow only those wireless clients with the AP's SSID to communicate with the Access Point.

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

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

Security

This page is where you configure the security features supported by this Access Point.


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

Password

Administrator id: admin

AP Password New: ****

Confirm: ****

MAC Filter ○ Enabled ● Disabled

○ Only **deny** PCs with MAC listed below to access device

● Only **allow** PCs with MAC listed below to access device

1~10

MAC 1 __ - __ - __ - __ - __ - __

MAC 2 __ - __ - __ - __ - __ - __

MAC 3 __ - __ - __ - __ - __ - __

MAC 4 __ - __ - __ - __ - __ - __

Password:

Allow you to change the new login password. Here are the necessary steps:

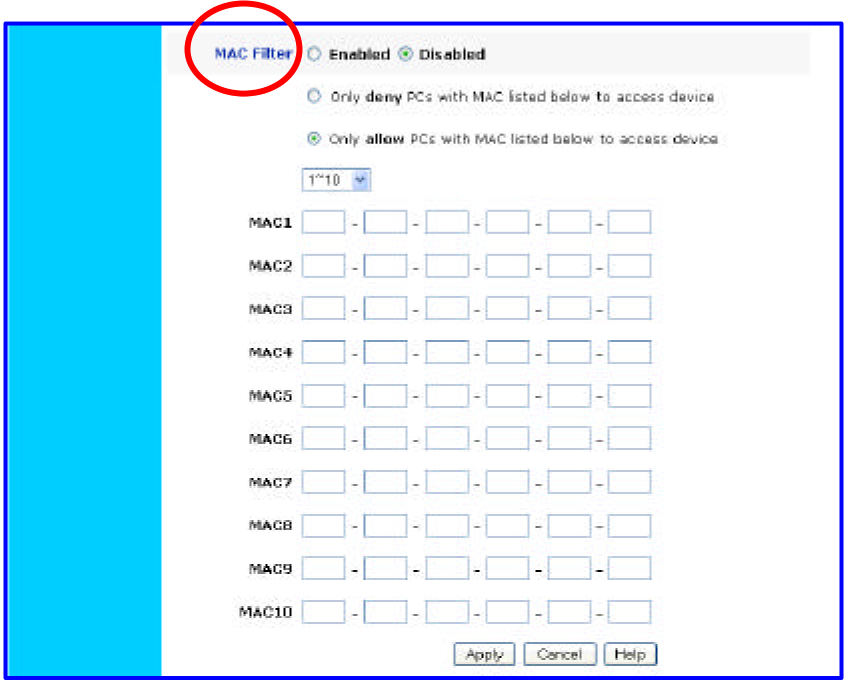
1. Enter the new password in the "**AP Password New:**" field.
2. Enter the new password again in the "**Confirm**" field.
3. Click "**Apply**"

Note**!** The wireless clients will not be able to recognize the Access Point using Site Survey utilities, such as zero configuration utility provided in Windows XP.

MAC Filter

MAC Filter function controls the MAC of the network devices that are listed in this table for access authorization or denial. When MAC Filter is enabled, by selecting the "**Enabled**" radio box, select one of two choices:

- Only deny PCs with MAC listed below to access device, or
- Only allow PCs with MAC listed below to access device



MAC Filter ○ Enabled ● Disabled

○ Only **deny** PCs with MAC listed below to access device

● Only **allow** PCs with MAC listed below to access device

1~10

MAC1 □ - □ - □ - □ - □ - □

MAC2 □ - □ - □ - □ - □ - □

MAC3 □ - □ - □ - □ - □ - □

MAC4 □ - □ - □ - □ - □ - □

MAC5 □ - □ - □ - □ - □ - □

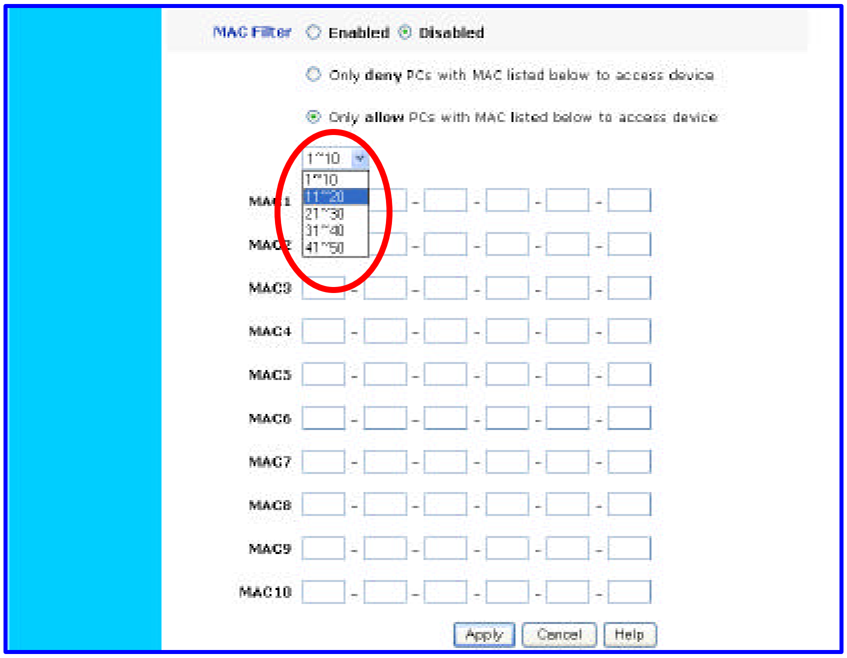
MAC6 □ - □ - □ - □ - □ - □

MAC7 □ - □ - □ - □ - □ - □

MAC8 □ - □ - □ - □ - □ - □

MAC9 □ - □ - □ - □ - □ - □

MAC10 □ - □ - □ - □ - □ - □



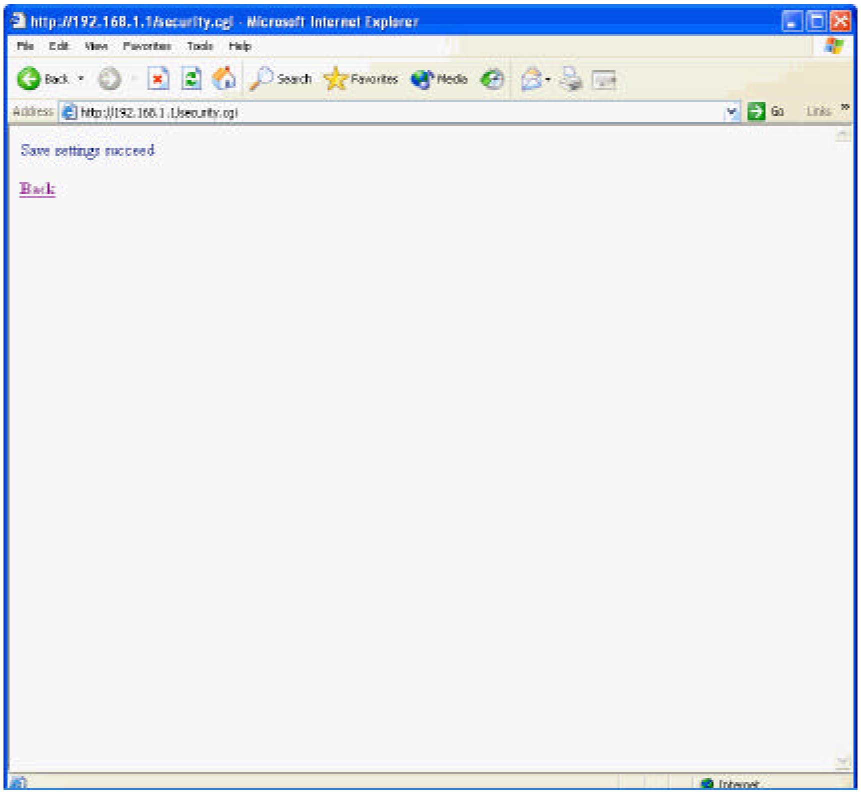
MAC Filter ○ Enabled ● Disabled

○ Only **deny** PCs with MAC listed below to access device

● Only **allow** PCs with MAC listed below to access device

1~10

The maximum number of MAC addresses that can be stored in Access Pint is 50. You can browse through the MAC address saved by selecting the drop-down box.


http://192.168.1.1/security.cgi - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/security.cgi
Go Links
Internet

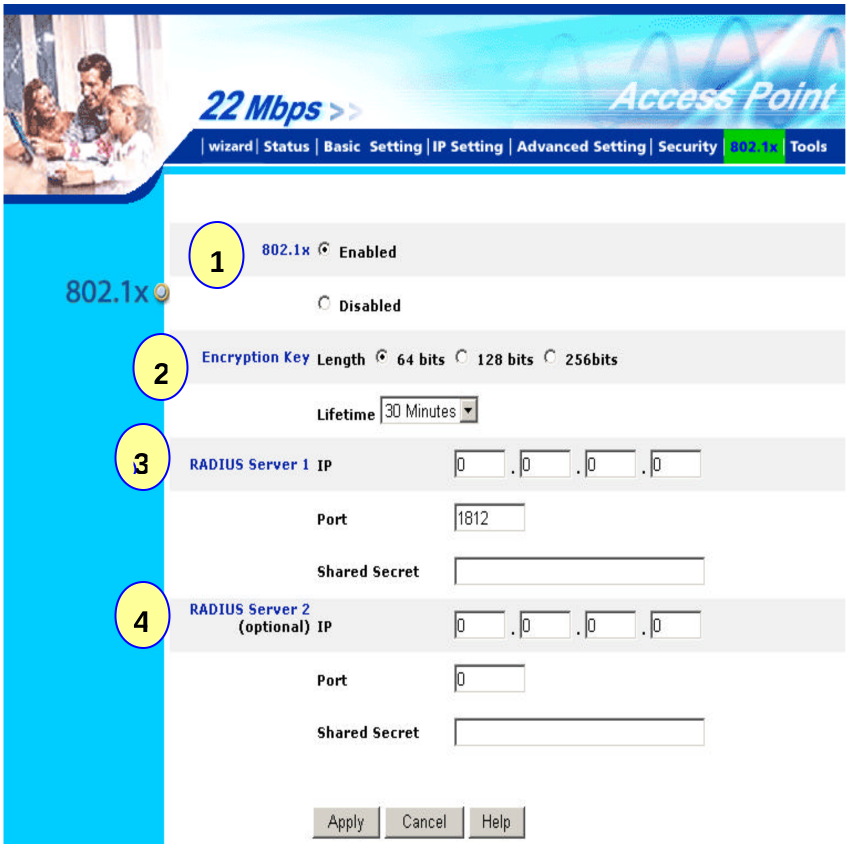
Save settings succeed

Back

For any changes made in the security page, click “**Apply**” for the changes to be effective. When the above page will appear. Click “**Back**” to go back to the previous page.

802.1x

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


22 Mbps >>
Access Point
wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
802.1x
1
2
3
4
Apply
Cancel
Help

802.1x ● Enabled
○ Disabled

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

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 method is used then you can skip step 2 and go to step 3.
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.

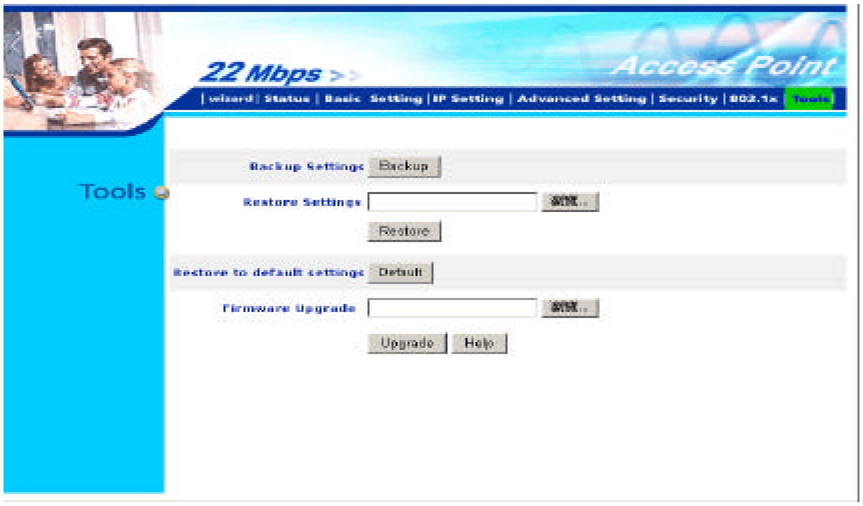
Click “**Help**” to get interpretation for Encryption Key and Radius Server

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.

Tools

Three functions are provided in this page, Backup/Restore Settings, Restore default settings and Firmware Upgrade.


22 Mbps >>
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools |
Tools
Backup Settings: Backup
Restore Settings: 瀏覽...
Restore
Restore to default settings: Default
Firmware Upgrade: 瀏覽...
Upgrade
Help

Backup Settings:

Click on "**Backup**" button, which will open a FileSave Dialog box, where you get to save all the current settings and configurations to a file.

Restore Settings:

Click on the "**Browse**" button to open a FileOpen Dialog box, where you get to select the file, which you save previous settings and configurations, to be opened.

Upon selecting the saved file, click "**Restore**" and complete the restore process when the Access Point re-operates after it restarts.

Restore to default settings:

Click on "**Default**" button to restore the Access Point back to it's manufacture default settings.

Firmware Upgrade:

Click on the "**Browse**" button to open a FileOpen Dialog box, where you get to select the firmware file, which you download from the web for the latest version.

Upon selecting the firmware file, click "**Upgrade**" and complete the firmware upgrade process when the Access Point re-operates after it restarts.

USING AP 22M UTILITY FOR MANAGEMENT

Installing AP 22M Utility

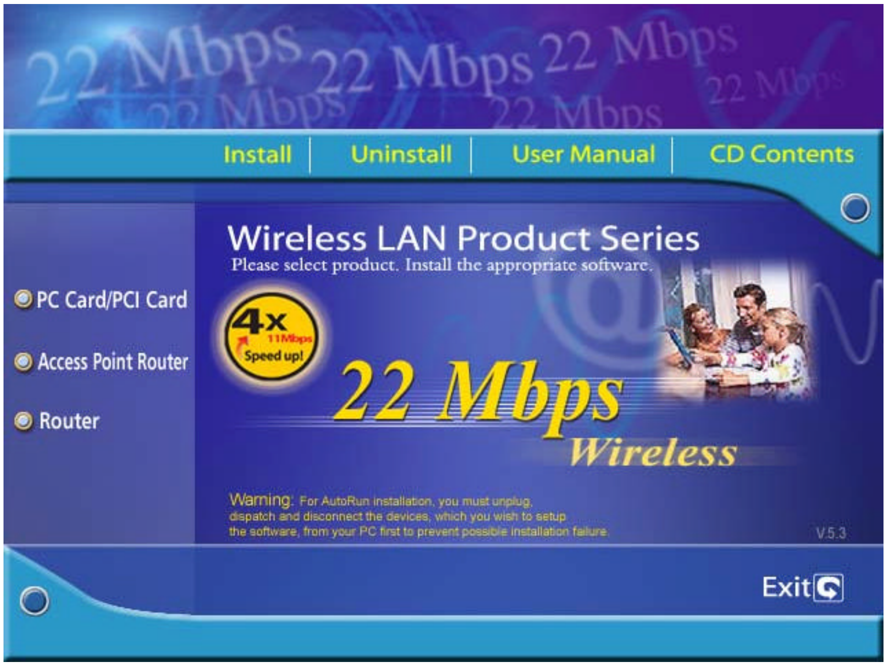
The AP 22M Utility is a program that runs on your PC, which offers easy management for all existing 22mbps Access Points in the same network domain. Please follow the steps below for installation and refer to "Manage and Configure AP with AP 22M Utility" session Access point configuration.

Note! The installation demonstrated is based on Windows XP operating system. The other Windows operation system will have very similar installation.

1. Turn on your PC

2. After Windows starts up, insert the 22Mbps Access Point Product CD into the CD tray of the CD-ROM

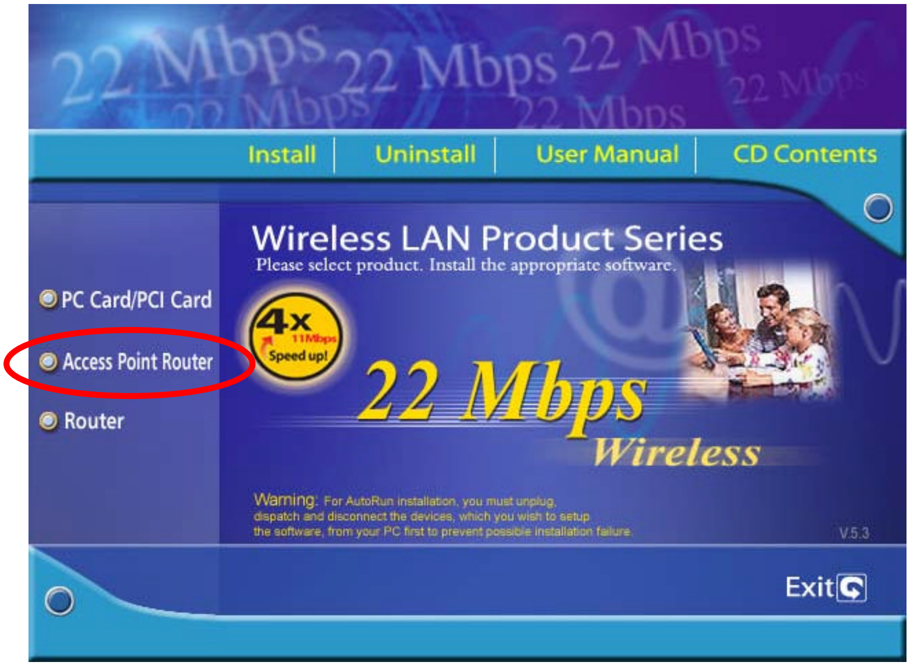
3. The following screen would appear.



Please select product. Install the appropriate software.

Warning: For AutoRun installation, you must unplug, dispatch and disconnect the devices, which you wish to setup the software, from your PC first to prevent possible installation failure.

4. Select menu option, “**Access Point**”, on the left side of screen.

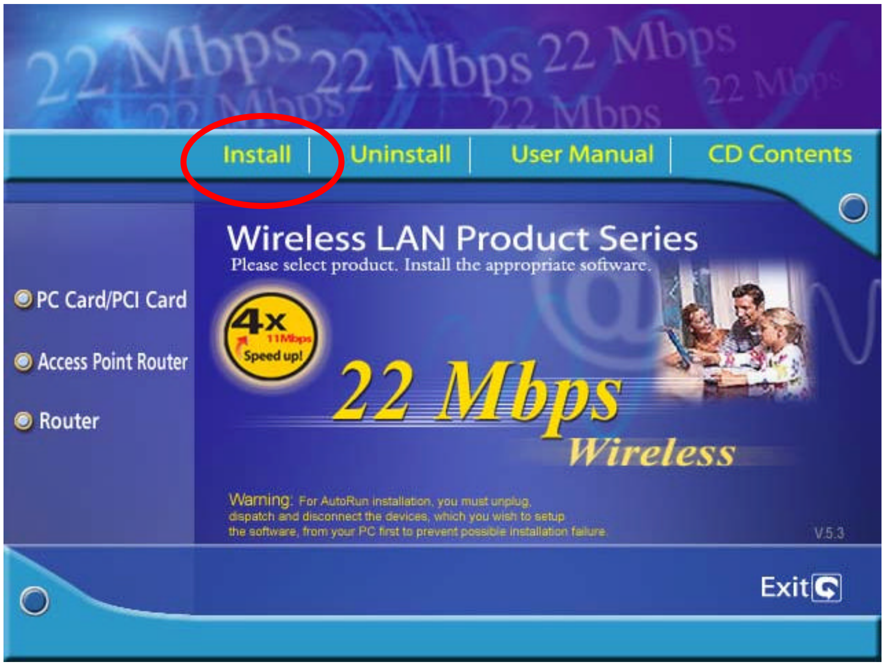


Wireless LAN Product Series

Please select product. Install the appropriate software.

Warning: For AutoRun installation, you must unplug, dispatch and disconnect the devices, which you wish to setup the software, from your PC first to prevent possible installation failure.

5. Click “**Install**” on the menu bar to proceed with 22M AP installation.

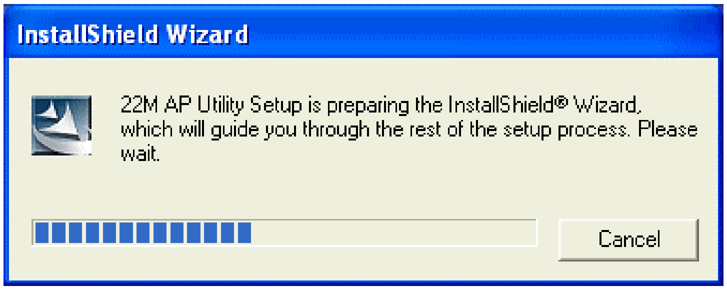


Wireless LAN Product Series

Please select product. Install the appropriate software.

Warning: For AutoRun installation, you must unplug, dispatch and disconnect the devices, which you wish to setup the software, from your PC first to prevent possible installation failure.

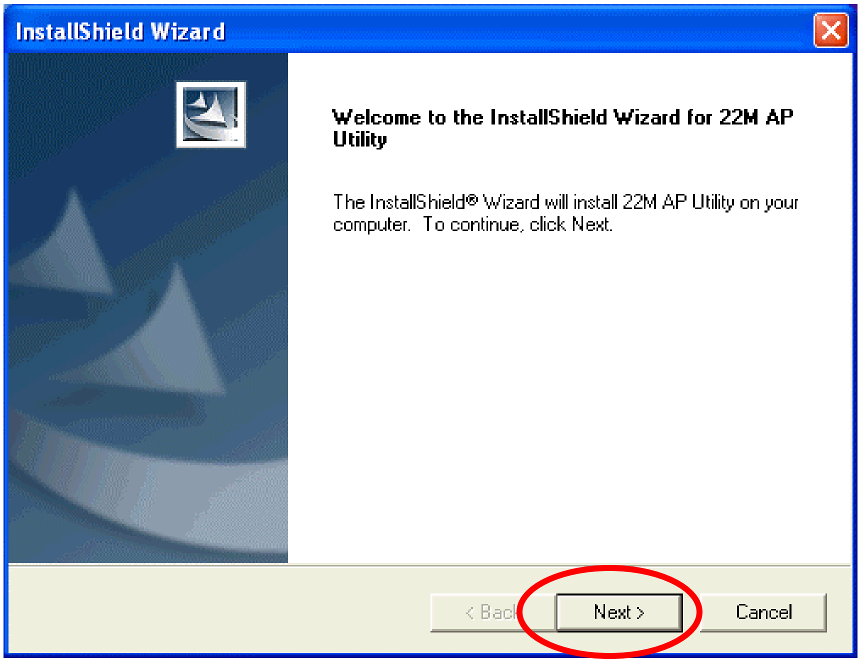
6. The 22M AP Utility loads the Install wizard for installation.



InstallShield Wizard

22M AP Utility Setup is preparing the InstallShield® Wizard, which will guide you through the rest of the setup process. Please wait.

Click "**Next**" to start installation.

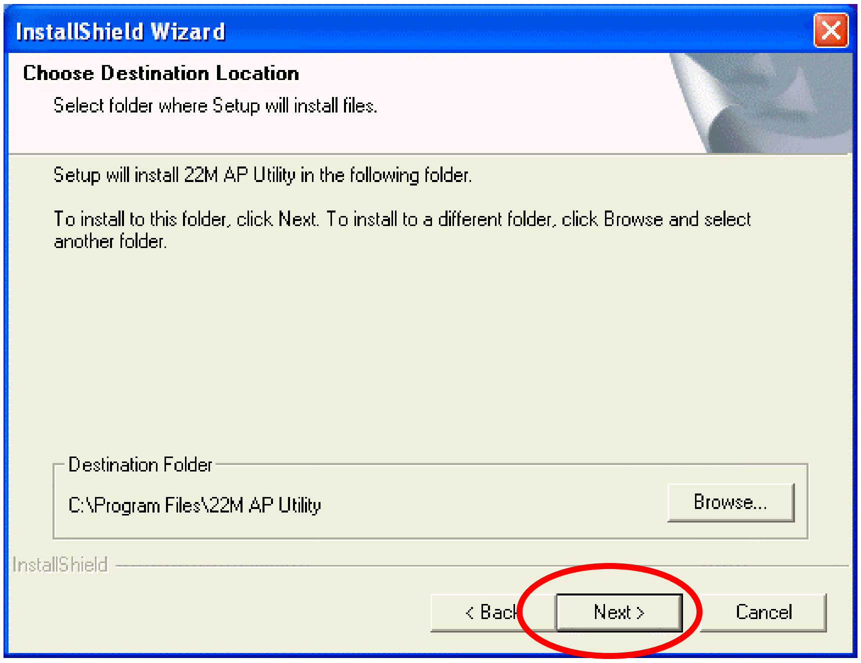


InstallShield Wizard

Welcome to the InstallShield Wizard for 22M AP Utility

The InstallShield® Wizard will install 22M AP Utility on your computer. To continue, click Next.

Click "**Next**" to install in default folder or Click "**Browse** " to install in a different folder.



InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

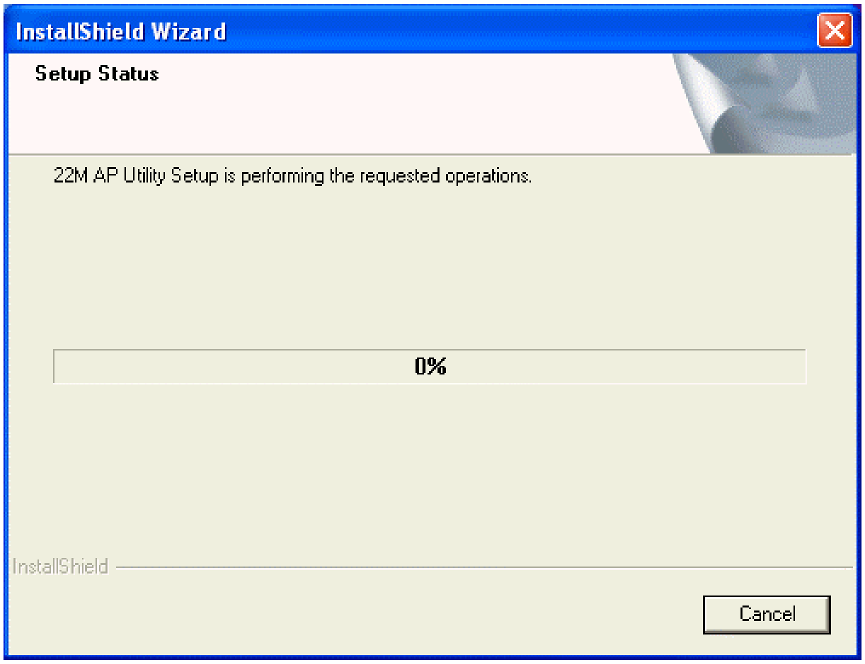
Setup will install 22M AP Utility in the following folder.

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

Destination Folder

C:\Program Files\22M AP Utility

Installation wizard copies the utility program files in your PC.



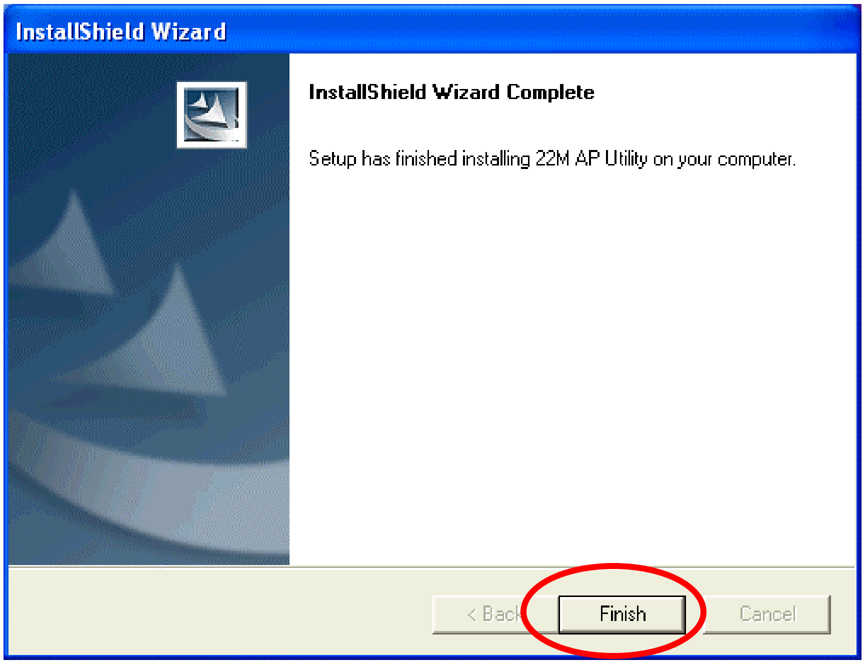
InstallShield Wizard

Setup Status

22M AP Utility Setup is performing the requested operations.

0%

7. Click “**Finish**” to complete the installation.

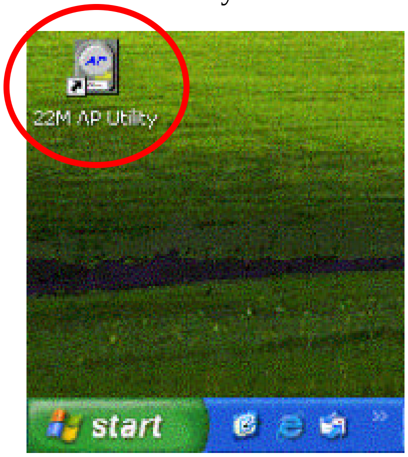


InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing 22M AP Utility on your computer.

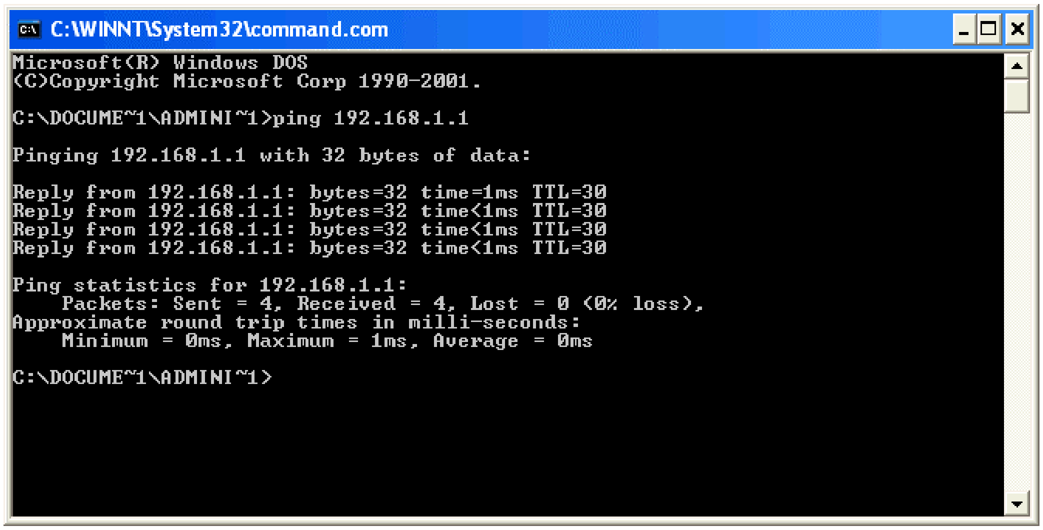
8. The 22M AP Utility icon would then appear on your desktop for easy access.



Manage and Configure Access Point with 22M AP Utility

The AP 22M Utility can be useful in a way that allows you to configure one AP to another to save the trouble of logging into the web configuration utility of each AP. However, all the Access Points that you wish to configure using 22M AP Utility must be in the same network domain as your PC's.

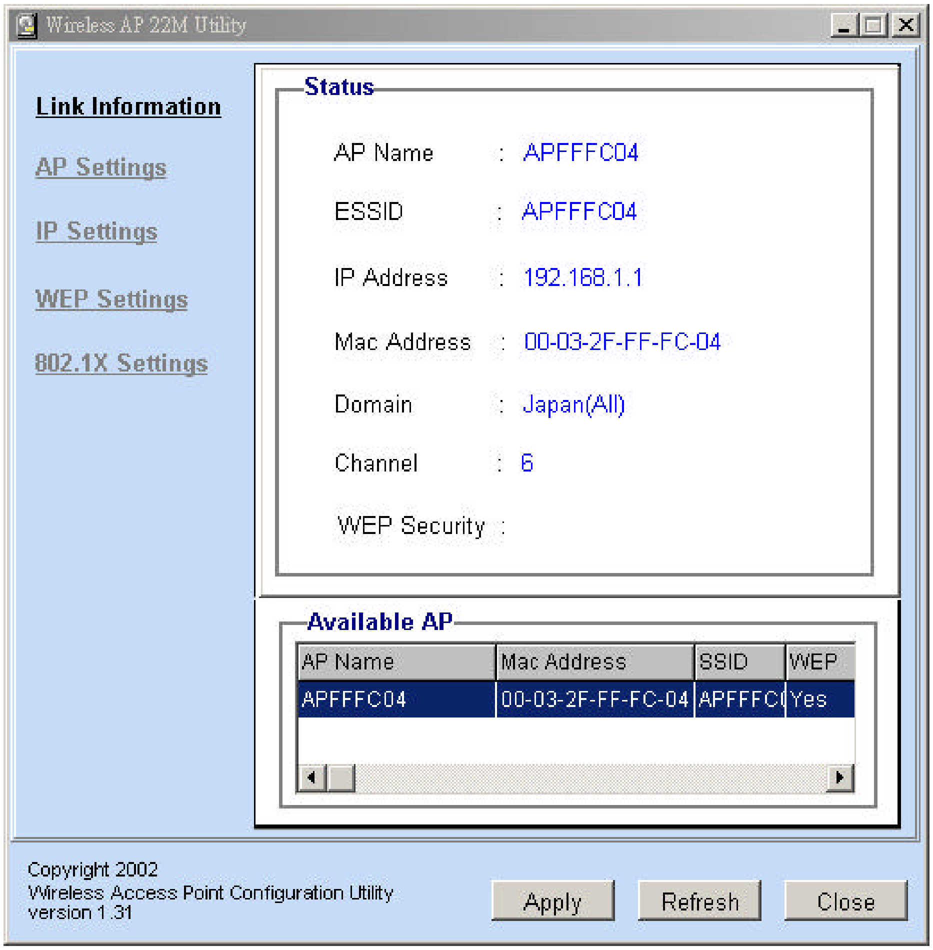
You may also check the existence with the Access Point by pinging the IP of the Access Point, for example, 192.168.1.1, in the command prompt window.



```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\DOCUME~1\ADMINI~1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=30
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\DOCUME~1\ADMINI~1>
```

Link Information

This is the default page when 22M AP Utility starts up.



Status

AP Name : APFFFC04

ESSID : APFFFC04

IP Address : 192.168.1.1

Mac Address : 00-03-2F-FF-FC-04

Domain : Japan(All)

Channel : 6

WEP Security :

Available AP

AP Name	Mac Address	SSID	WEP
APFFFC04	00-03-2F-FF-FC-04	APFFFC(	Yes

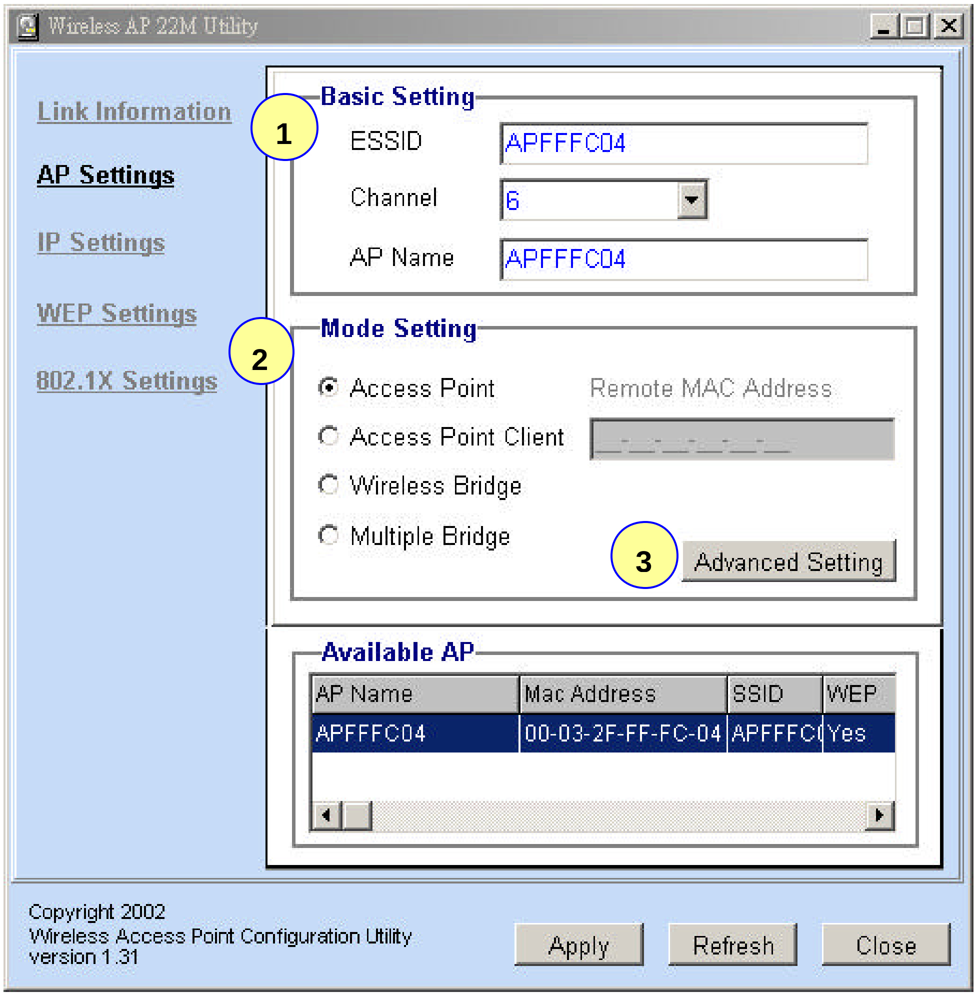
Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

Status – displays the basic settings of the selected Access Point.

Available AP – lists all the 22mpbs Access Point of the same network domain detected on the network. You can select a particular Access Point from the list to view and change its configuration.

AP Settings

This is the page that allows you to change the settings of the Access Point.



Basic Setting

ESSID: APFFFC04

Channel: 6

AP Name: APFFFC04

Mode Setting

● Access Point

○ Access Point Client

○ Wireless Bridge

○ Multiple Bridge

Remote MAC Address: __-__-__-__-__-__

Available AP

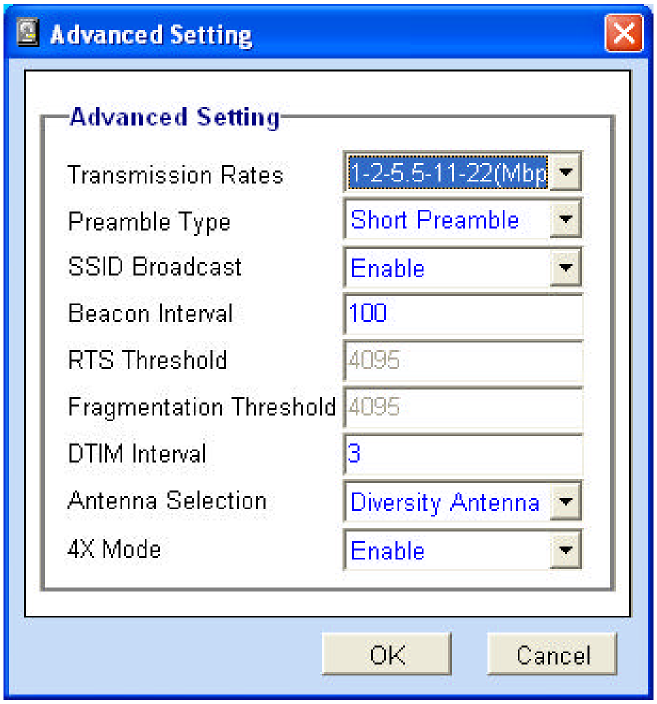
AP Name	Mac Address	SSID	WEP
APFFFC04	00-03-2F-FF-FC-04	APFFFC(	Yes

Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

1 **Basic Setting** – allows you to enter the new values for ESSID, Channel and AP Name of the Access Point.

2 **Mode Setting** – allows you to change the operating mode of the Access Point. There are 4 modes that you can choose: (1) Access Point, (2) Access Point Client, (3) Wireless Bridge and (4) Multiple Bridge. Please refer to Appendix C, Glossary for the functionalities and definitions of these operating modes.

3 **Advanced Setting** – recommended for advanced users who are familiar with wireless networks, and it's where you set additional parameters and settings of the Access Point.



Advanced Setting

Advanced Setting

Transmission Rates	1-2-5.5-11-22(Mbp
Preamble Type	Short Preamble
SSID Broadcast	Enable
Beacon Interval	100
RTS Threshold	4095
Fragmentation Threshold	4095
DTIM Interval	3
Antenna Selection	Diversity Antenna
4X Mode	Enable

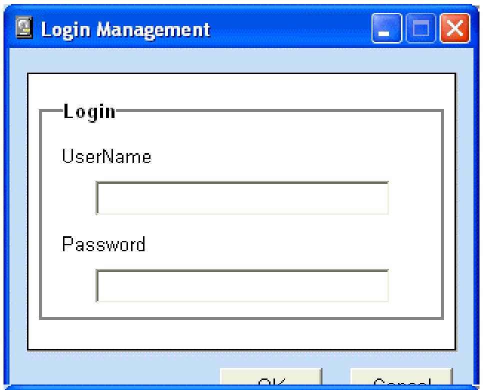
4X Mode : When “4X enable” is selected, you will be running 22Mbps PBCC+4X mode, the wireless transmission speed can achieve over 12Mbps real throughput assuming that the wireless client device is also running 22Mbps PBCC+4X.

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

Please refer to Appendix C, Glossary for the definitions of other values and function.

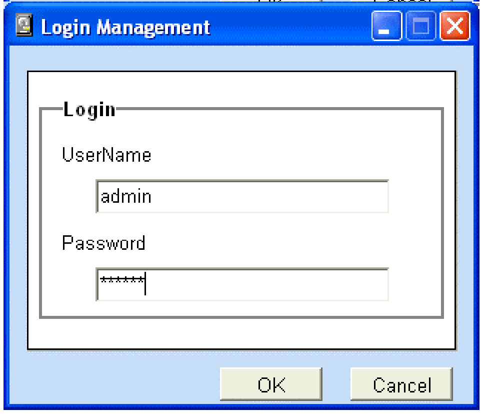
For any changes made to be effective, click “**Apply**” button.

The utility program will now prompt you for user name and password as part of the login and security protection to make sure you have the right authorization.



Enter “UserName” and “Password” for the Access Point

Click “**OK**” button

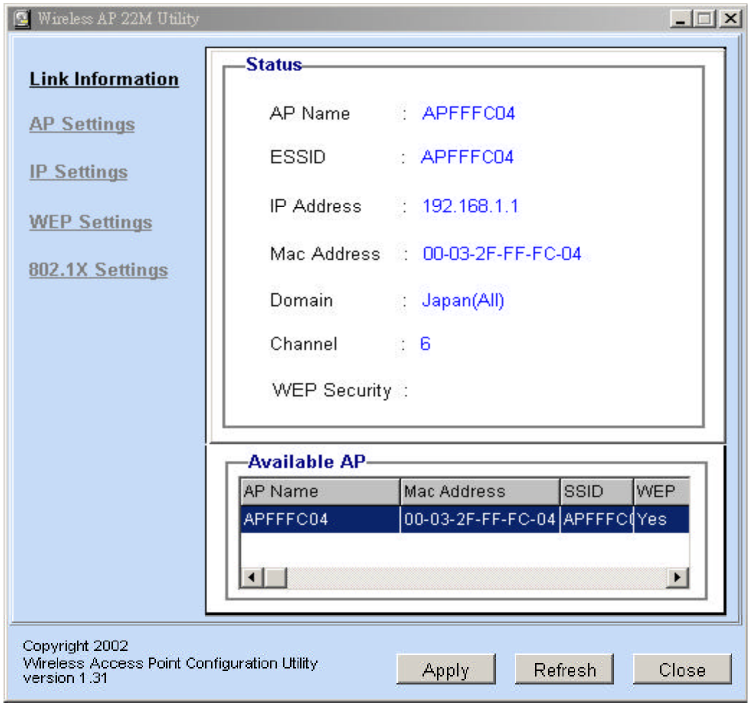


UserName: admin

Password: ******

Note! The default username is “admin” and the default password is also “admin”.

The Access Point restarts itself, and the screen will switch back to startup page – Link Information



Status

AP Name : APFFFC04

ESSID : APFFFC04

IP Address : 192.168.1.1

Mac Address : 00-03-2F-FF-FC-04

Domain : Japan(All)

Channel : 6

WEP Security :

Available AP

AP Name	Mac Address	SSID	WEP
APFFFC04	00-03-2F-FF-FC-04	APFFFC0	Yes

Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

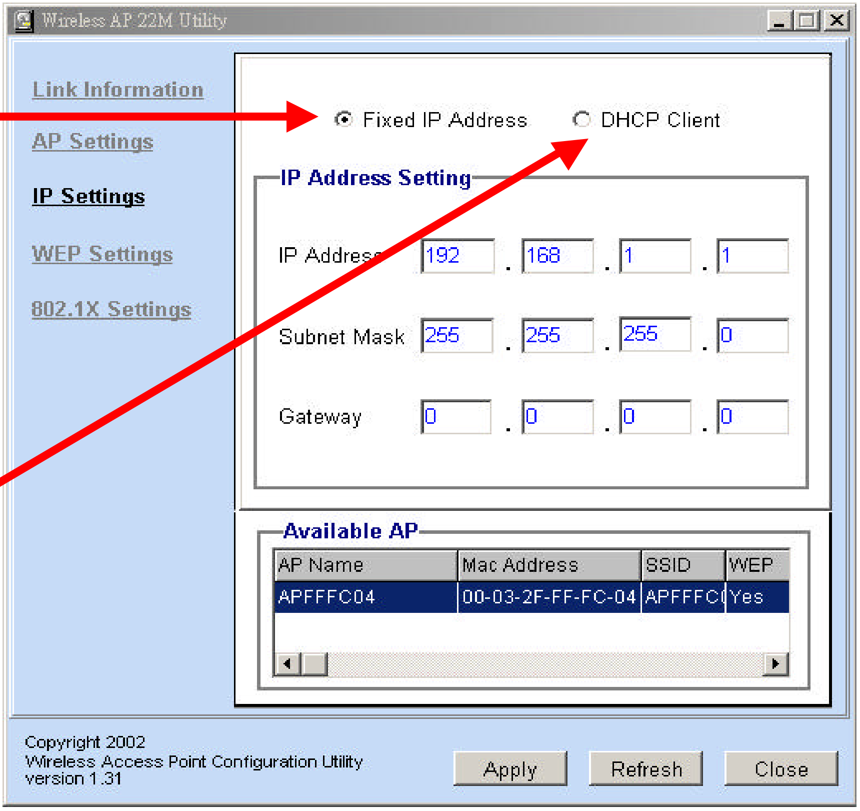
IP Settings

This is the page where you configure the IP settings for the Access Point.

Select "Fixed IP Address" and enter the IP address of the Access Point and Gateway.

Select "**DHCP Client**" if there is a DHCP server assigning IP addresses on the network.

Please also refer to Appendix B to learn more about Network and IP address.



● Fixed IP Address ○ DHCP Client

IP Address Setting

IP Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

Gateway 0 . 0 . 0 . 0

Available AP

AP Name	Mac Address	SSID	WEP
APFFFC04	00-03-2F-FF-FC-04	APFFFC(	Yes

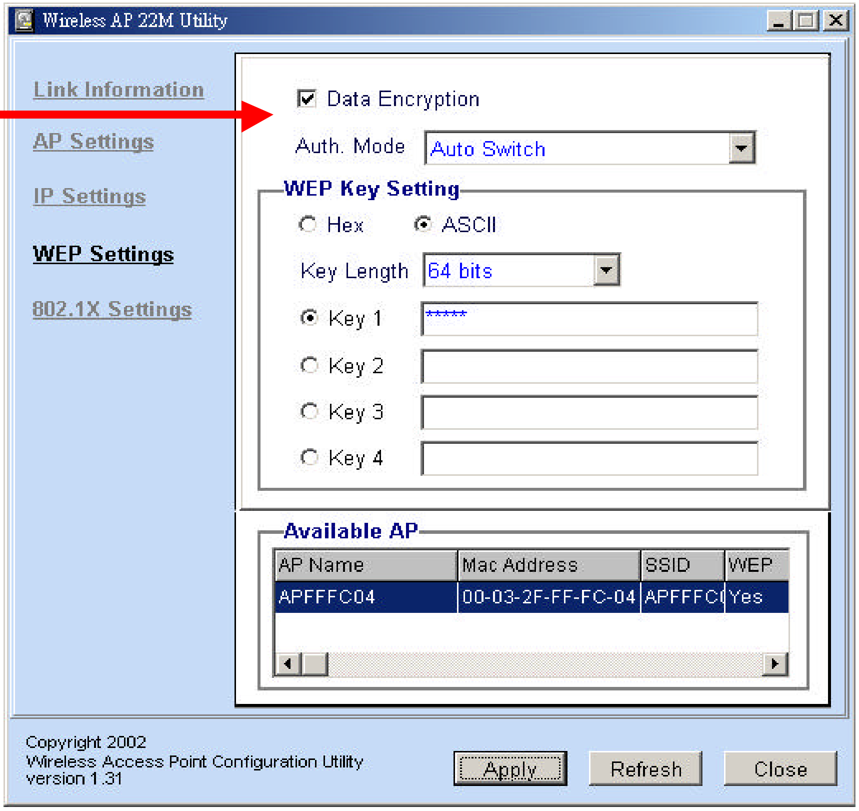
Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

Click "**Apply**" button for any changes made to be effective. The utility program will prompt you for user name and password for security protection.

WEP Settings

This is the page that allows you to configure the WEP settings for the Access Point.

Enable WEP Key security by clicking "**Data Encryption**"



☑ Data Encryption

Auth. Mode: Auto Switch

WEP Key Setting

○ Hex ● ASCII

Key Length: 64 bits

● Key 1: *****

○ Key 2

○ Key 3

○ Key 4

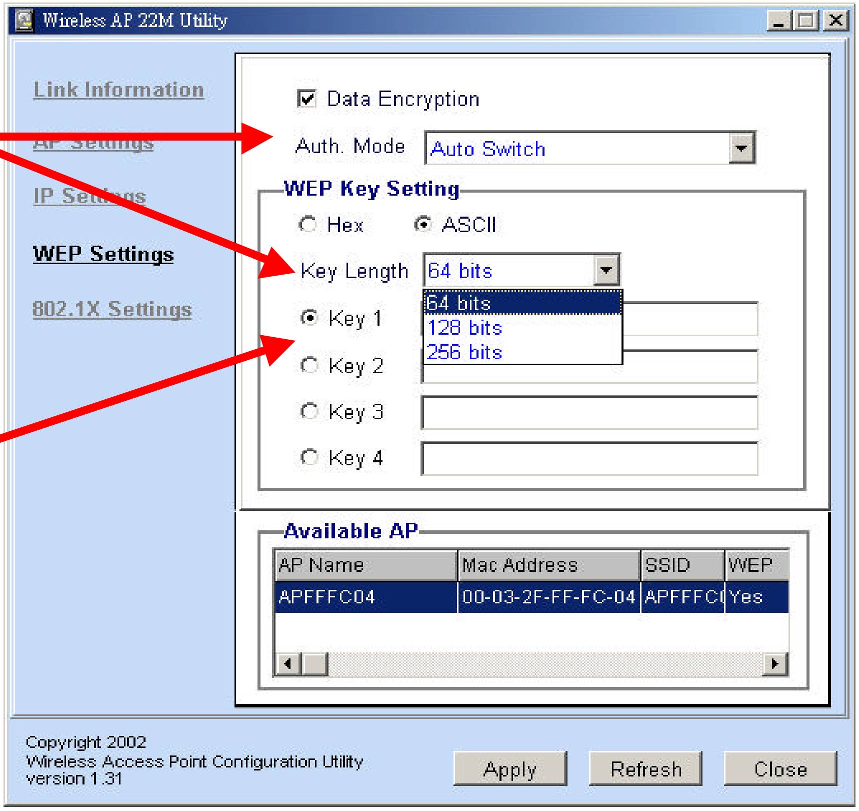
Available AP

AP Name	Mac Address	SSID	WEP
APFFFC04	00-03-2F-FF-FC-04	APFFFC(	Yes

Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

Select the "**Auth. Mode**" and the "**Key Length**"

Fill at least one of the 4 Web Key fields with Hex or ASCII values.



☑ Data Encryption

Auth. Mode: Auto Switch

WEP Key Setting

○ Hex ● ASCII

Key Length: 64 bits

● Key 1

○ Key 2

○ Key 3

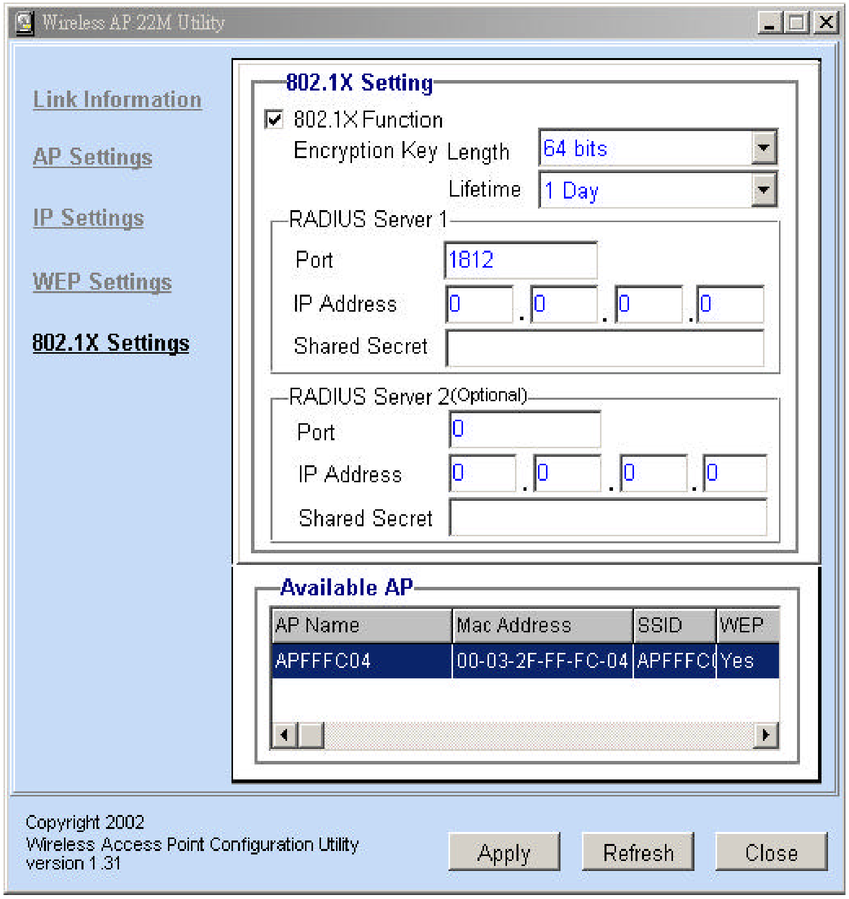
○ Key 4

Available AP

AP Name	Mac Address	SSID	WEP
APFFFC04	00-03-2F-FF-FC-04	APFFFC(	Yes

Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

802.1x Settings



Wireless AP 22M Utility

802.1X Setting

☑ 802.1X Function

Encryption Key Length: 64 bits

Lifetime: 1 Day

RADIUS Server 1

Port: 1812

IP Address: 0 . 0 . 0 . 0

Shared Secret:

RADIUS Server 2(Optional)

Port: 0

IP Address: 0 . 0 . 0 . 0

Shared Secret:

Available AP

AP Name	Mac Address	SSID	WEP
APFFFC04	00-03-2F-FF-FC-04	APFFFC(	Yes

Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

1. Enable 802.1x security by clicking the “802.1X Function” checkbox.
2. If **MD5** EAP methods is used then you can skip step 3 and go to step 4.
3. Select the **Encryption Key Lifetime** 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. Select the **Length** ranging from 64 to 256 Bits that you would like to use for Encryption Key Length.
5. RADIUS Server 1: Enter the **IP address** of and the **Port** used by the **Primary** Radius Server Enter the **Shared Secret**, which is used by the Radius Server.
6. RADIUS Server 2: Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.
7. Click “**Apply**” button for the 802.1x settings to take effect after Access Point reboots itself.

Note! As soon as 802.1x security is enabled, all the wireless client stations that are connected to the Access Point currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected. Please refer to **Appendix C** for detail 802.1x setup and installation.

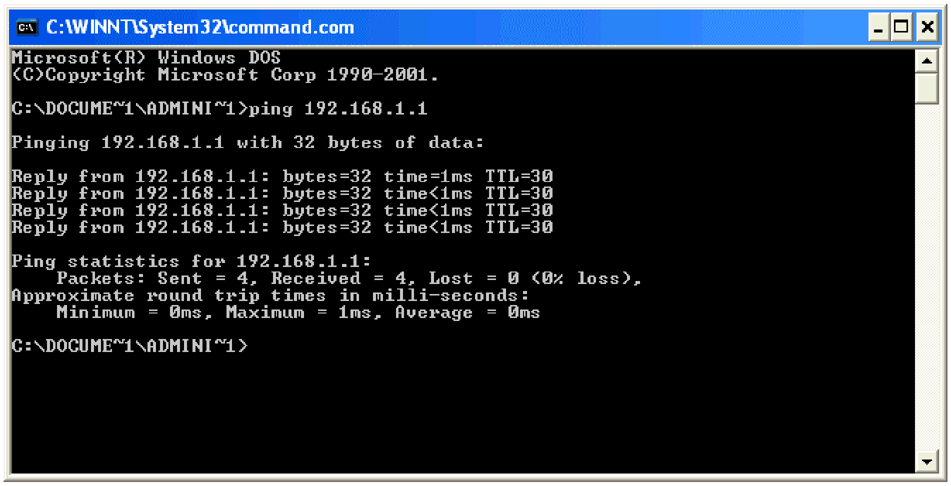
APPENDIX A: TROUBLESHOOTING

This chapter provides solutions to frequently encountered problems that can occur during the installation and operation of the Wireless Access Point. Please read through the following to solve your problems.

1. **The computer connected to the Wireless Access Point through Ethernet network cannot access the configuration menu.**
   - Check that the Ethernet Adapter is working properly. Make sure that the drivers for the network adapters are installed properly.
   - Check that the Ethernet cable is connect to the Wireless Access Point properly, and the Ethernet LED of the Wireless Access Point is ON.
   - Check that the IP address of the computer is in the same IP range and subnet as that of the Wireless Access Point. Please refer to the Networking Basis in APPENDIX B in this manual for more information if necessary.

Note! The default IP Address of the Wireless Access Point is 192.168.1.1. All the computers on the network must have a unique IP address in the same range, e.g., 192.168.1.xxx, and they must all have the same subnet mask, e.g., 255.255.255.0.

- Check the connection of computer and Wireless Access Point by doing a simple Ping test.
- Go to Start>Run>Type "command"> Type "ping 192.168.1.1". A successful ping will show responses from the Wireless Access Point.

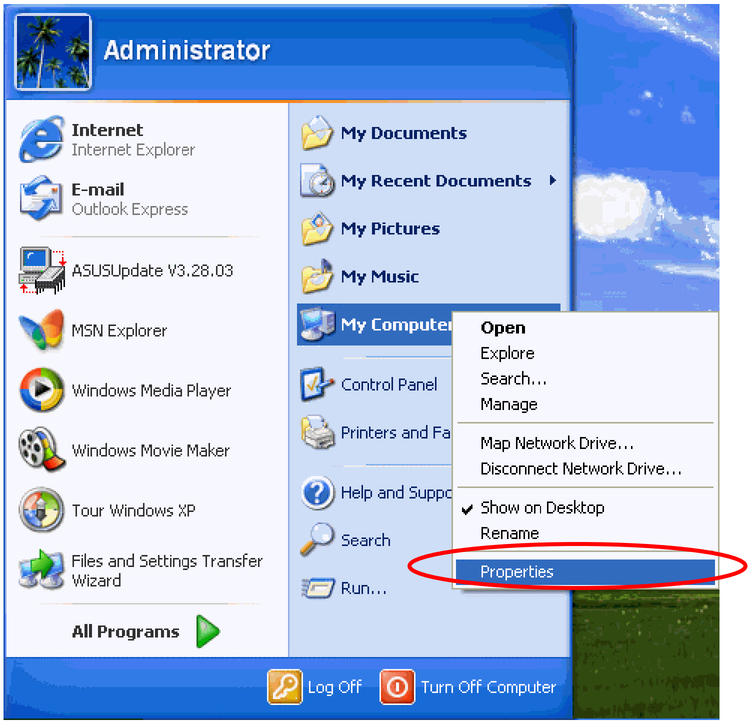


```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\DOCUME~1\ADMINI~1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=30
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\DOCUME~1\ADMINI~1>
```

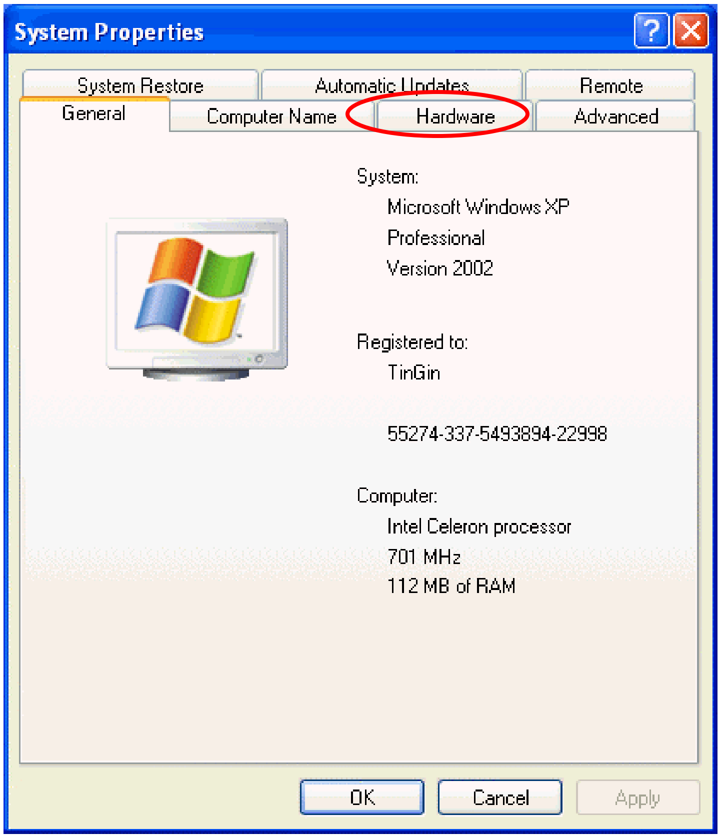
2. The wireless clients cannot access the network in the infrastructure mode.

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

Go to “Start” > Right mouse click on “My Computer” > “Properties”



Go to “Hardware”



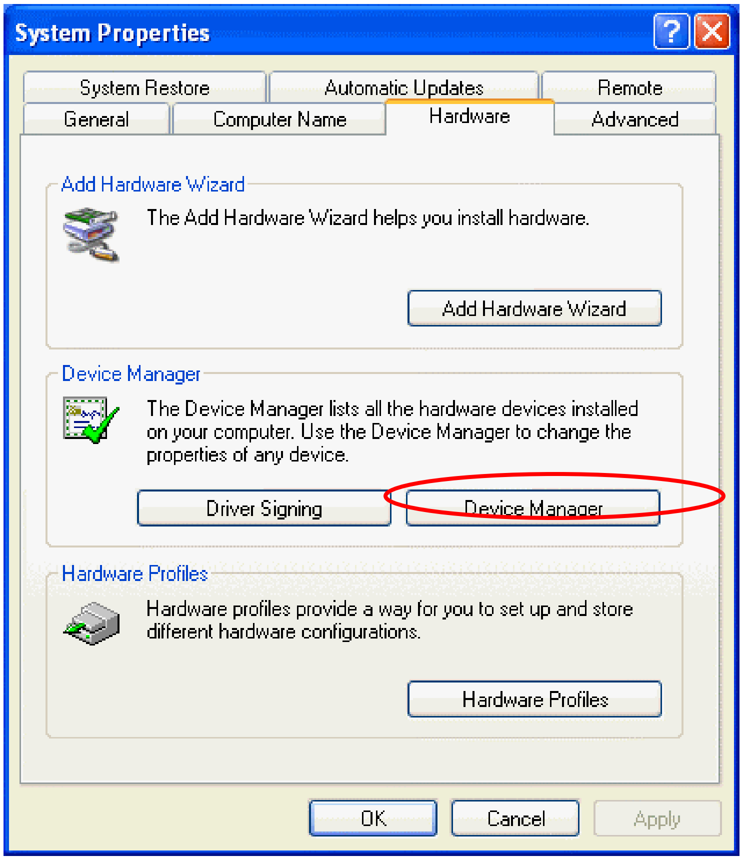
System:
Microsoft Windows XP
Professional
Version 2002

Registered to:
TinGin

55274-337-5493894-22998

Computer:
Intel Celeron processor
701 MHz
112 MB of RAM

Go to "Device Manager"

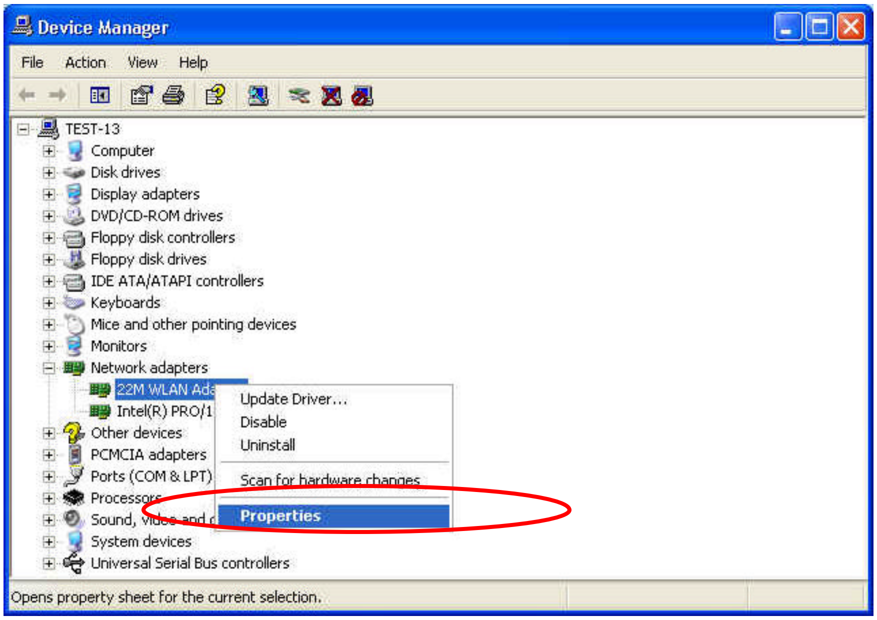


The Add Hardware Wizard helps you install hardware.

The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

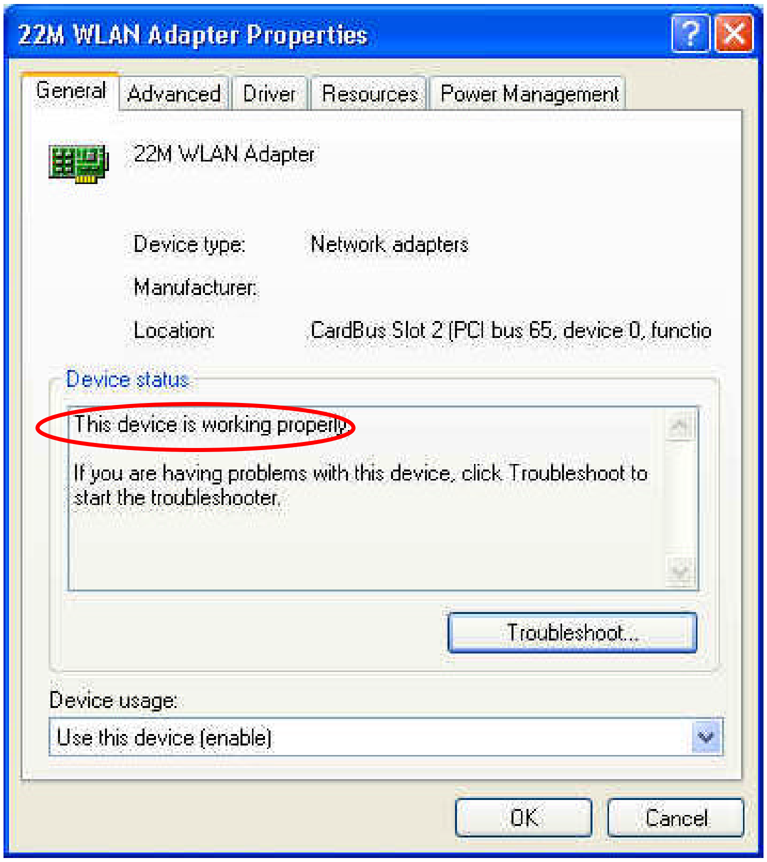
Hardware profiles provide a way for you to set up and store different hardware configurations.

Right mouse click on the network adapter which you connect RJ45 cable with. And go to "Properties"



Opens property sheet for the current selection.

Check and make sure that the network adapter is working properly



22M WLAN Adapter

Device type: Network adapters

Manufacturer:

Location: CardBus Slot 2 (PCI bus 65, device 0, functio

Device status

This device is working properly.

If you are having problems with this device, click Troubleshoot to start the troubleshooter.

Device usage:

Use this device (enable)

3. Resetting the Wireless Access Point to Factory Default Setting.

You may choose to Reset the Wireless Access Point by doing the following:

- ➢ Locate the Reset button on the back of the Wireless Access Point
- ➢ Use a paper clip to press the Reset button
- ➢ Hold the reset button for at least 5 seconds before you release
- ➢ Wait till the Wireless Access Point reboots itself (it may take a few minutes), then the configuration will be set back to factory default values.

4. What are the operation modes supported by the Wireless Access Point?

The Wireless Access Point supports 4 operation modes:

- Access Point:
  Forms a wireless network and works as a bridge to communicate with Ethernet LAN network.
- AP Client:
  Acts as an wireless client which allows the computers that are connected to the AP to communicate with other wireless clients.
- Point-to-Point Bridge:
  Connects two independent Ethernet LAN networks or computers wirelessly.
- Multi-point Bridge:
  Connects more than two independent Ethernet LAN networks or computers wirelessly.

5. **What is the difference between 22mbps and 11mbps wireless products? What's the benefit of 22mbps Wireless Access Point?**

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

6. **What is Roaming?**

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

7. **What is a MAC Address?**

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking devices, e.g. a network adapter, that allows the network to identify it at the hardware level. Unlike IP addresses, which can be changed or dynamically assigned by the network, the MAC address of a networking device is permanent.

8. **What is WEP?**

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

9. **Would the information be transmitted securely in the air?**

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

10. **What is ISM band?**

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

11. **What is 4X mode?**

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

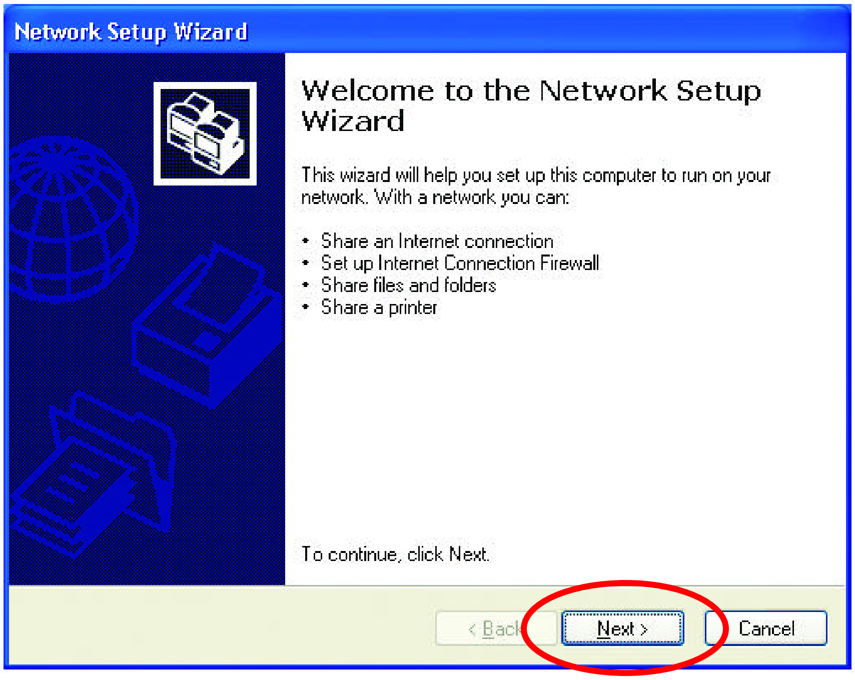
APPENDIX B: NETWORKING BASIS

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

Using the Windows XP Network Setup Wizard

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

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



Network Setup Wizard

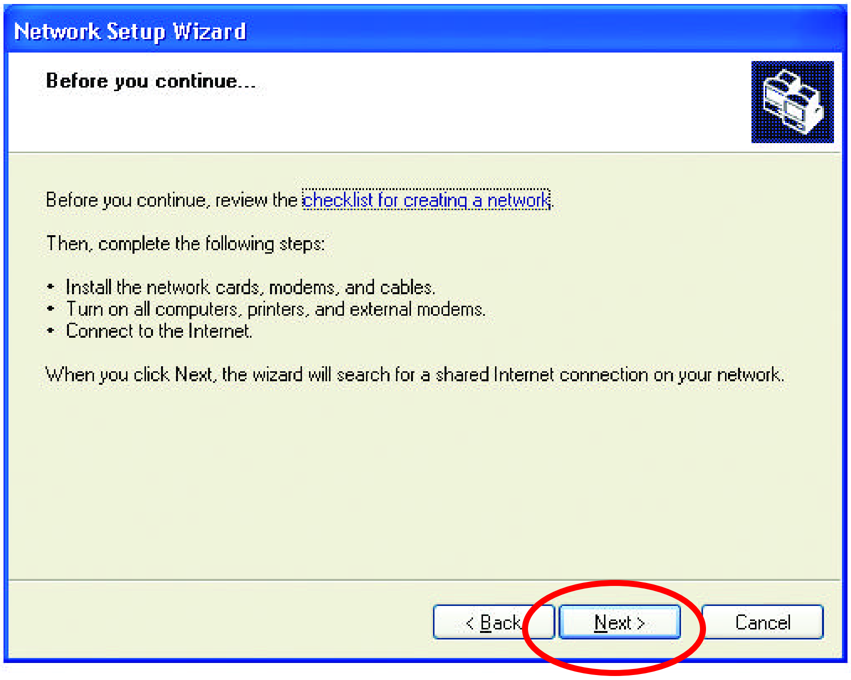
Welcome to the Network Setup Wizard

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 procced



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.

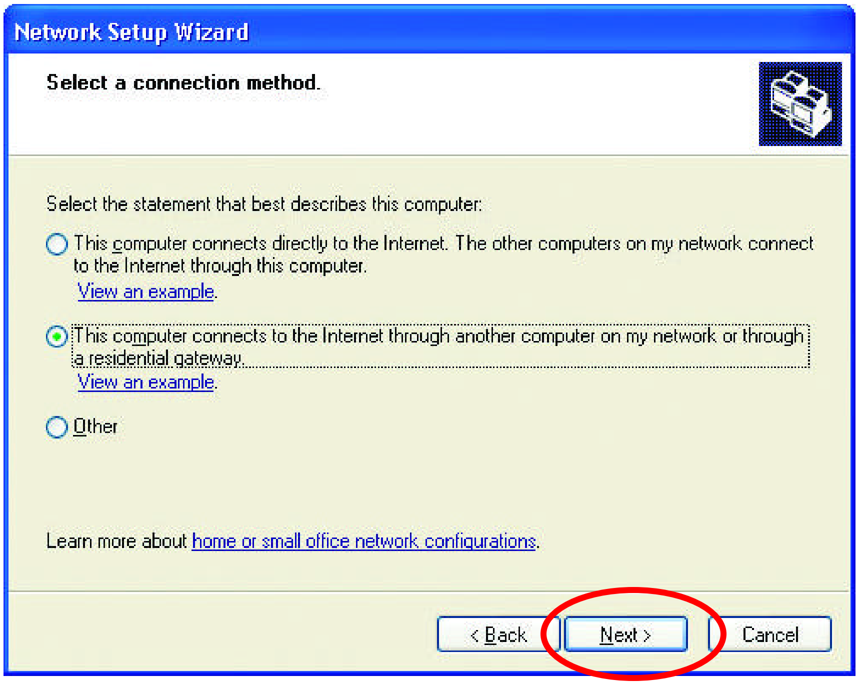
When you click Next, the wizard will search for a shared Internet connection on your network.

Click "**Next**" to continue

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

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

Click "**Next**" to continue.



Select a connection method.

Select the statement that best describes this computer:

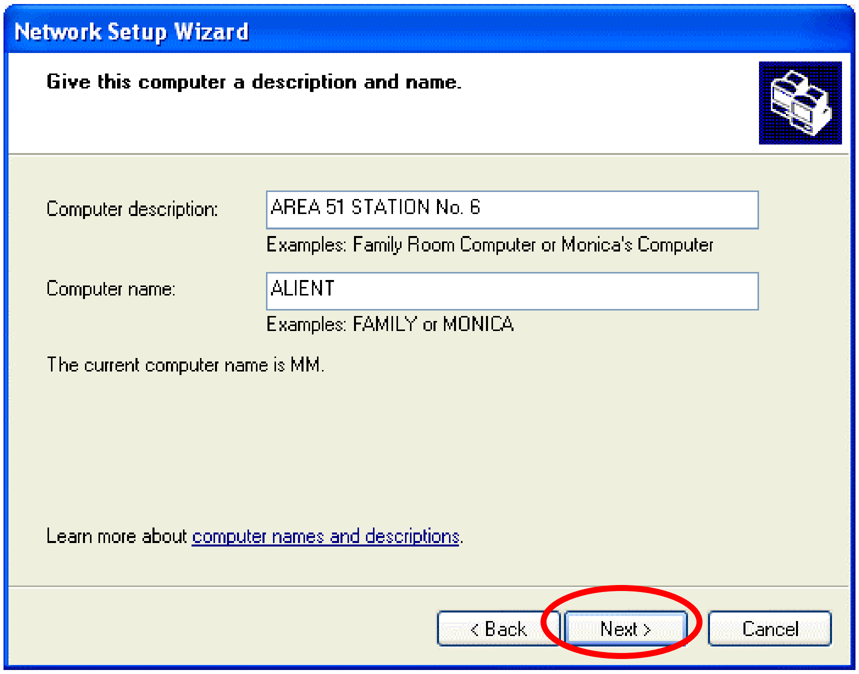
○ This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.

● 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.



Give this computer a description and name.

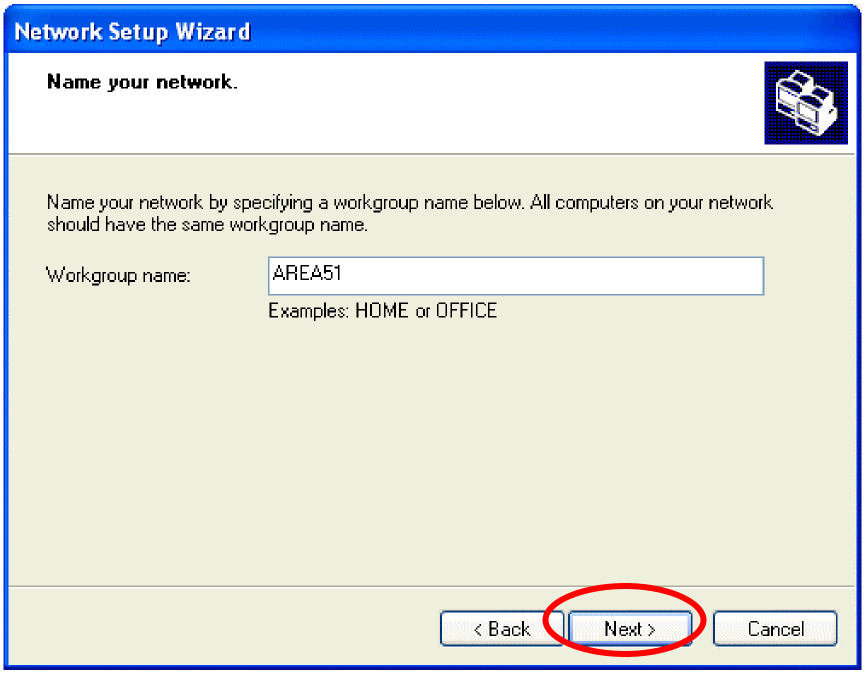
Computer description: AREA 51 STATION No. 6
Examples: Family Room Computer or Monica's Computer

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

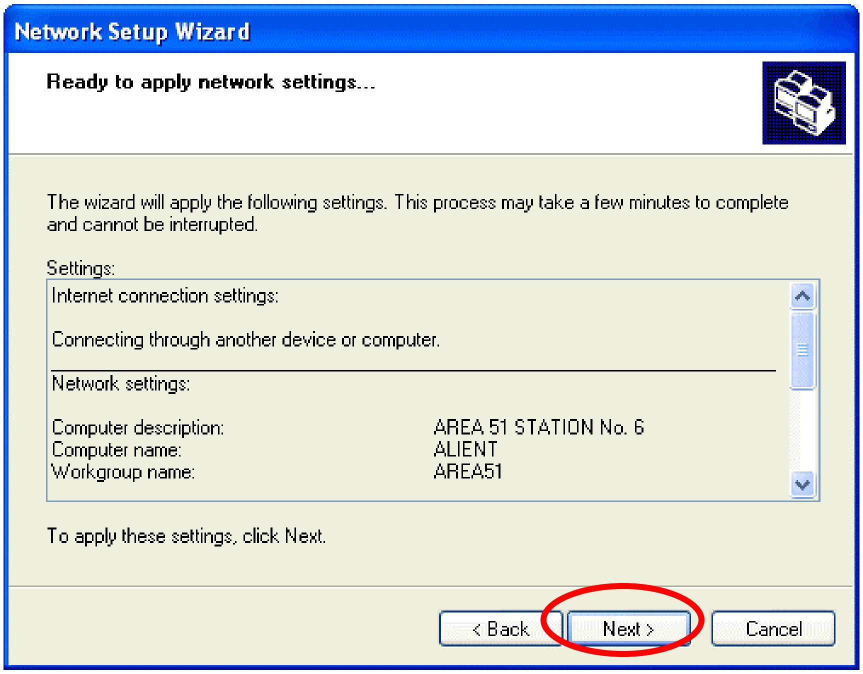
Name your network.

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:

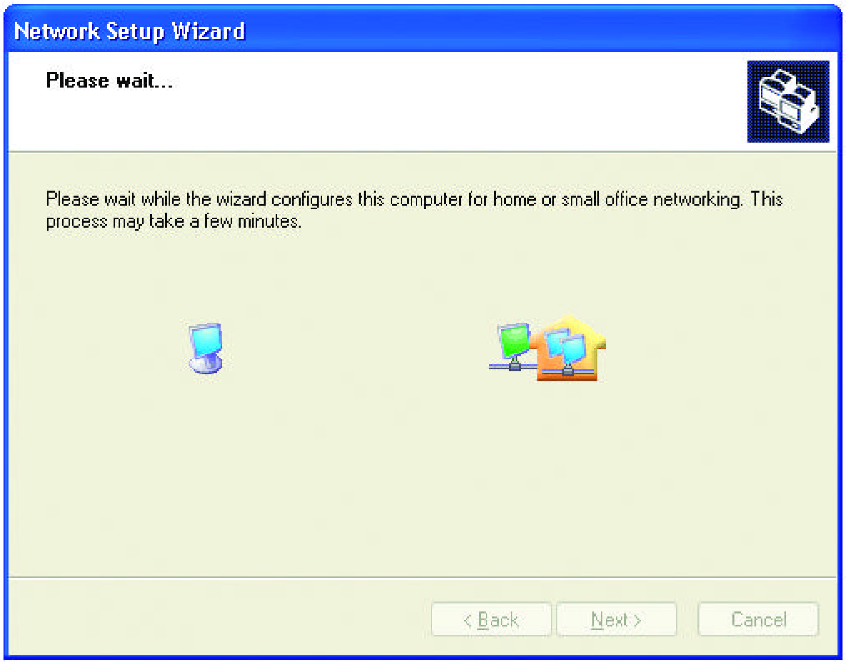
Internet connection settings:

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.



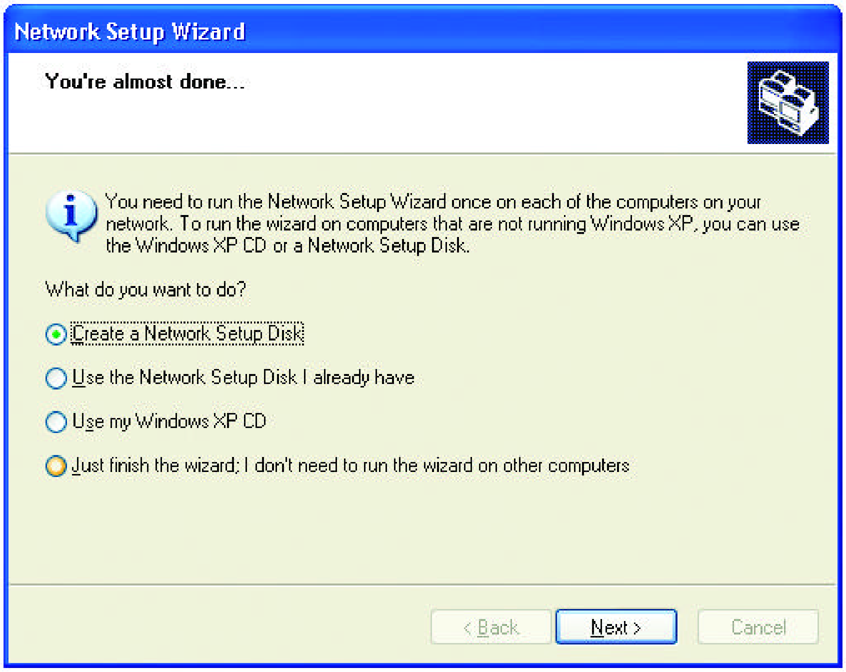
Please wait...

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.



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

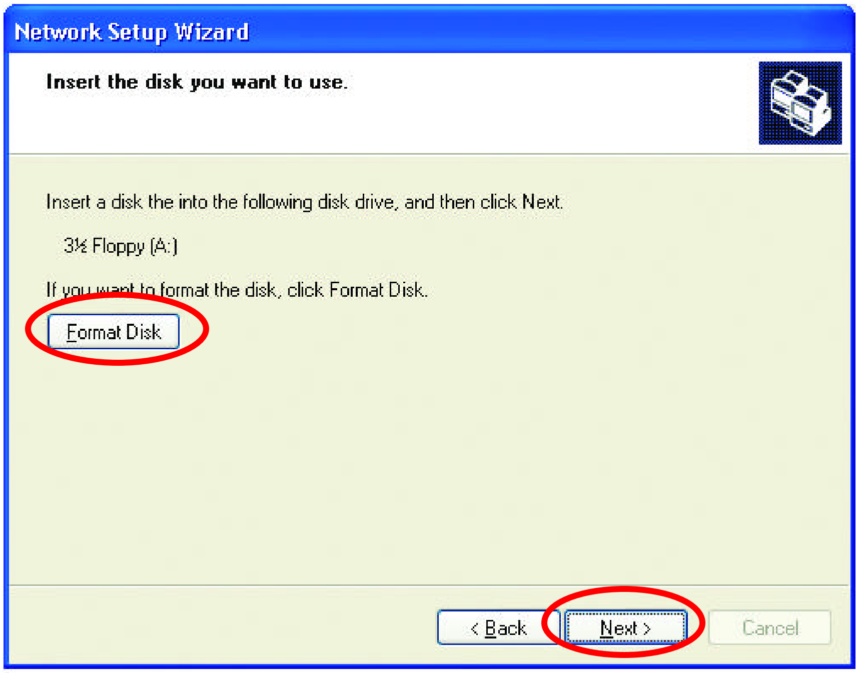
○ Use the Network Setup Disk I already have

○ 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.



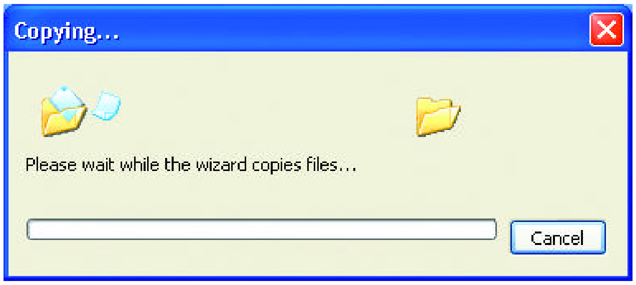
Network Setup Wizard

Insert the disk you want to use.

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

3½ Floppy (A:)

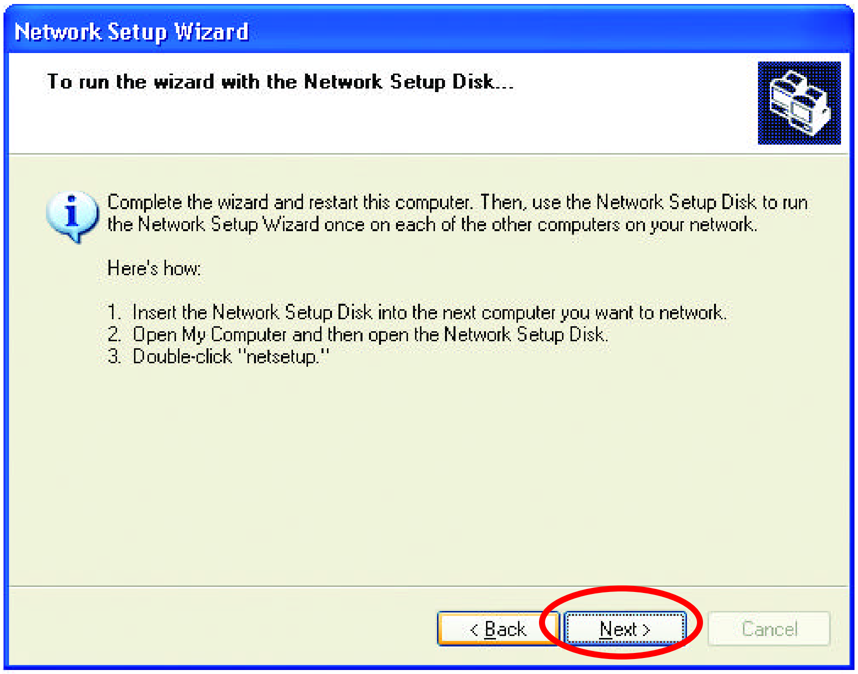
If you want to format the disk, click Format Disk.



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...

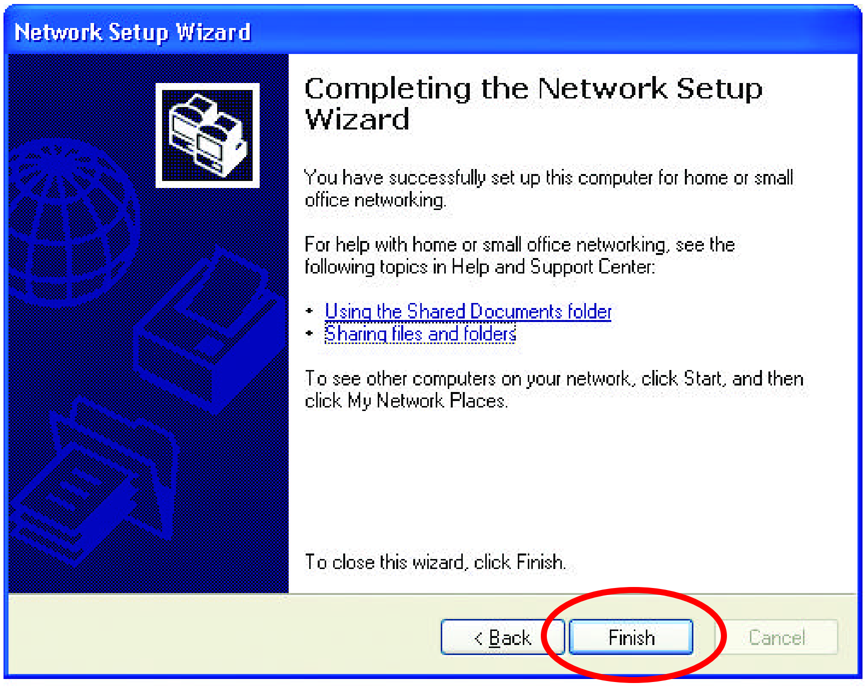
Complete the wizard and restart this computer. Then, use the Network Setup Disk to run the Network Setup Wizard once on each of the other computers on your network.

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:

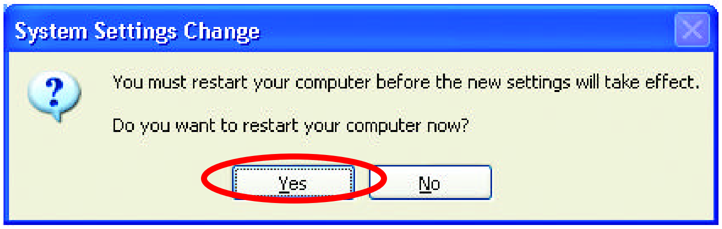
- Using the Shared Documents folder
- Sharing files and folders

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.

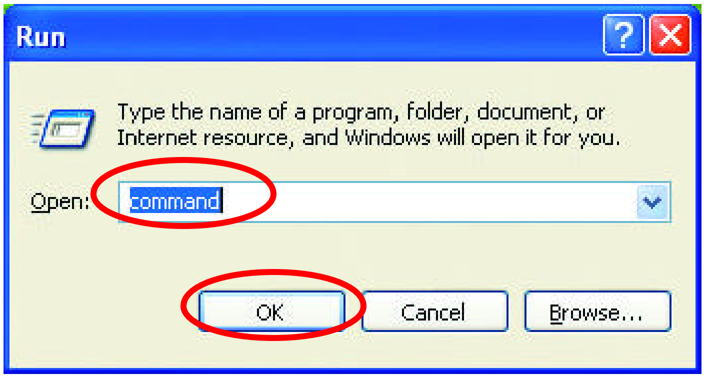
Do you want to restart your computer now?

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**"

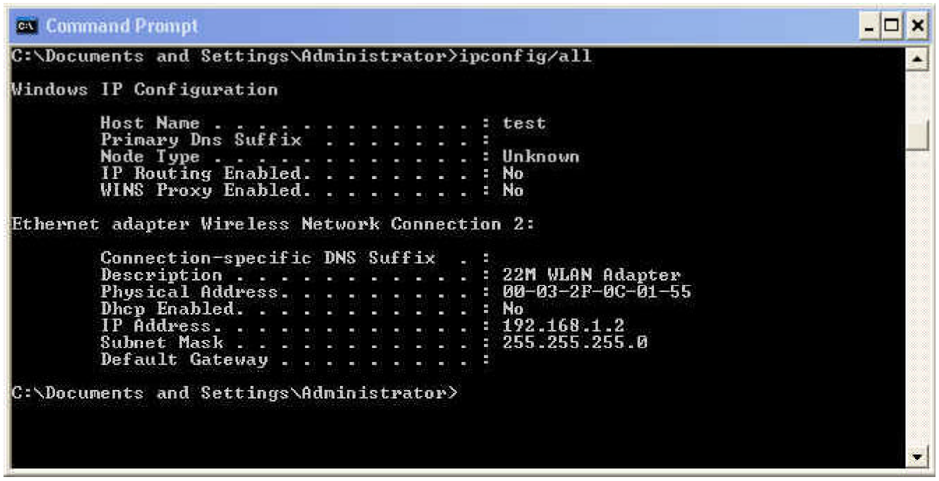


Run

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.



Command Prompt

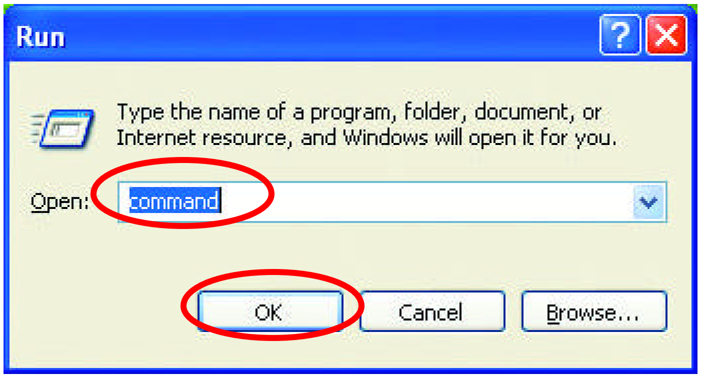
```
C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

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

Ethernet adapter Wireless Network Connection 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 22M WLAN Adapter
        Physical Address. . . . . . . . . : 00-03-2F-0C-01-55
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

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

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

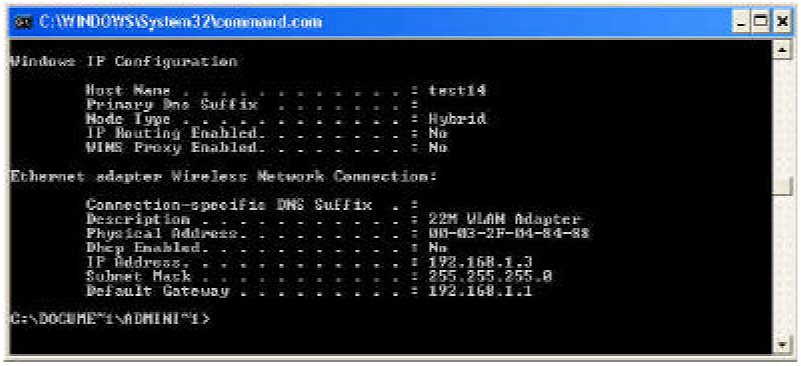
If the IP address is assigned by DHCP server on the network, there are chances you might have to release the IP and acquire it from DHCP server again. Here is how you do it.

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

Click **"OK"**


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

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



```
Windows IP Configuration

        Host Name . . . . . . . . . . . . : test14
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 22M WLAN Adapter
        Physical Address. . . . . . . . . : 00-03-2F-04-84-88
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\DOCUME~1\ADMINI~1>
```

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

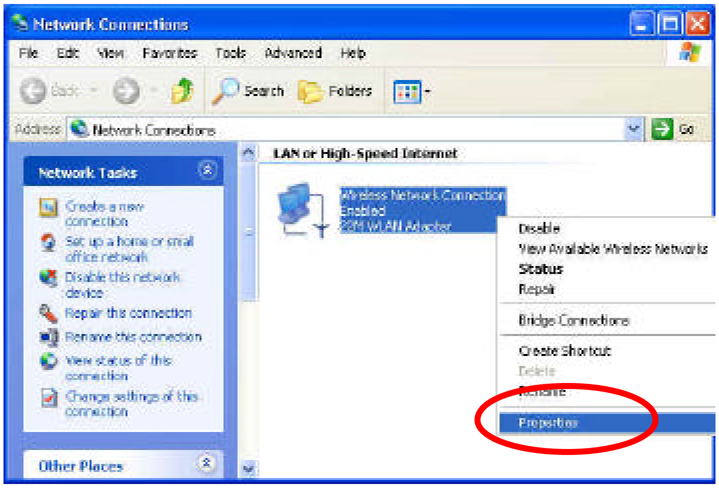
If the above methods for IP renew fail, you will have to try and restart the computer, which will reinitializes the network adapter settings during startup including renewing IP address. If you still have problems getting an IP address after computer restarts, you will have to consult with your MIS in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

Dynamic IP Address V.S. Static IP Address

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

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

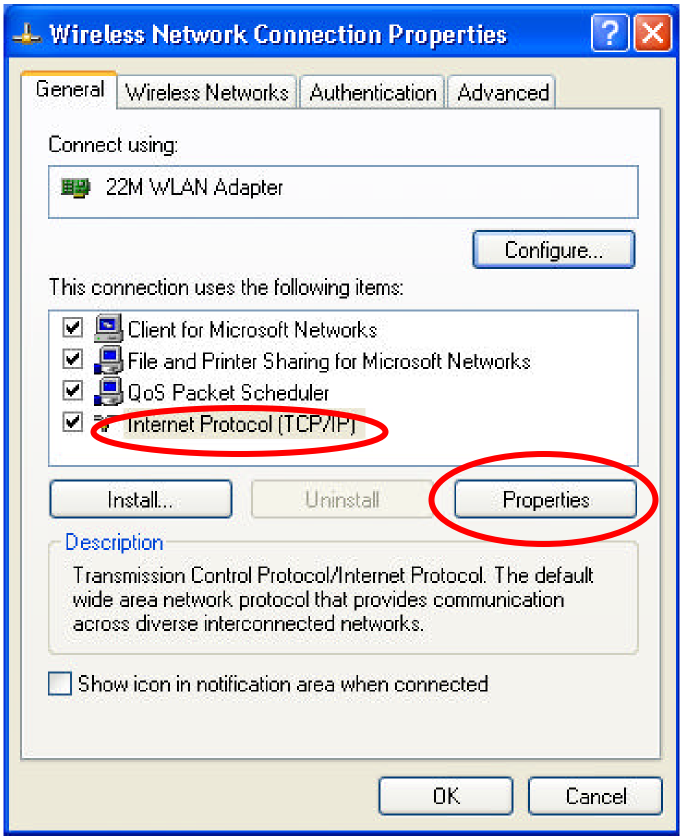
Go to **Start** menu > **Control Panel** > **Network Connections** > Right-click on the active **Local Area connection** > Select "**Properties**"


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
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 “**Intemet Protocol (TCP/IP)**” and Click “**Properties**” to continue.



Connect using:

22M WLAN 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.

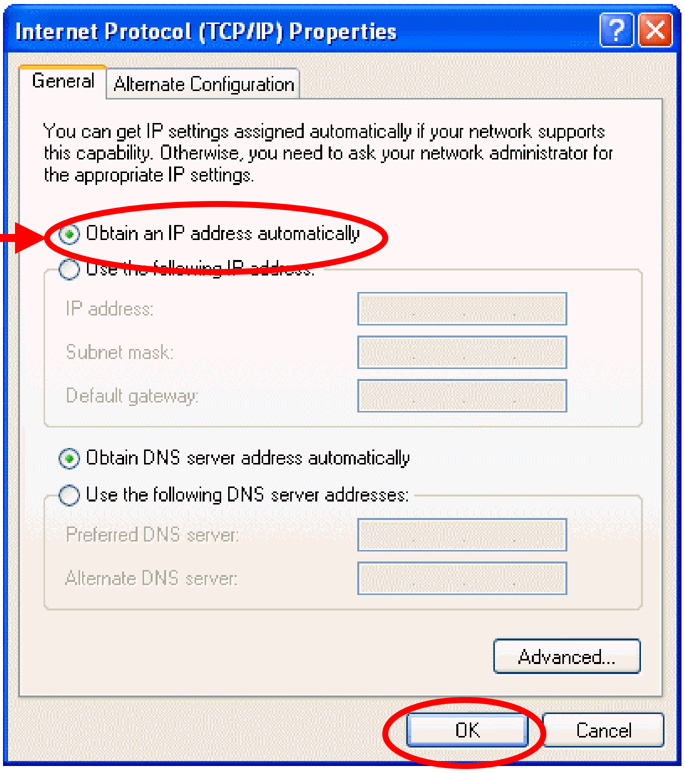
□ Show icon in notification area when connected

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:

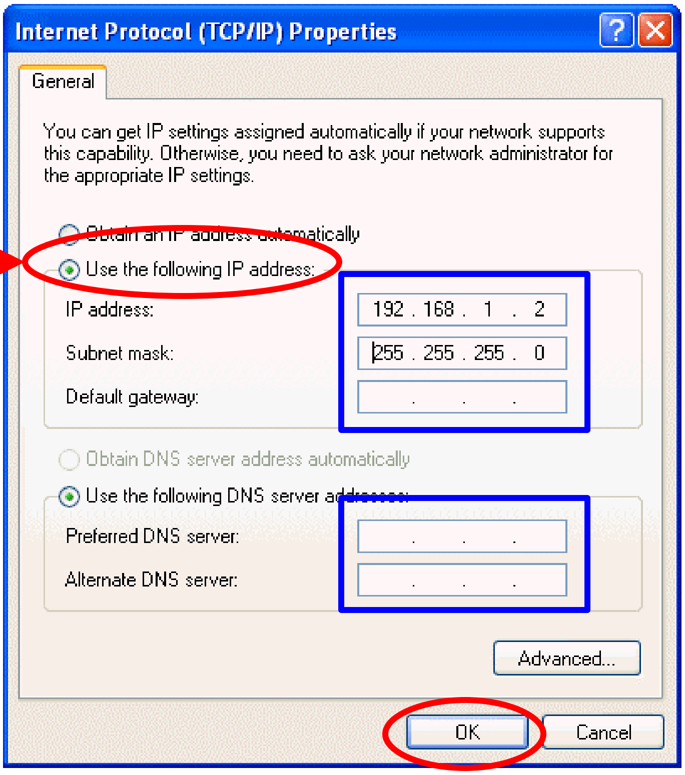
Static IP Address

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

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



Internet Protocol (TCP/IP) Properties

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

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

IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

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

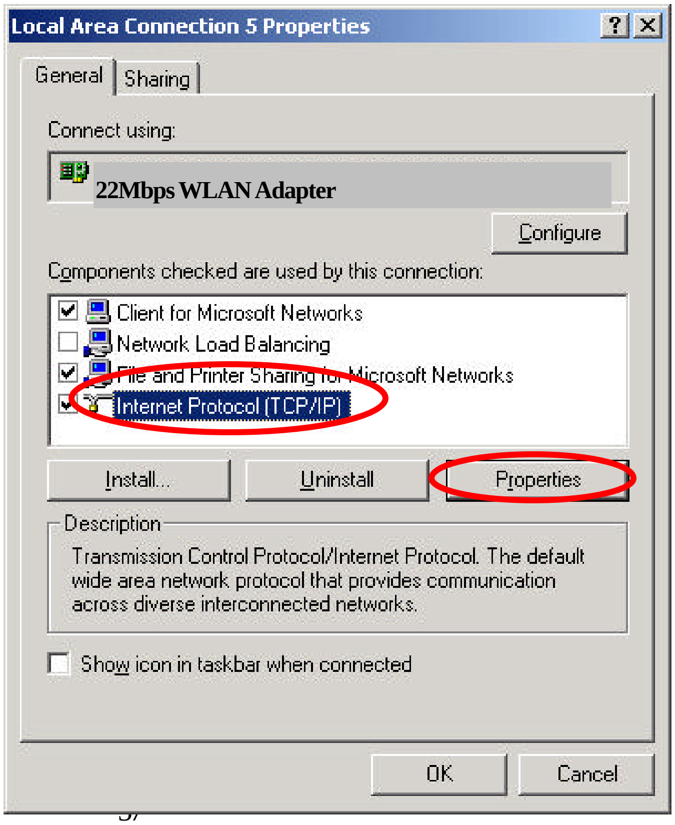
Preferred DNS server: . . .
Alternate DNS server: . . .

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:
22Mbps WLAN 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)

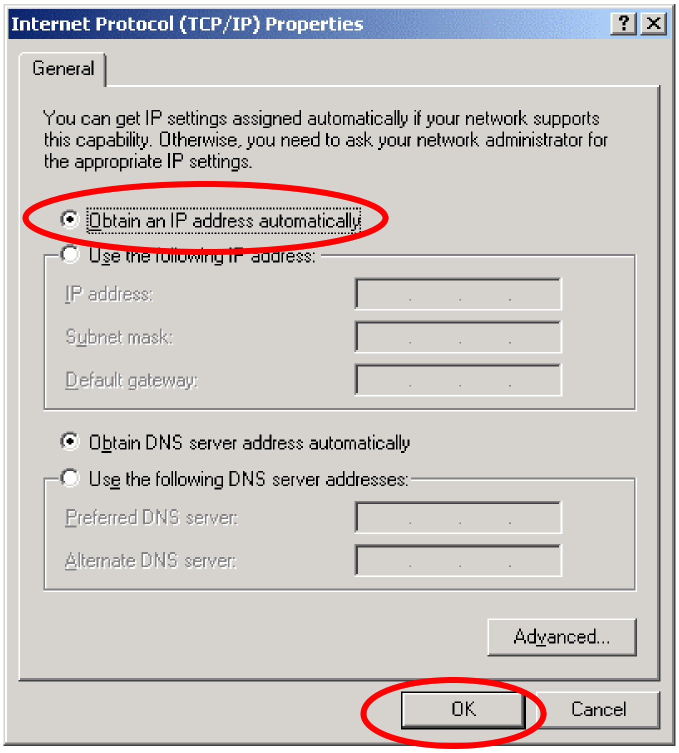
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ 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

General

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

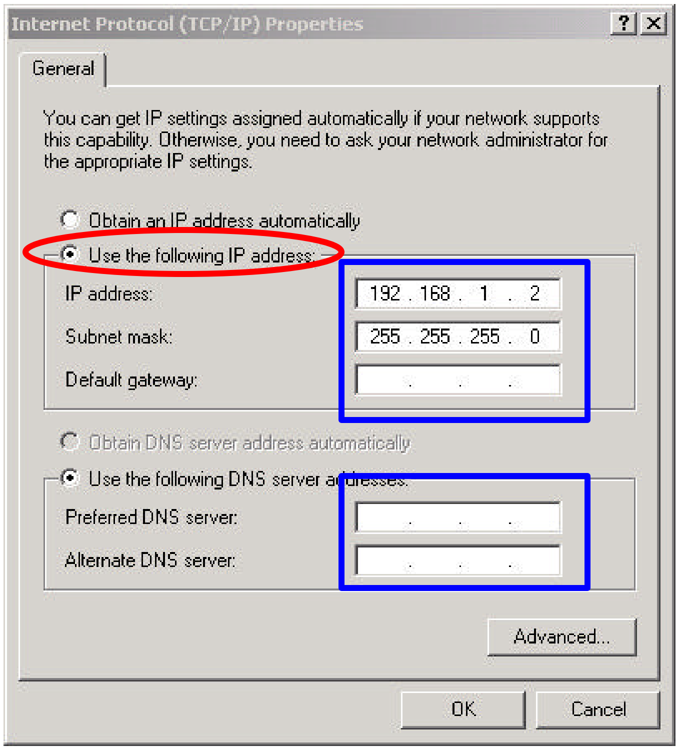
Select “**Use the following IP address**”

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

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

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

Click “**Ok**” to close the window



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

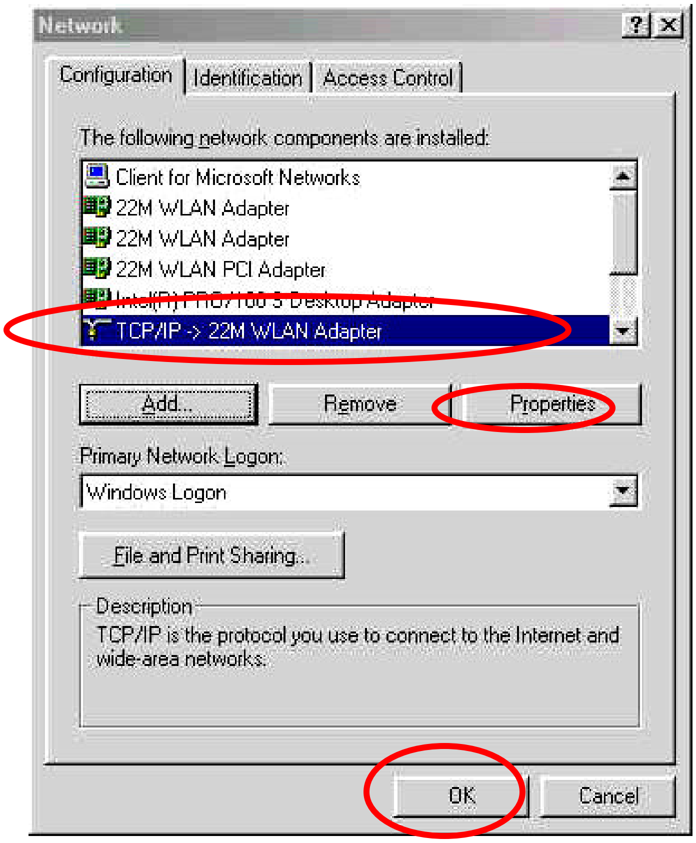
Alternate DNS server: . . .

Wireless Network In Windows 98 and Windows ME

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

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

Click "**Properties**" to continue



Network

Configuration | Identification | Access Control

The following network components are installed:

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

Primary Network Logon:
Windows Logon

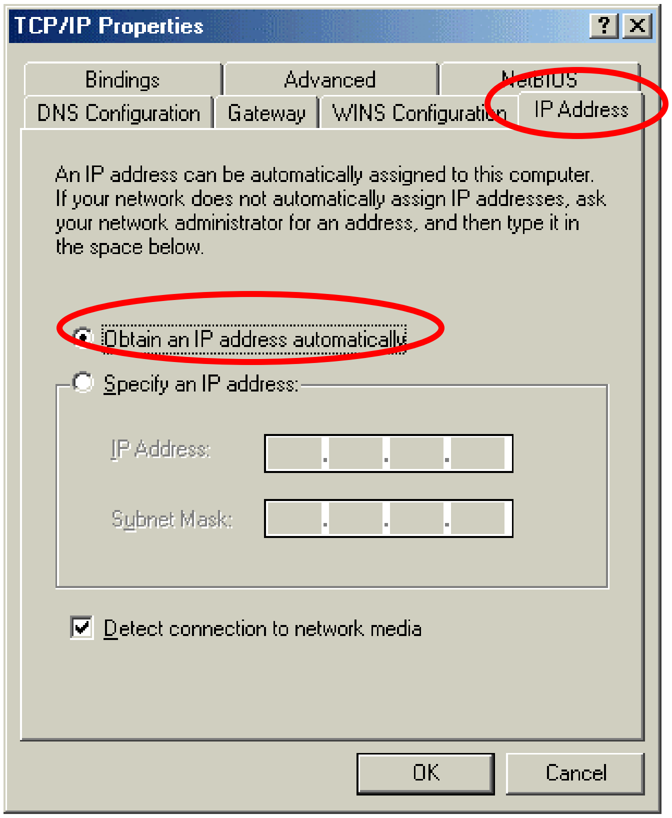
Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

The Access Point restarts itself, and the screen will switch back to startup page – Link Information

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

Bindings | Advanced | NetBIOS
DNS Configuration | Gateway | WINS Configuration | IP Address

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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

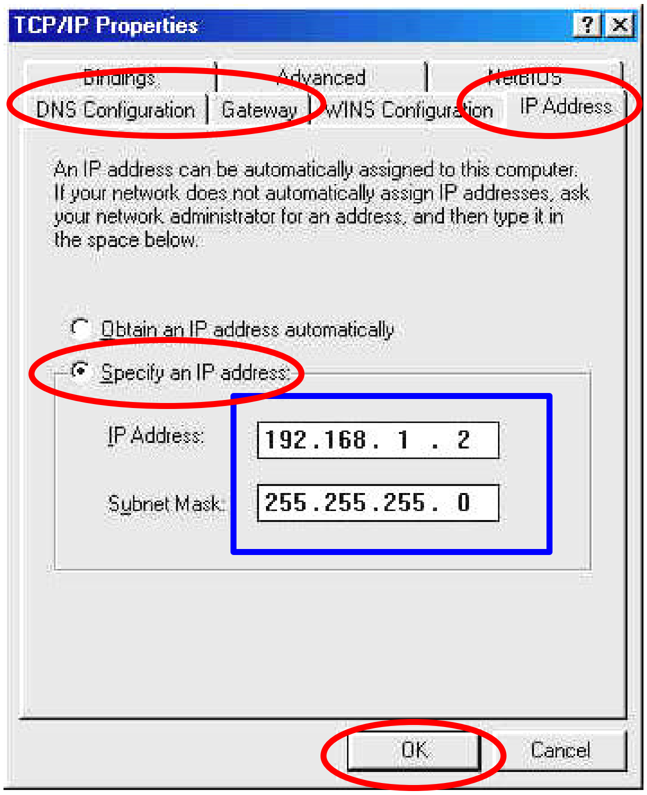
Subnet Mask: . . .

☑ 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



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:

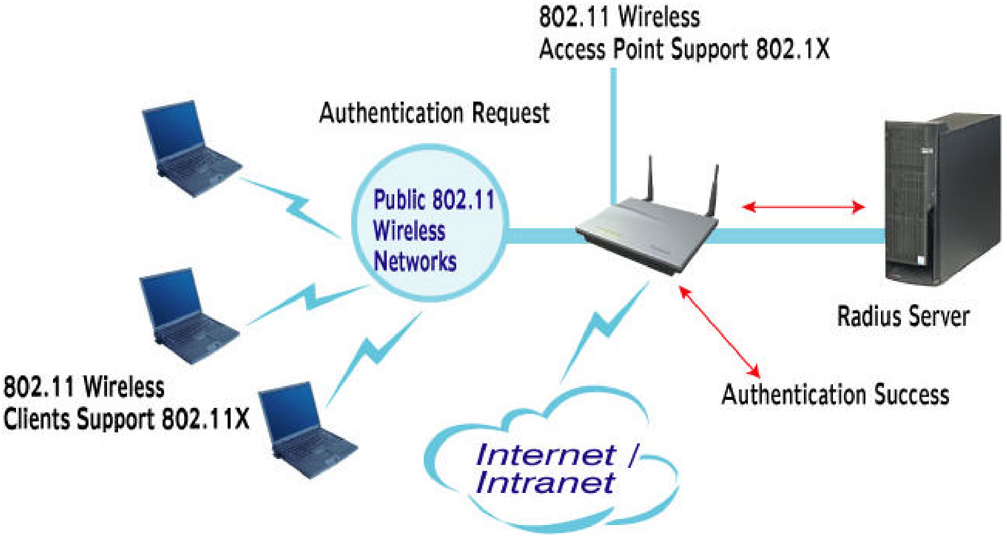
IP Address: 192.168. 1 . 2

Subnet Mask: 255.255.255. 0

APPENDIX C: 802.1x Authentication Setup

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

802.1x Authentication Infrastructure



The Infrastructure diagram showing above illustrates that a group of 802.11 wireless clients is trying to form a 802.11 wireless network with the Access Point in order to have access to the Internet/Intranet. In 802.1x authentication infrastructure, each of these wireless clients would have to be authenticated by the Radius server, which would grant the authorized client and notified the Access Point to open up a communication port to be used for the granted client. There are 2 Extensive Authentication Protocol (EAP) methods supported: (1) MD5 and (2) TLS.
MD5 authentication is simply a validation of existing user account and password that is stored in the server with what are keyed in by the user. Therefore, wireless client user will be prompted for account/password validation every time when he/she is trying to get connected. TLS authentication

is a more complicated authentication, which involves using certificate that is issued by the Radius server, for authentication. TLS authentication is a more secure authentication, since not only the Radius server authenticates the wireless client, but also the client can validate the Radius server by the certificate that it issues. The authentication request from wireless clients and reply by the Radius Server and Access Point process can be briefed as follows:

1. The client sends an EAP start message to the Access Point
2. The Access Point replies with an EAP Request ID message
3. The client sends its Network Access Identifier (NAI) – its user name – to the Access Point in an EAP Respond message.
4. The Access Point forwards the NAI to the RADIUS server with a RADIUS Access Request message.
5. The RADIUS server responds to the client with its digital certificate.
6. The client validates the digital certificate, and replies its own digital certificate to the RADIUS server.
7. The RADIUS server validates client's digital certificate.
8. The client and RADIUS server derive encryption keys.
9. The RADIUS server sends the access point a RADIUS ACCEPT message, including the client's WEP key.
10. The Access Point sends the client an EAP Success message along with the broadcast key and key length, all encrypted with the client's WEP key.

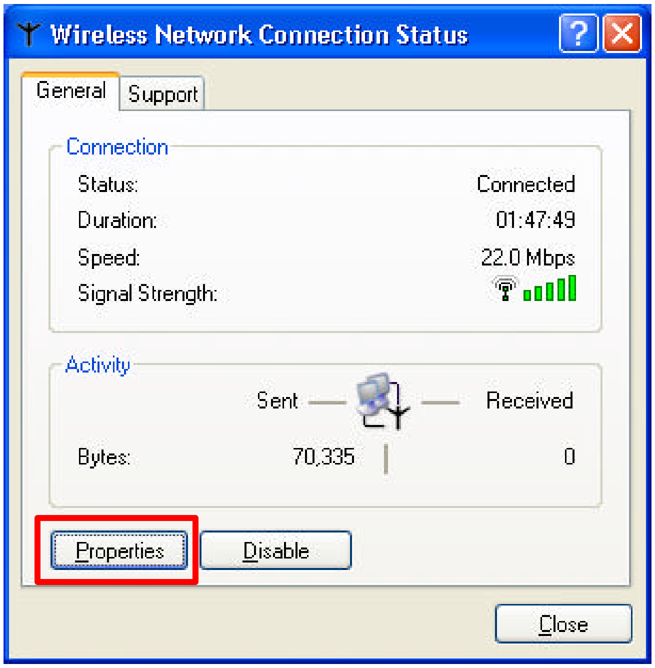
Supplicant: Wireless Network PC Card

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

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

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

4. Click ‘**Properties**” to open up the Properties setting window.



Status: Connected

Duration: 01:47:49

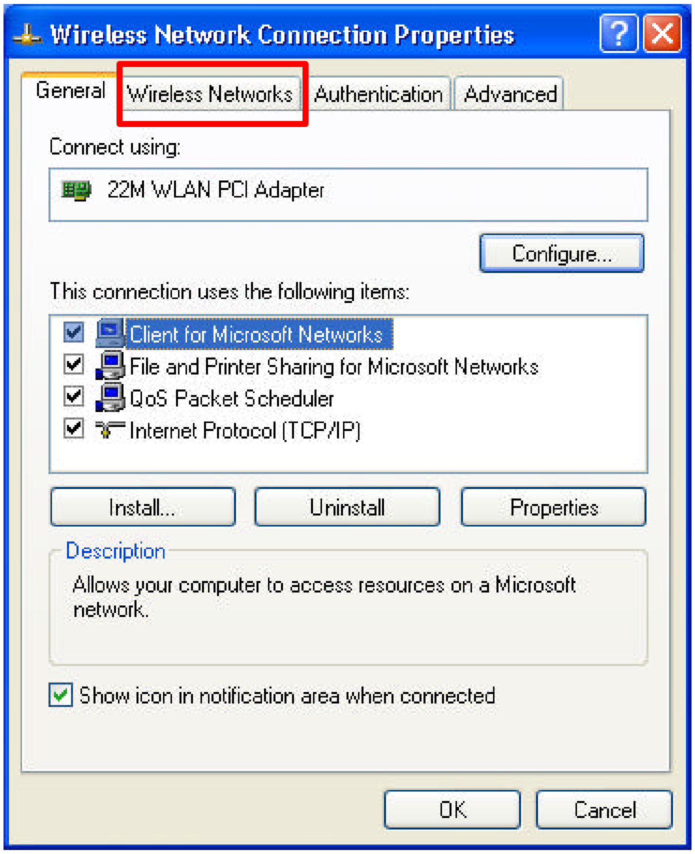
Speed: 22.0 Mbps

Signal Strength:

Sent — — Received

Bytes: 70,335 | 0

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



Connect using:

22M WLAN PCI Adapter

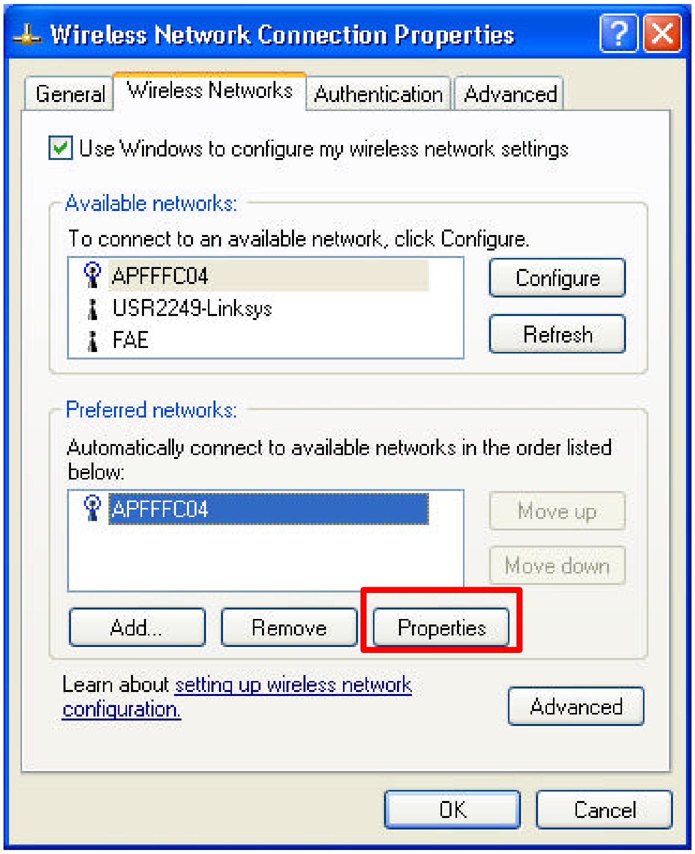
This connection uses the following items:

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

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.



☑ Use Windows to configure my wireless network settings

To connect to an available network, click Configure.

APFFFC04
USR2249-Linksys
FAE

Automatically connect to available networks in the order listed below:

APFFFC04

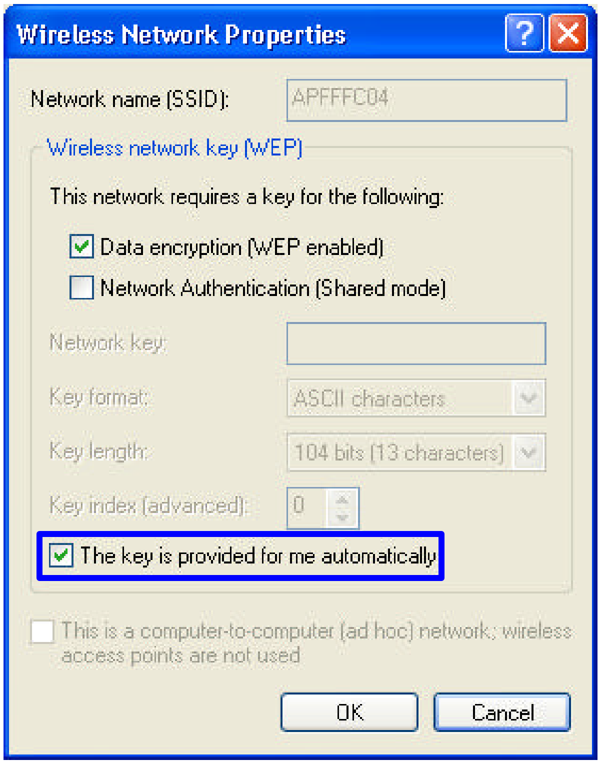
Learn about setting up wireless network configuration.

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



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: 104 bits (13 characters)

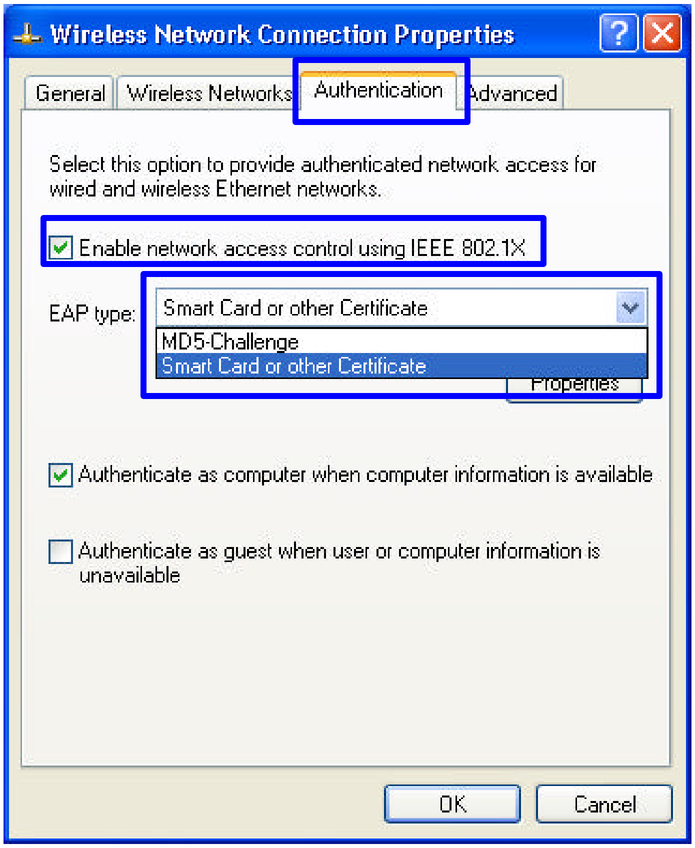
Key index (advanced): 0

☑ 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

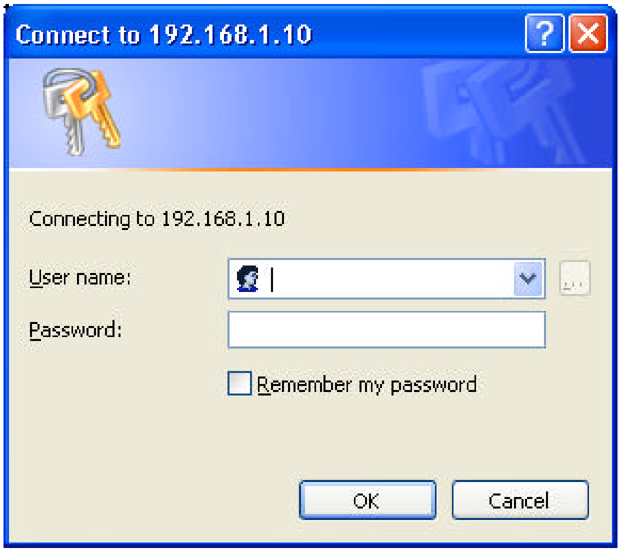
12. Click "**OK**" to close the Wireless Network Connection Properties window, thus make the changes effective.

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/passw ord, CA server location and etc. The following illustration is based on obtaining a certificate from Windows 2000 Server which can act as a CA server, assuming you have a valid account/password to access the server.

13. Connect to the server and ask for access, and the server will prompt you to enter your user name and password.
14. Enter your **user name** and **password**, then click "**OK**" to continue.



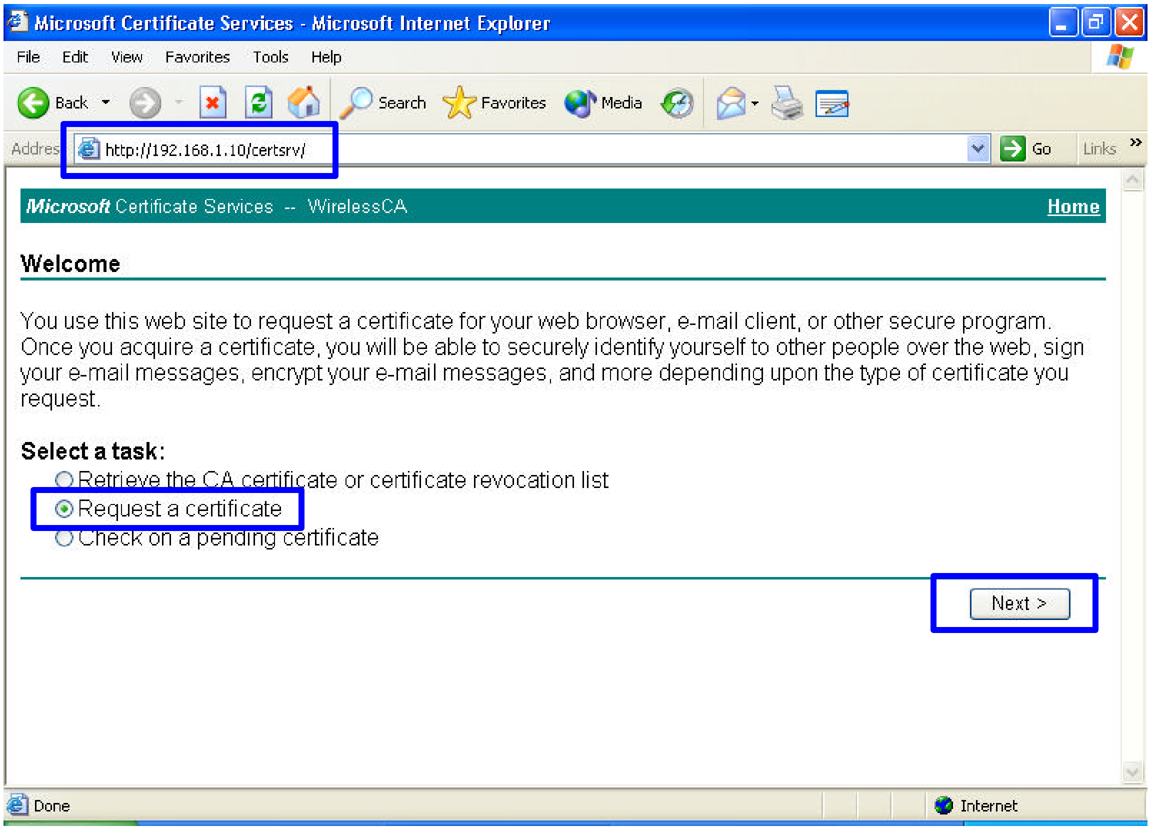
Please note that we use IP addresses for connection with the server for our illustration, and the IP of the server is 192.168.1.10.

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

http://192.168.1.10/certsrv

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

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



Microsoft Certificate Services -- WirelessCA

Home

http://192.168.1.10/certsrv/

Welcome

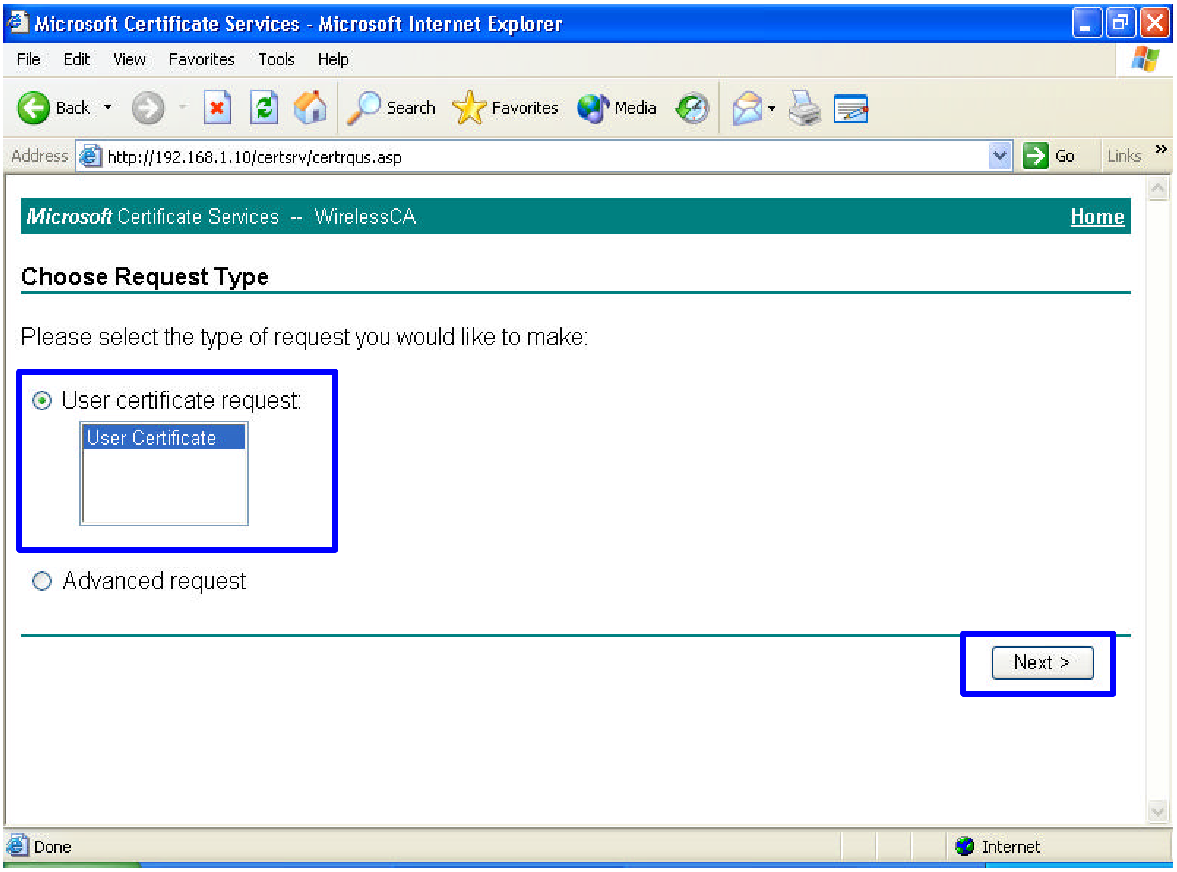
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the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

Select a task:

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

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Next >
Done
Internet

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



Microsoft Certificate Services - Microsoft Internet Explorer

http://192.168.1.10/certsrv/certrqus.asp

Microsoft Certificate Services -- WirelessCA

Choose Request Type

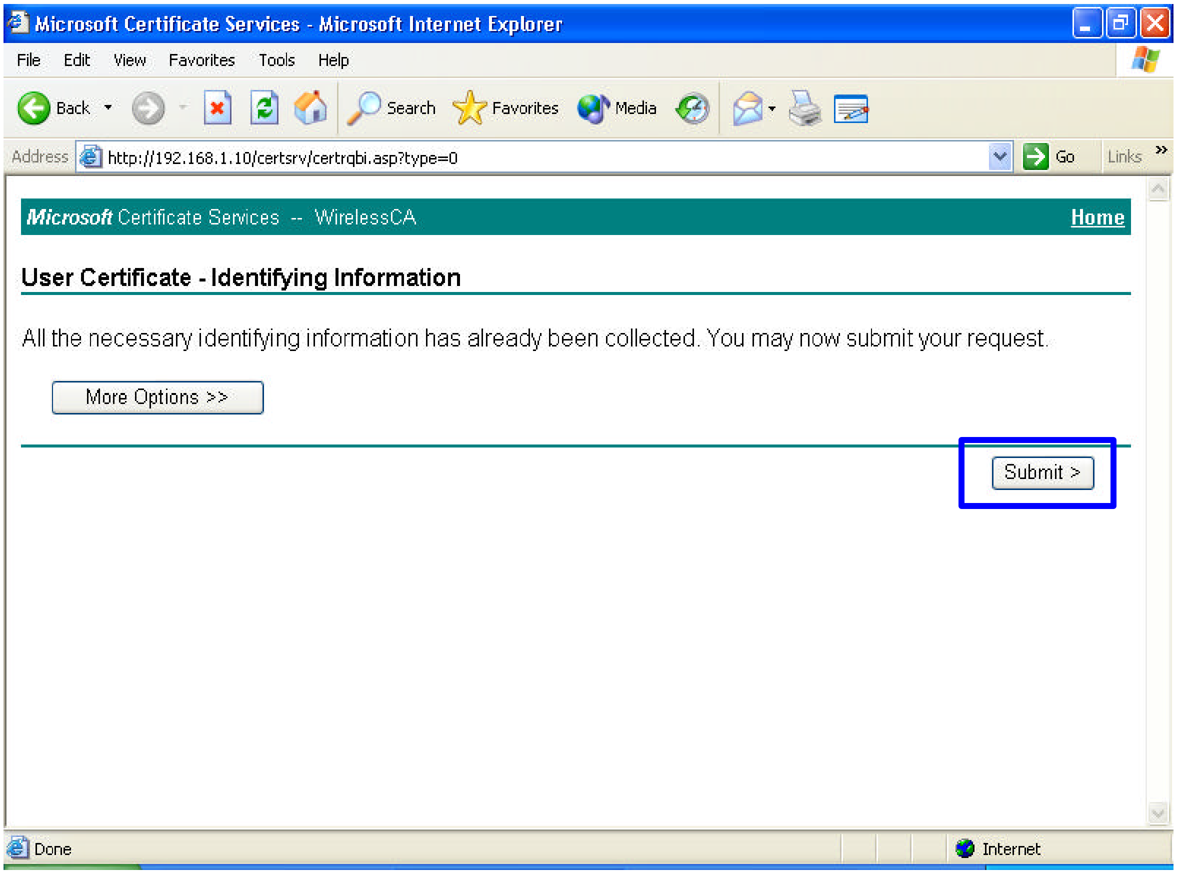
Please select the type of request you would like to make:

● User certificate request:

User Certificate

○ Advanced request

18. Click “**Submit >**” to continue.



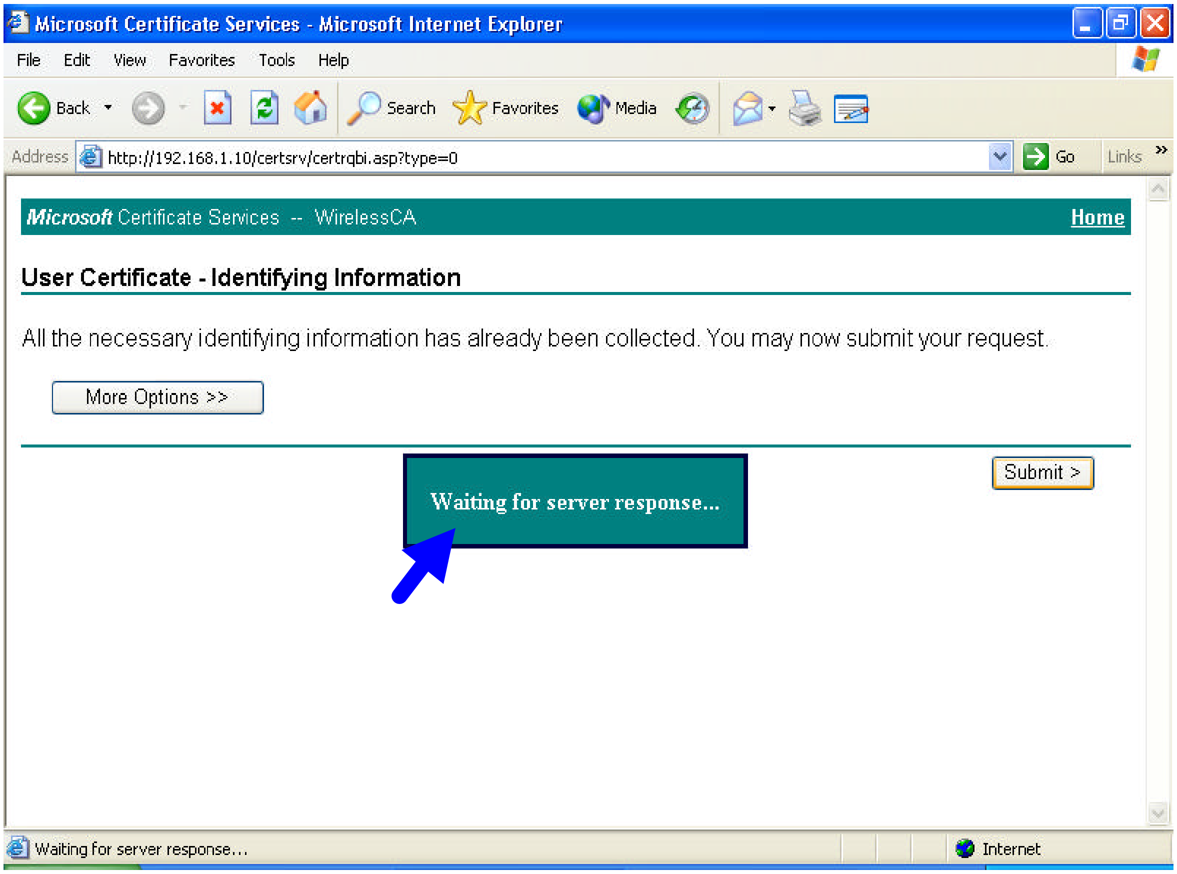
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrqbi.asp?type=0
Go Links
Microsoft Certificate Services -- WirelessCA
Home

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
Go
Links

http://192.168.1.10/certsrv/certrqbi.asp?type=0

Microsoft Certificate Services -- WirelessCA

Home

User Certificate - Identifying Information

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

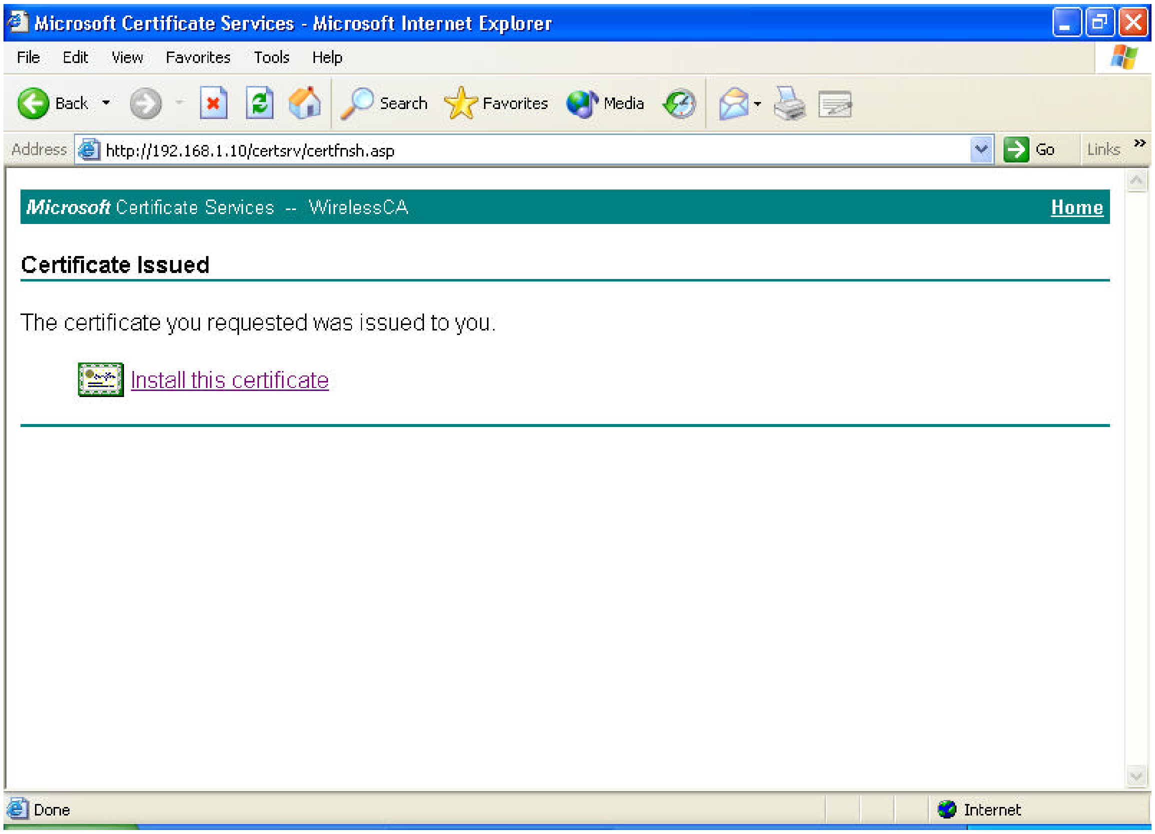
More Options >>

Submit >

Waiting for server response...

Waiting for server response...

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

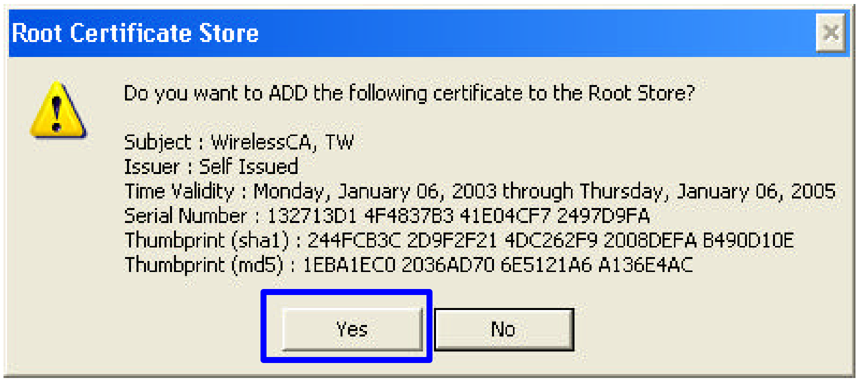

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://192.168.1.10/certsrv/certfnsh.asp
Go
Links
Microsoft Certificate Services -- WirelessCA
Home
Done
Internet

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

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

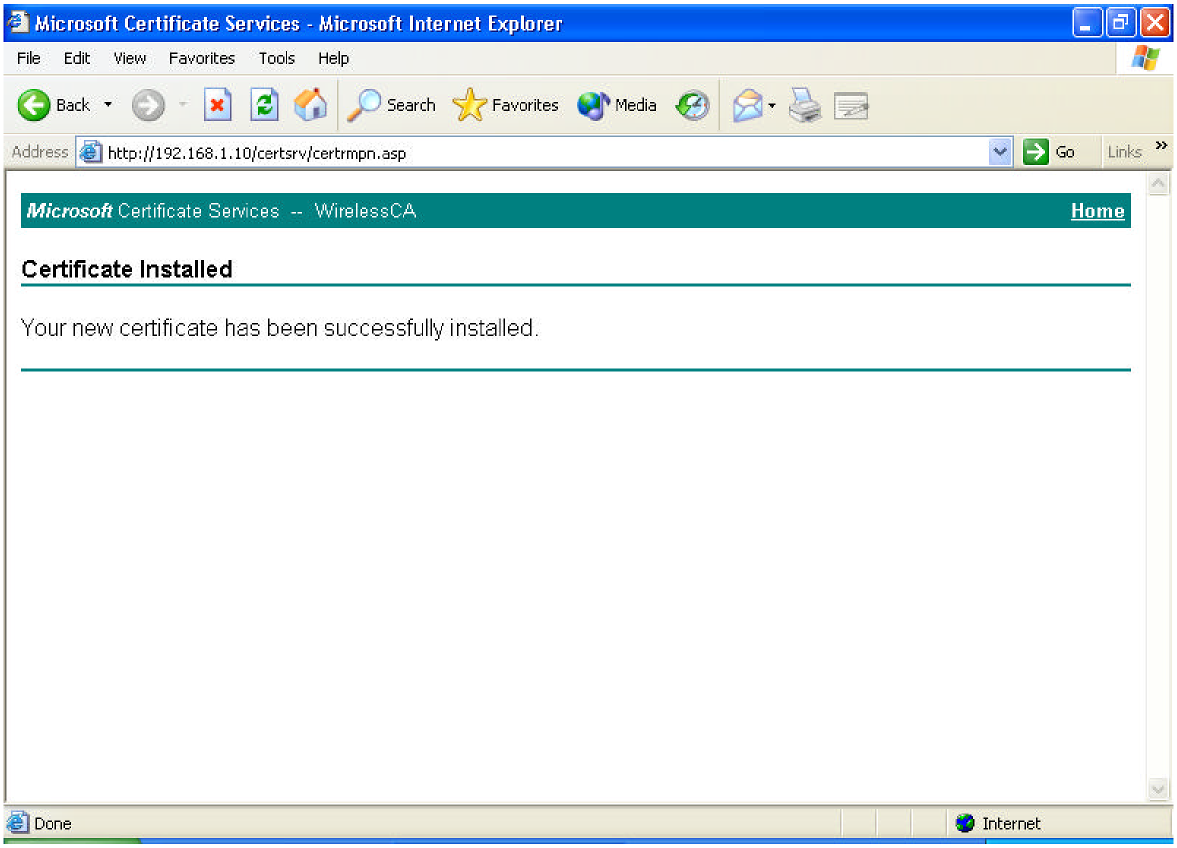


Root Certificate Store

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
Go
Links
Home
Done
Internet

http://192.168.1.10/certsrv/certrmpn.asp

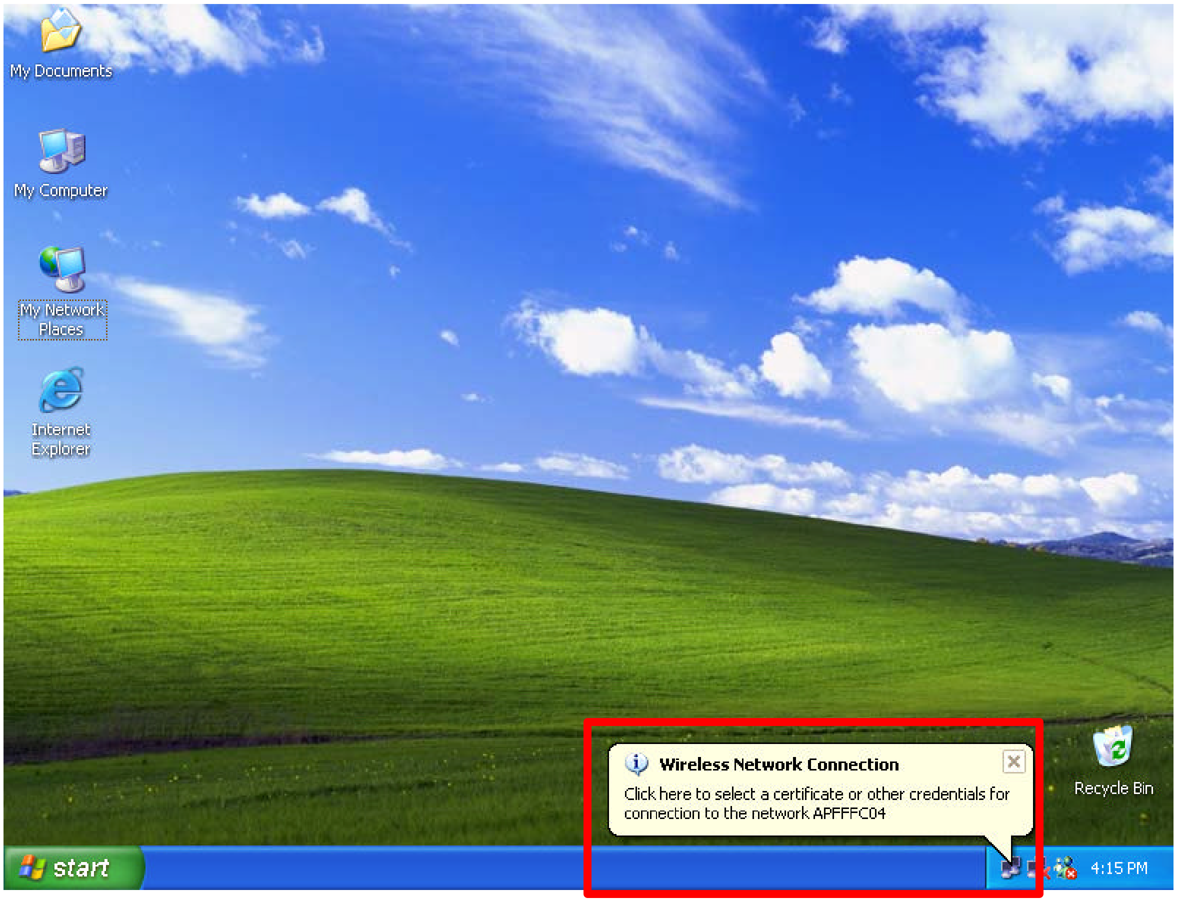
Microsoft Certificate Services -- WirelessCA

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.

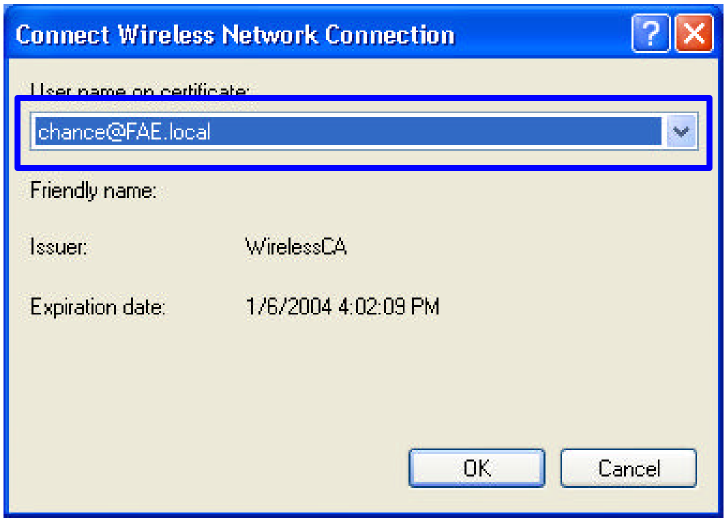
23. Windows XP will prompt you to select a certificate for wireless network connection. Click on the network connection icon in the system tray to continue.



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.



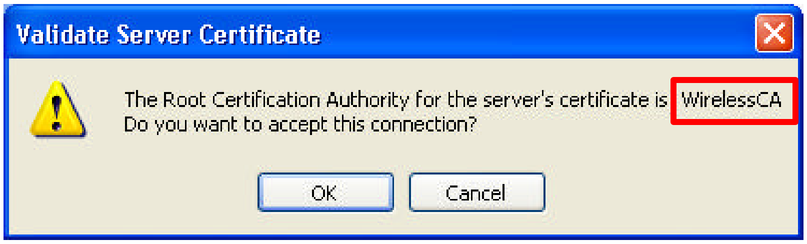
User name on certificate: chance@FAE.local

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.

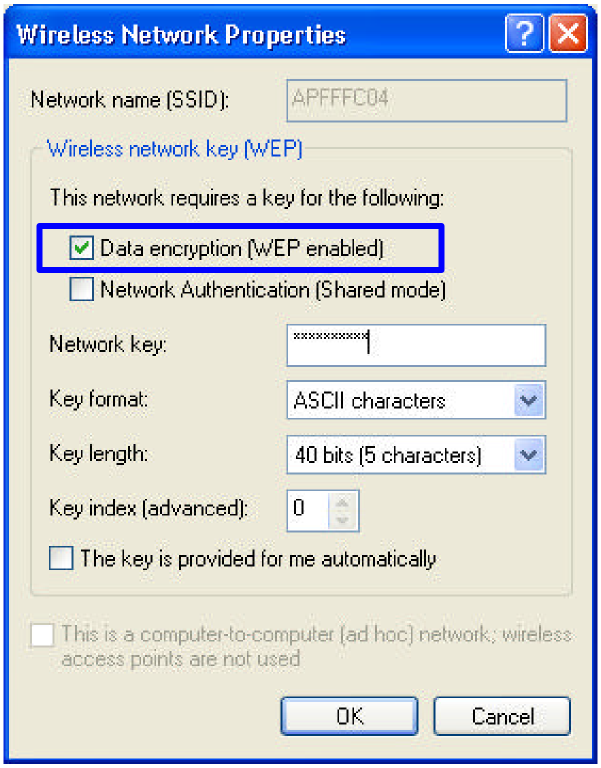


The Root Certification Authority for the server's certificate is WirelessCA
Do you want to accept this connection?

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.



Network name (SSID): APFFFC04

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

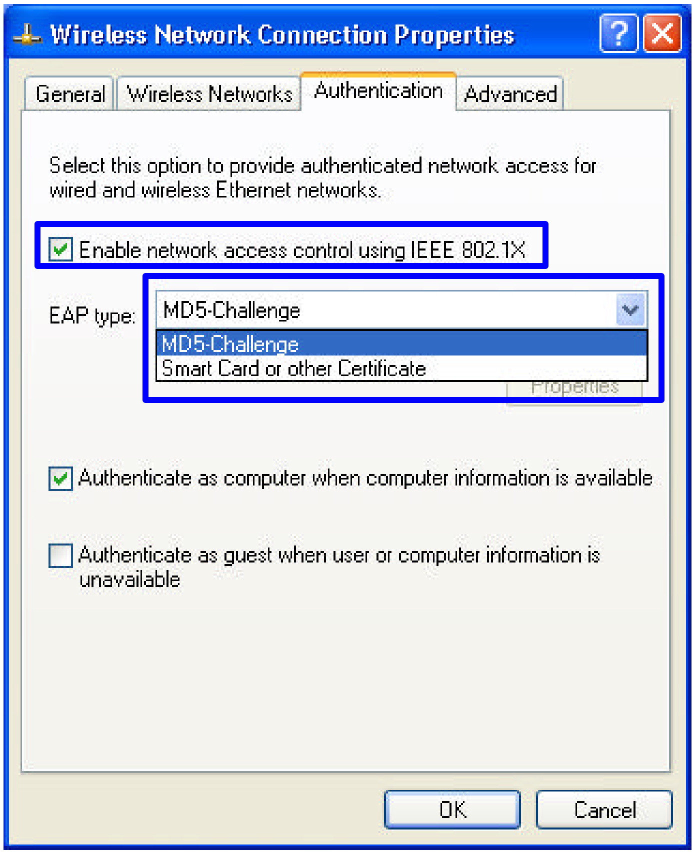
□ The key is provided for me automatically

□ 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

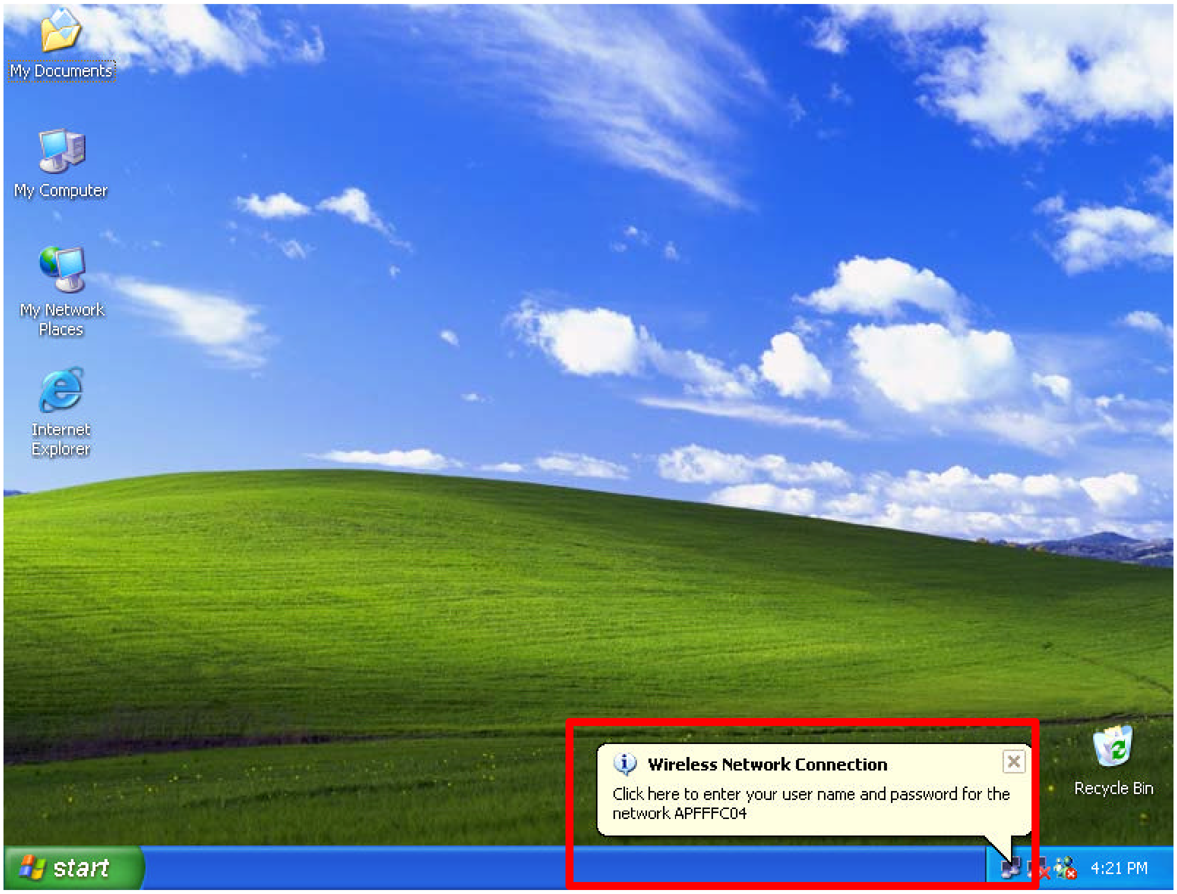
☑ Authenticate as computer when computer information is available

□ 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.

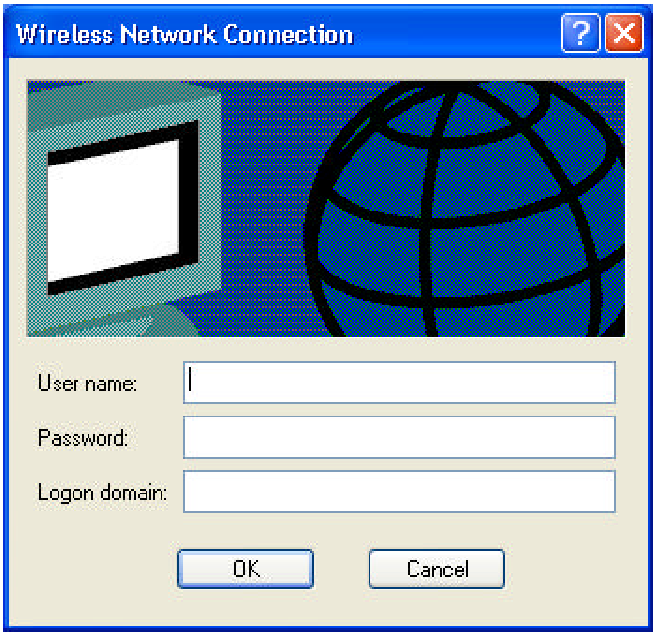


Wireless Network Connection

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

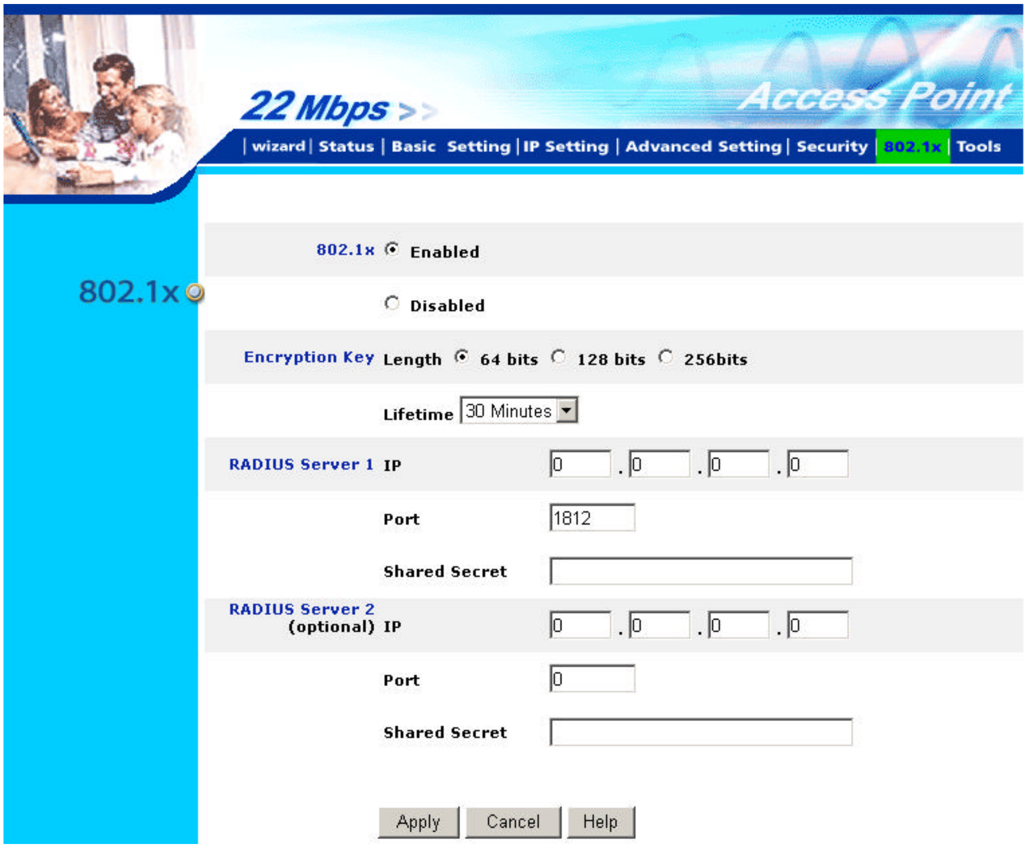
User name:

Password:

Logon domain:

Authenticator: Wireless Network Access Point

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


22 Mbps >>
Access Point
| 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 ○ 256bits

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

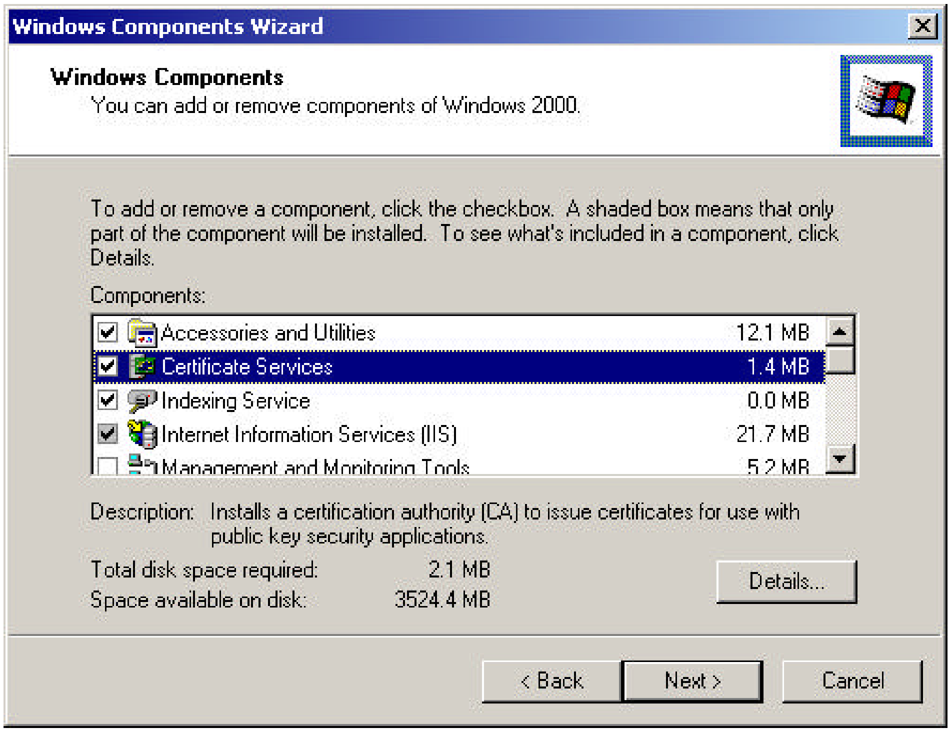
1. Enable 802.1x security by selecting "**Enable** ".
2. If **MD5** EAP methods is used then you can skip step 3 and go to step 4.
3. Select the **Encryption Key Length Size** ranging from 64 to 256 Bits that you would like to use. Select the **Lifetime of the Encryption Key** from 5 Minutes to 1 Day. 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.

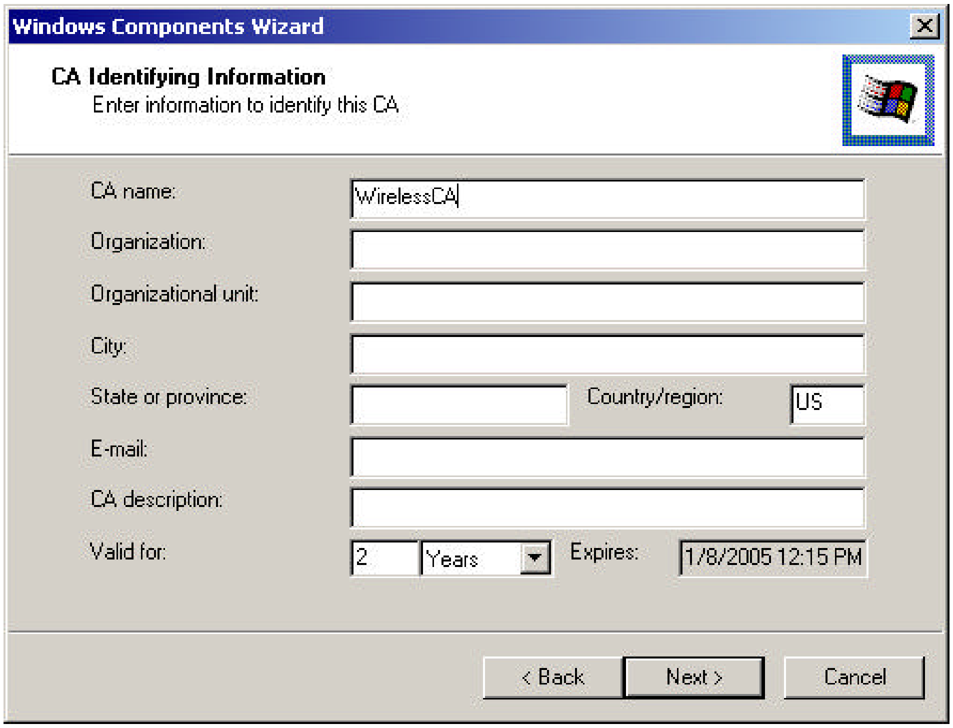
Components:

☑	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
CA Identifying Information
Enter information to identify this CA
< Back
Next >
Cancel

CA name: WirelessCA

Organization:

Organizational unit:

City:

State or province:

Country/region: US

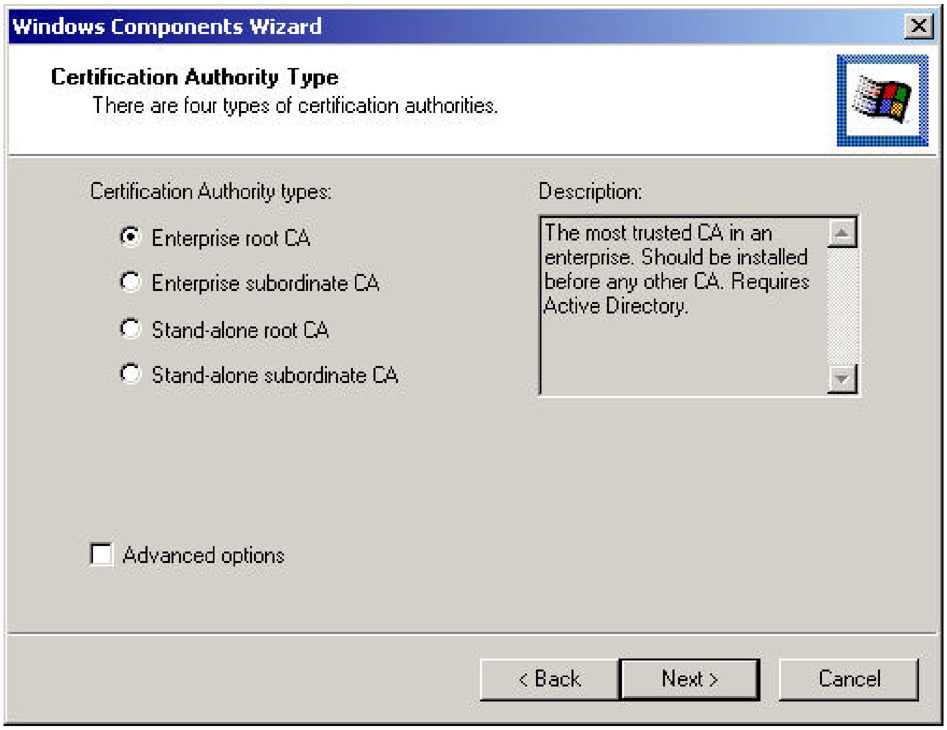
E-mail:

CA description:

Valid for: 2 Years

Expires: 1/8/2005 12:15 PM

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



Windows Components Wizard
Certification Authority Type
There are four types of certification authorities.
< Back
Next >
Cancel

Certification Authority types:

● Enterprise root CA

○ Enterprise subordinate CA

○ Stand-alone root CA

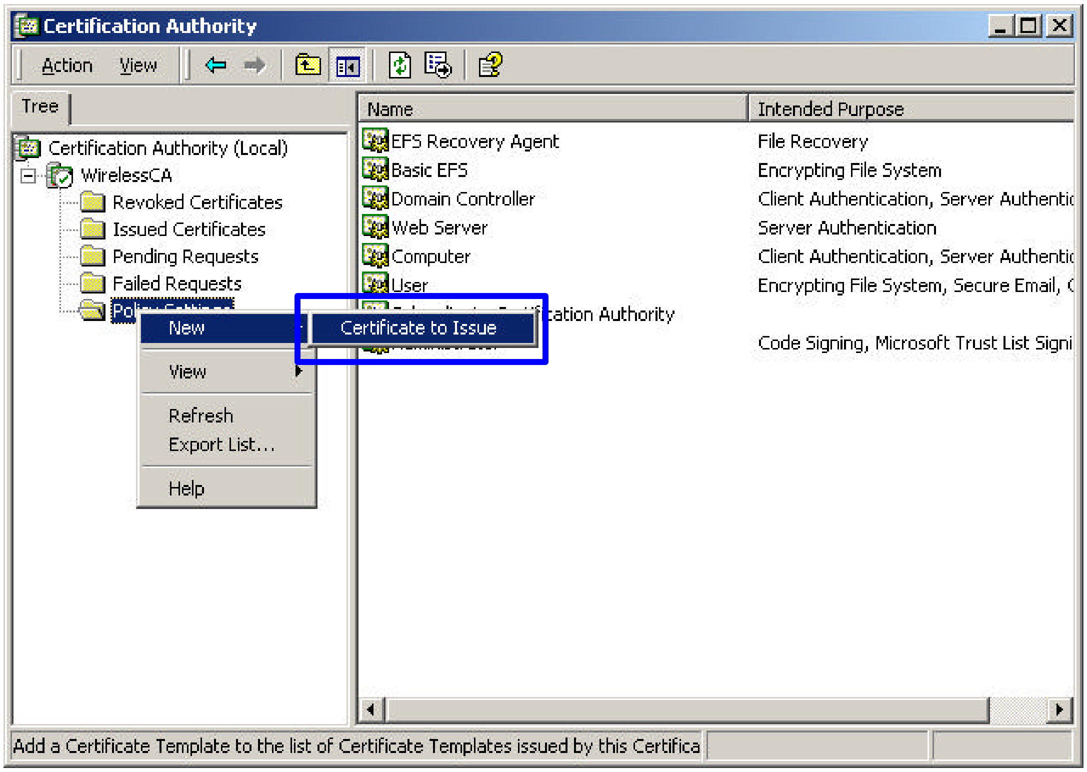
○ Stand-alone subordinate CA

Description:

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

□ Advanced options

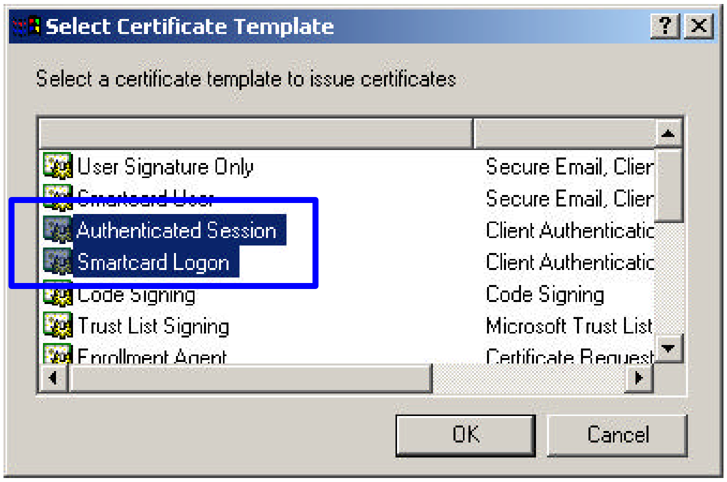
7. Go to Start > Program > Administrative Tools > **Certificate Authority**
8. Right-click on the "**Policy Setting**", select "**new**"
9. Select "**Certificate to Issue**"



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, (
cation 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.

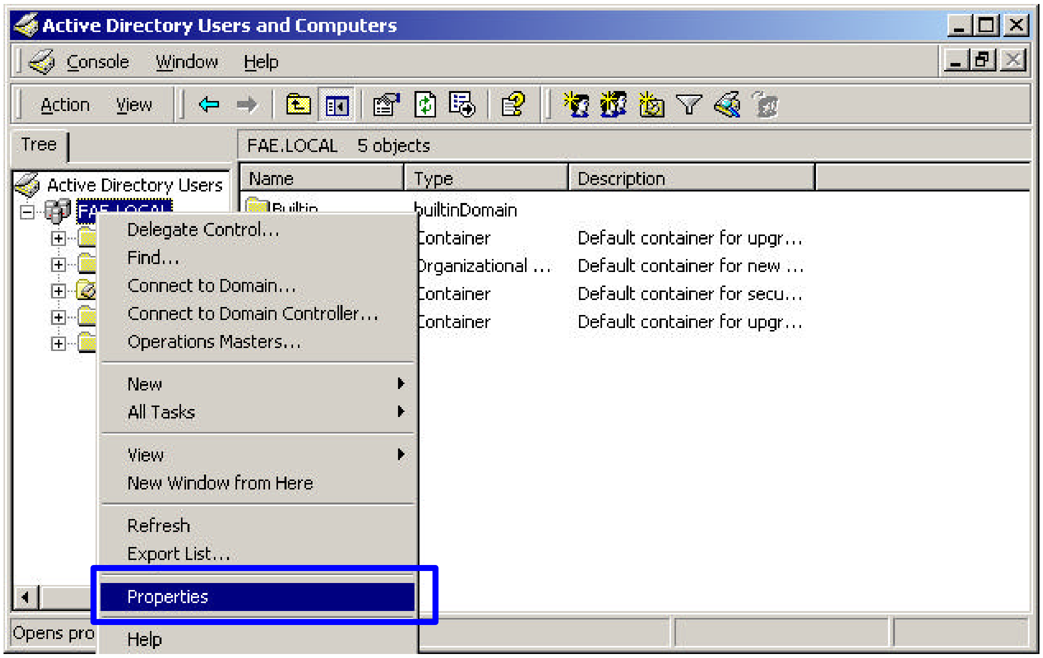


Select a certificate template to issue certificates

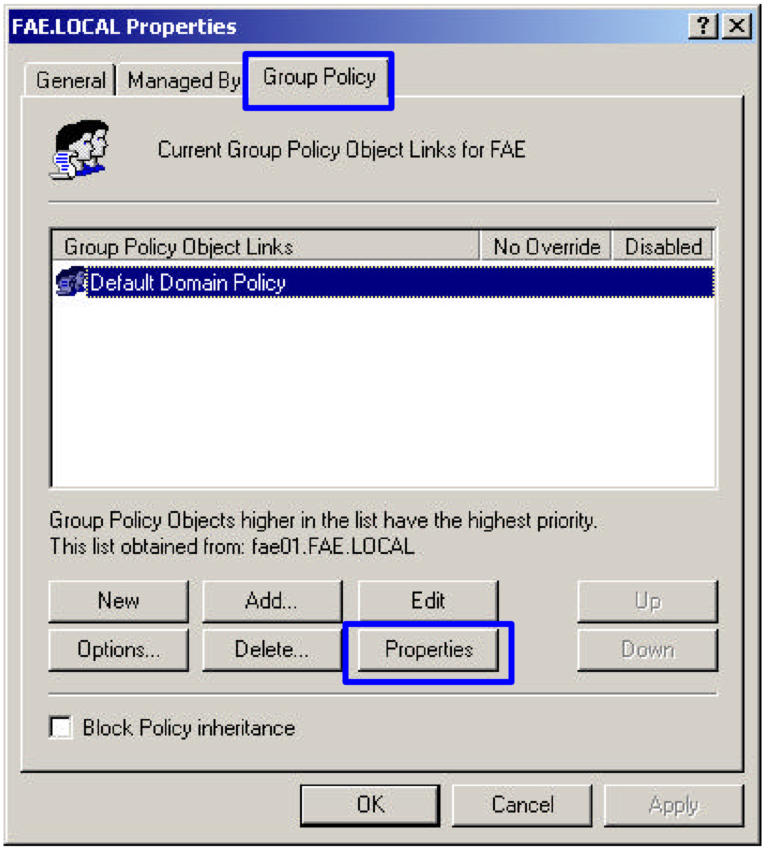
User Signature Only	Secure Email, Clier
Smartcard User	Secure Email, Clier
Authenticated Session	Client Authenticatic
Smartcard Logon	Client Authenticatic
Code Signing	Code Signing
Trust List Signing	Microsoft Trust List
Enrollment Agent	Certificate Request

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

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



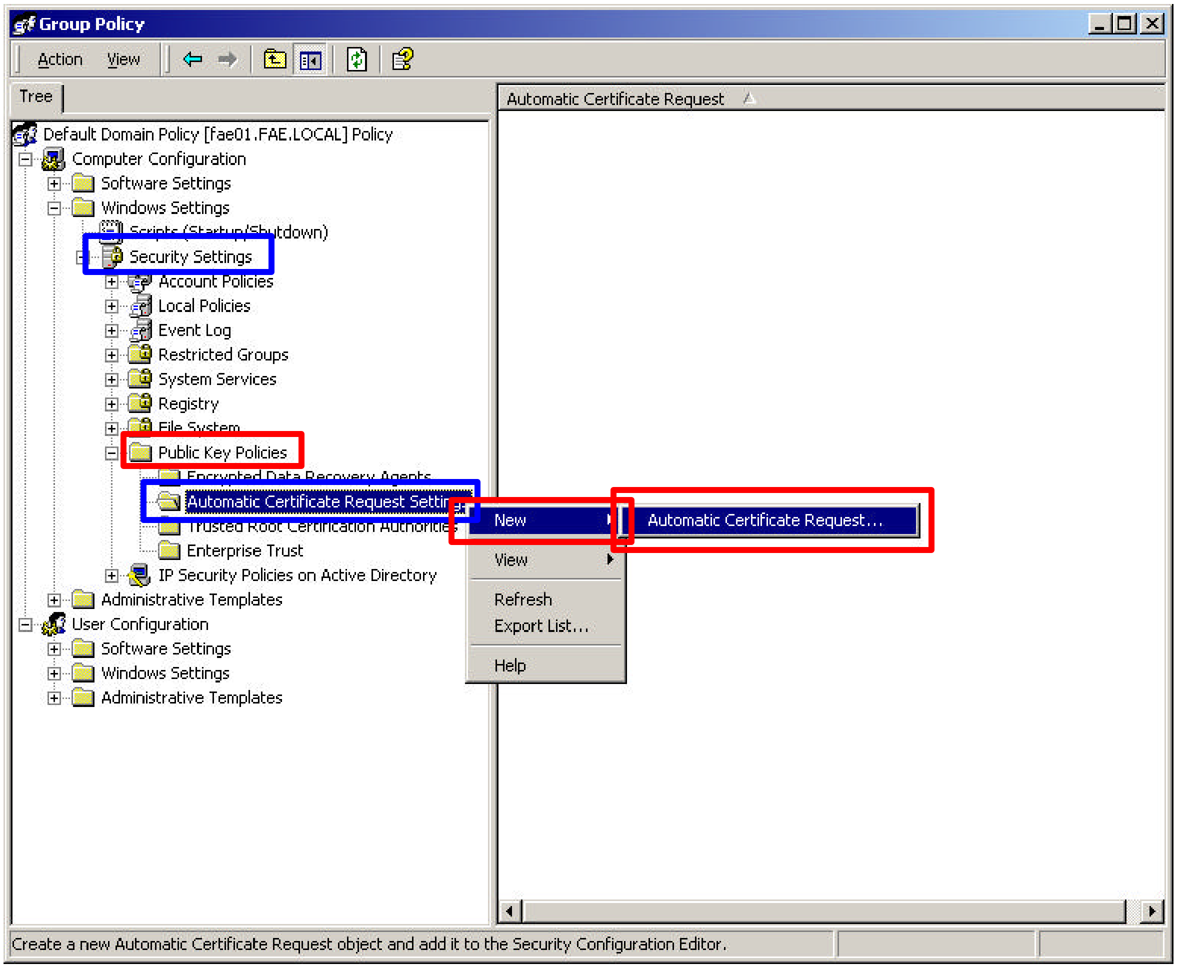
13. Select “**Group Policy**” tab and click “**Properties**” to continue.



Group Policy Object Links	No Override	Disabled
Default Domain Policy		

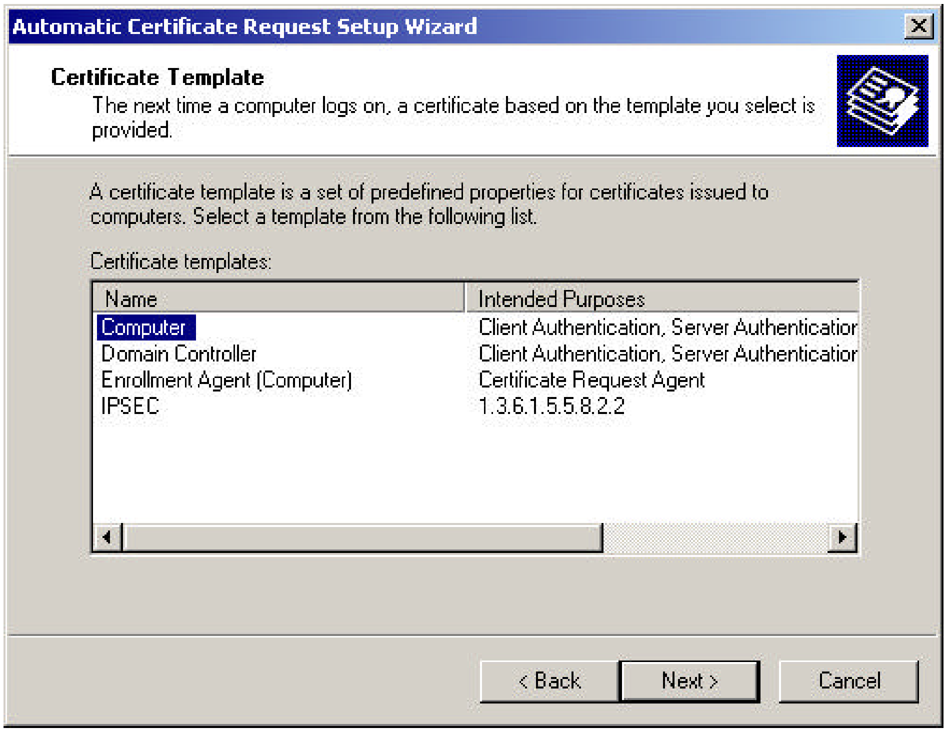
Group Policy Objects higher in the list have the highest priority.
This list obtained from: fae01.FAE.LOCAL

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.

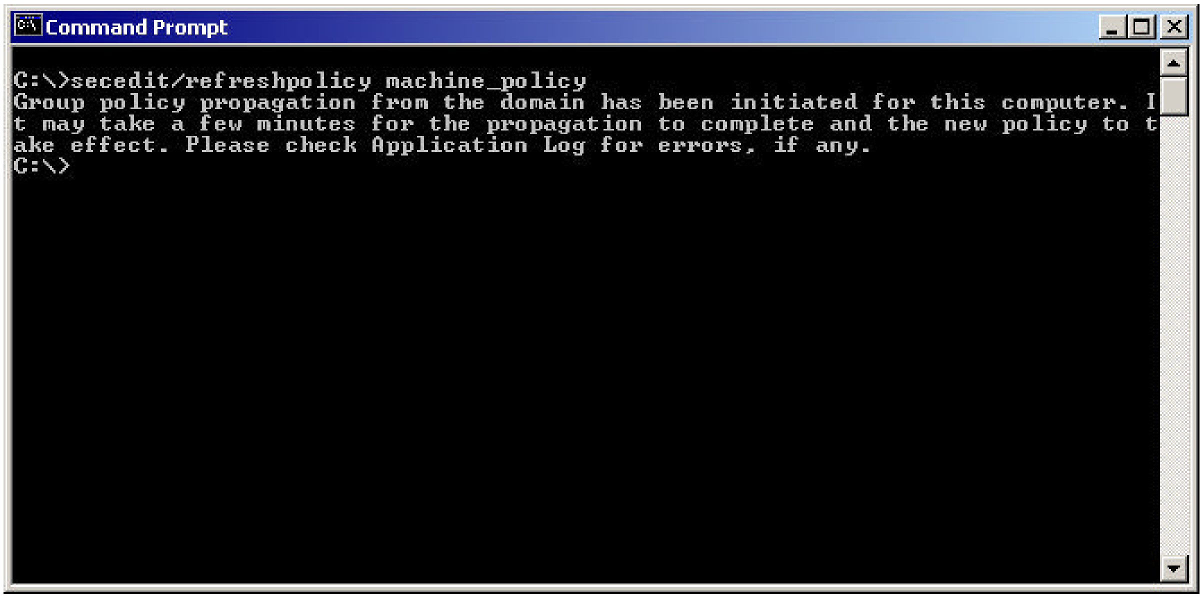
A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

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.

Adding Internet Authentication Service

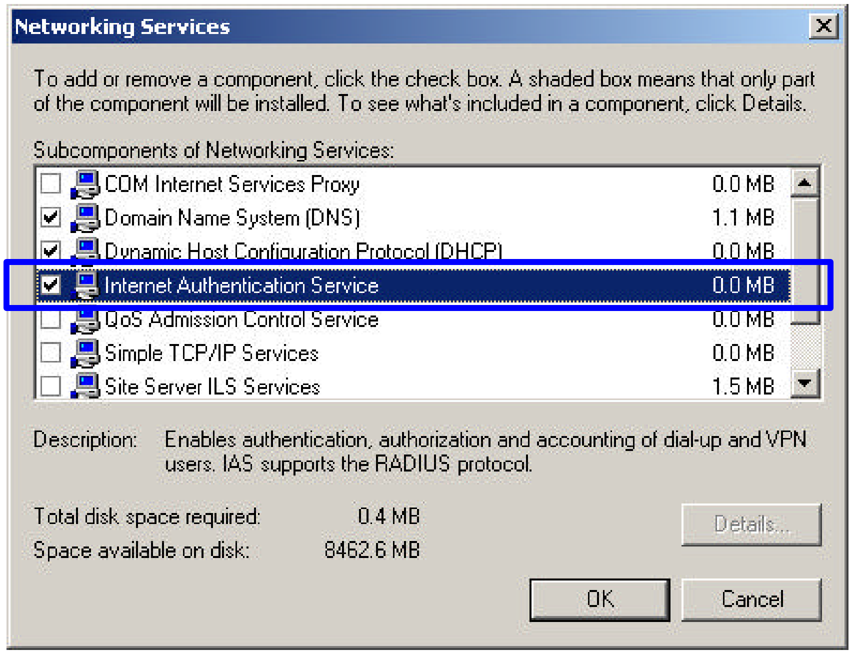


```
C:\>secedit/refreshpolicy machine_policy
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>
```

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

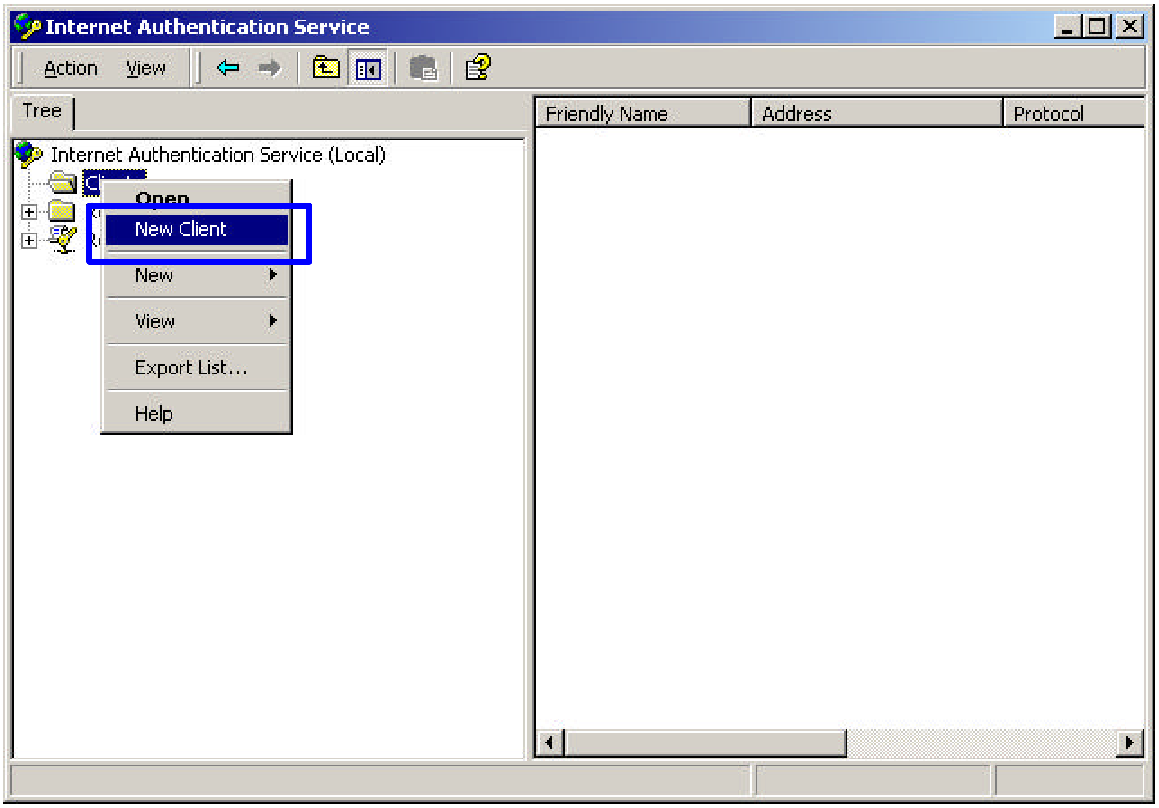
Description: Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.

Total disk space required: 0.4 MB

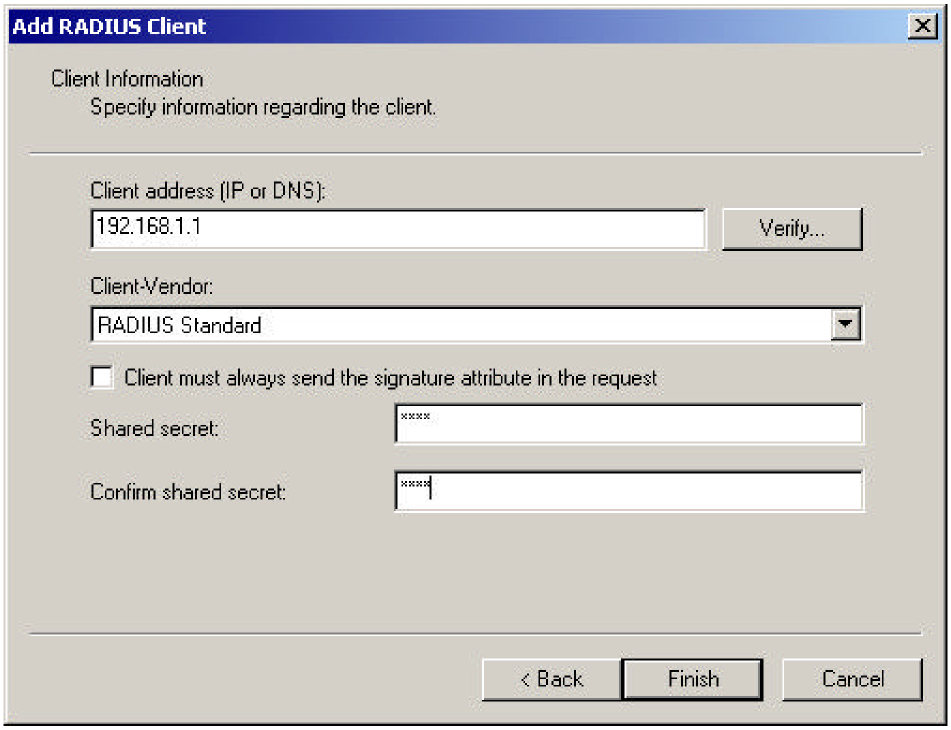
Space available on disk: 8462.6 MB

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

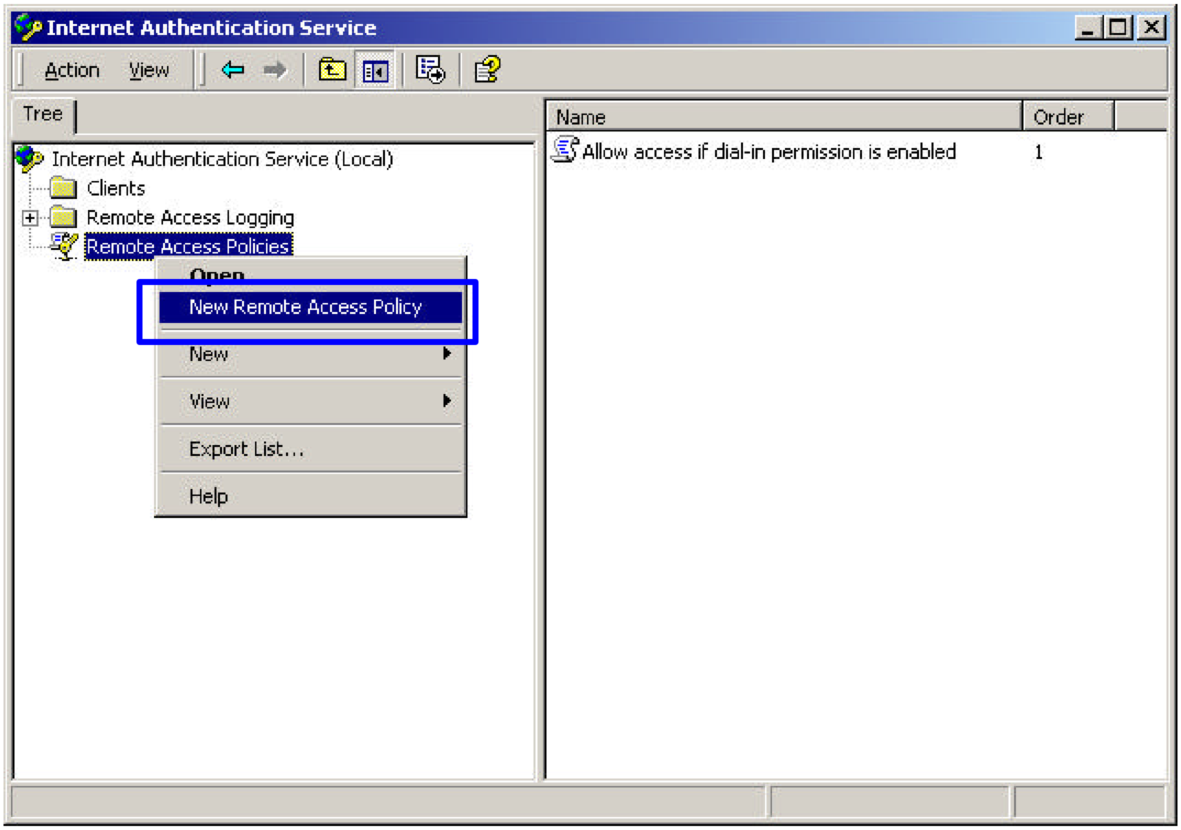
□ Client must always send the signature attribute in the request

Shared secret: ****

Confirm shared secret: ****

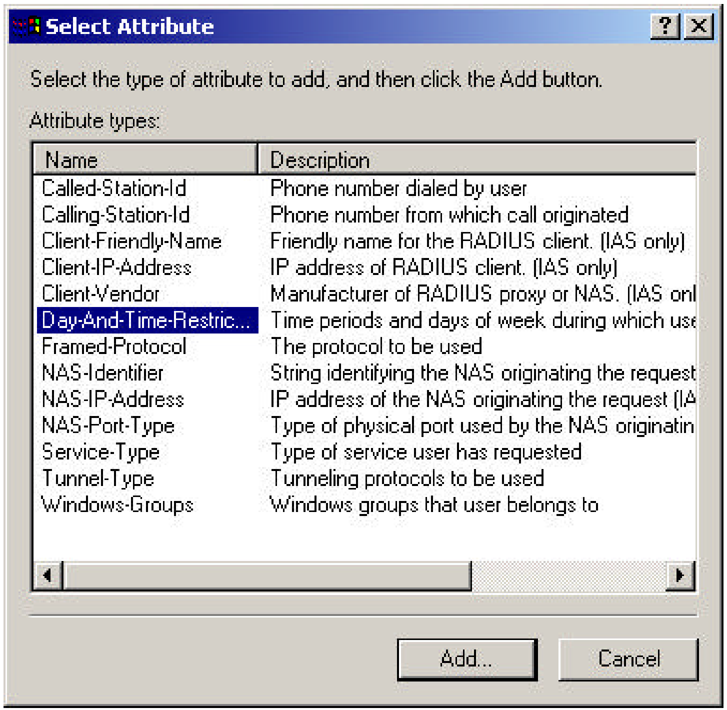
28. In the Internet Authentication Service, right-click “**Remote Access Policies**”

29. Select “New Remote Access Policy”.



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

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

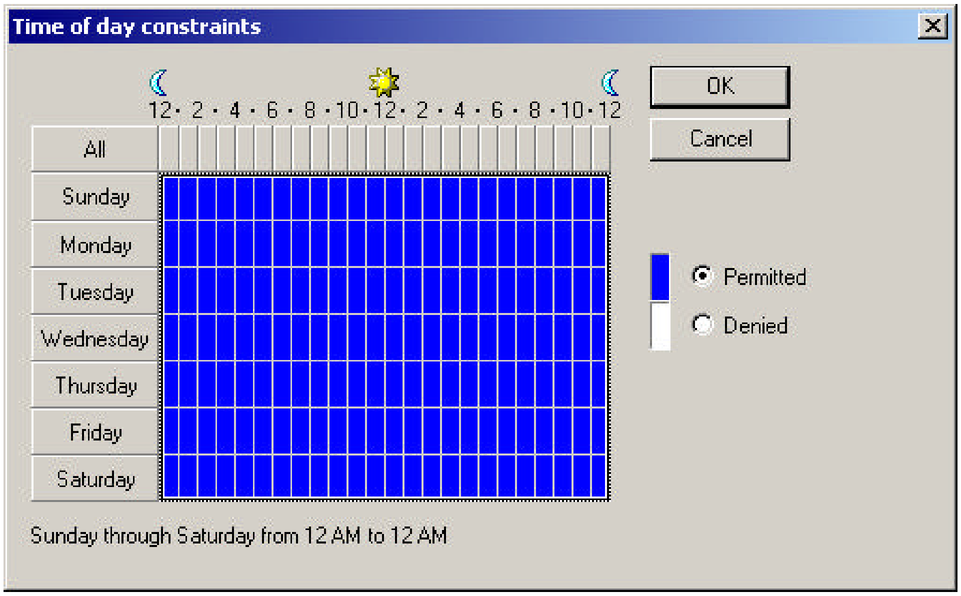


Select the type of attribute to add, and then click the Add button.

Attribute types:

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

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

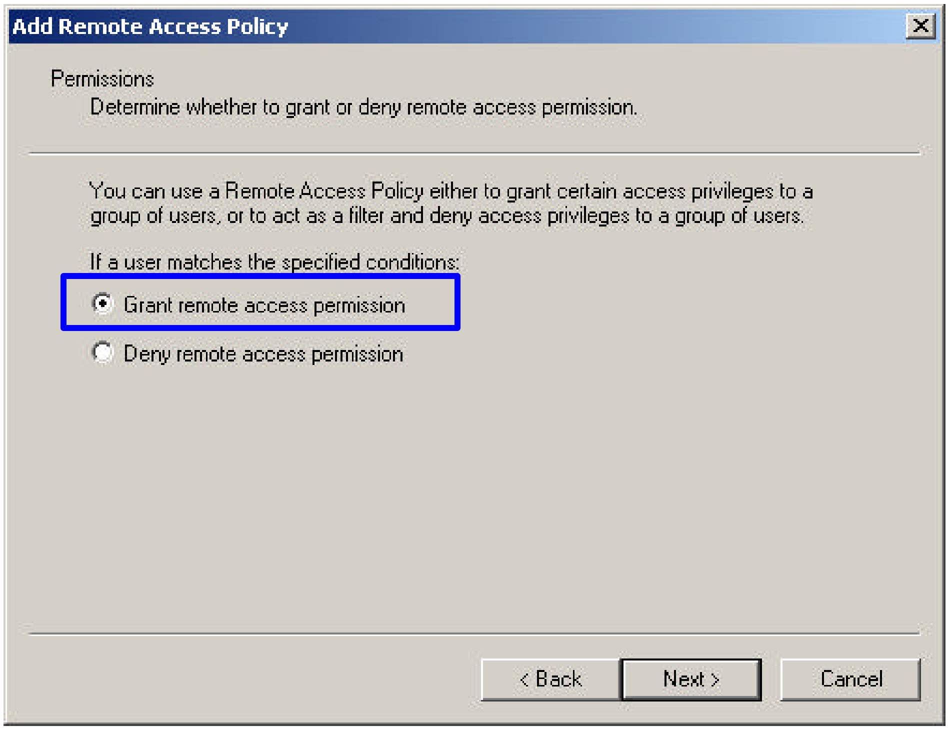


● Permitted

○ Denied

Sunday through Saturday from 12 AM to 12 AM

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



Permissions

Determine whether to grant or deny remote access permission.

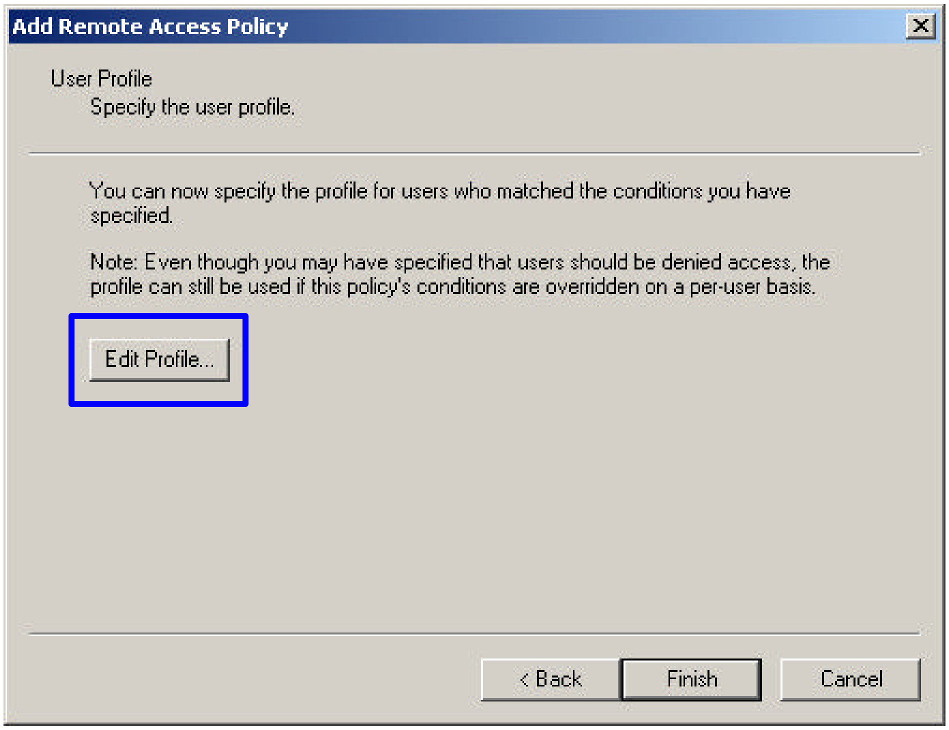
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.

If a user matches the specified conditions:

● Grant remote access permission

○ Deny remote access permission

33. Click "Edit Profile" to open up



Add Remote Access Policy

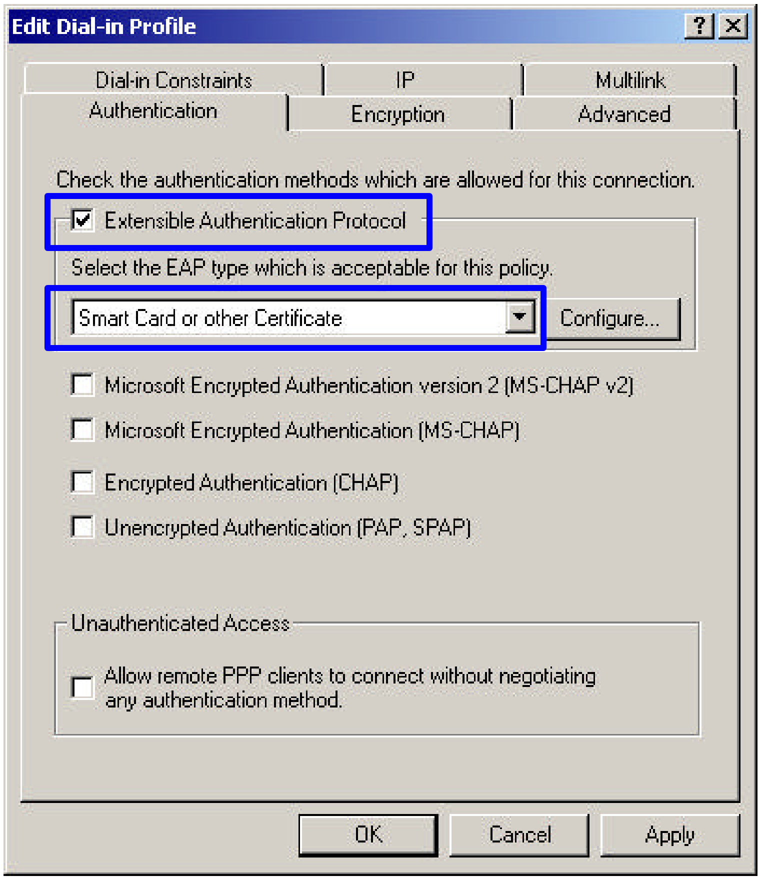
User Profile
Specify the user profile.

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

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

For TLS Authentication Setup (Steps 34 ~ 38)

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



Edit Dial-in Profile

Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

Smart Card or other Certificate

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

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

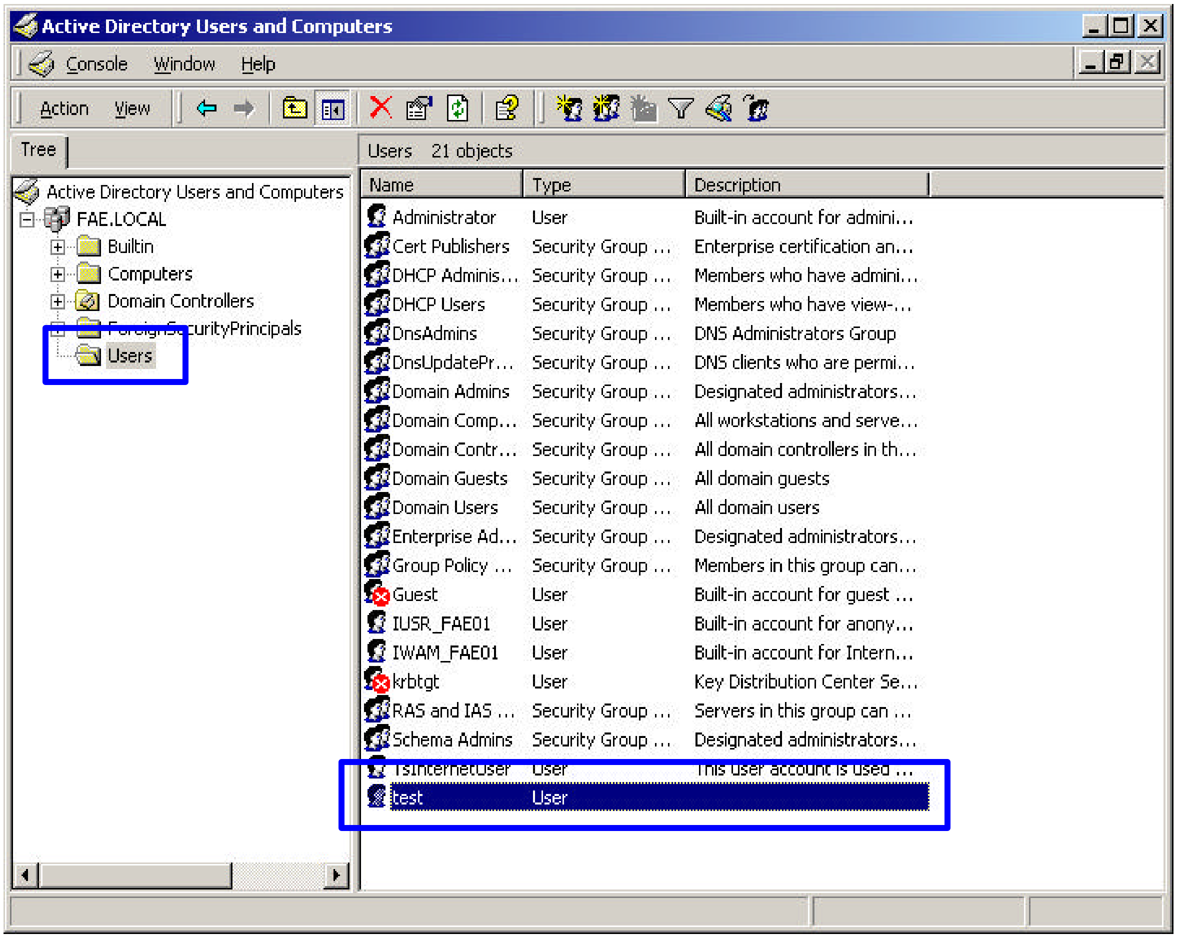
□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

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

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

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

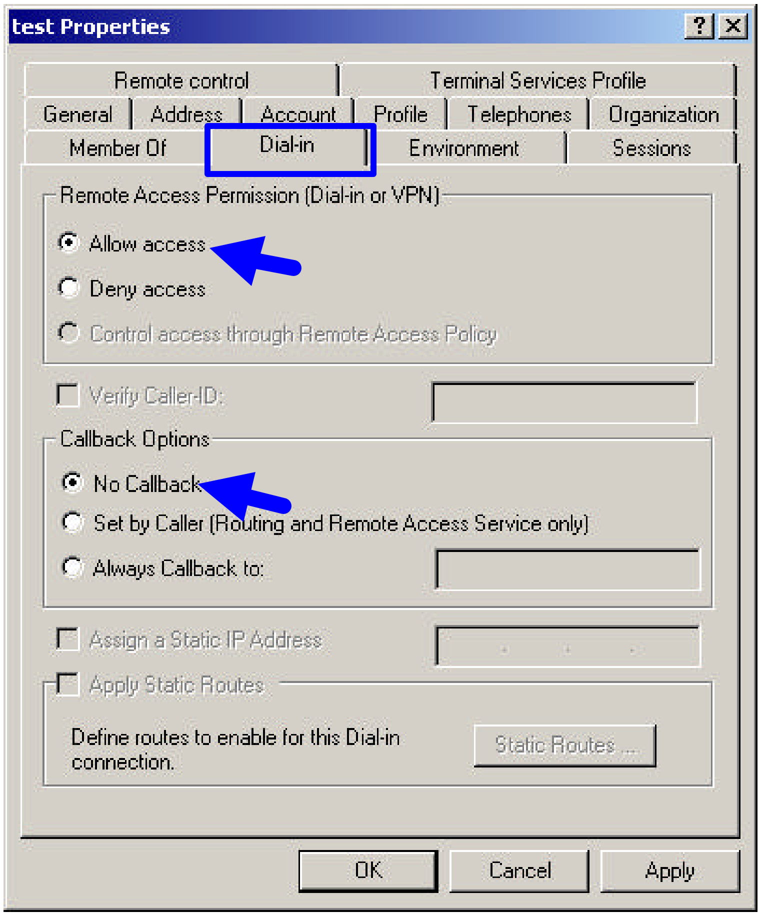

Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Active Directory Users and Computers
FAE.LOCAL
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

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.



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:

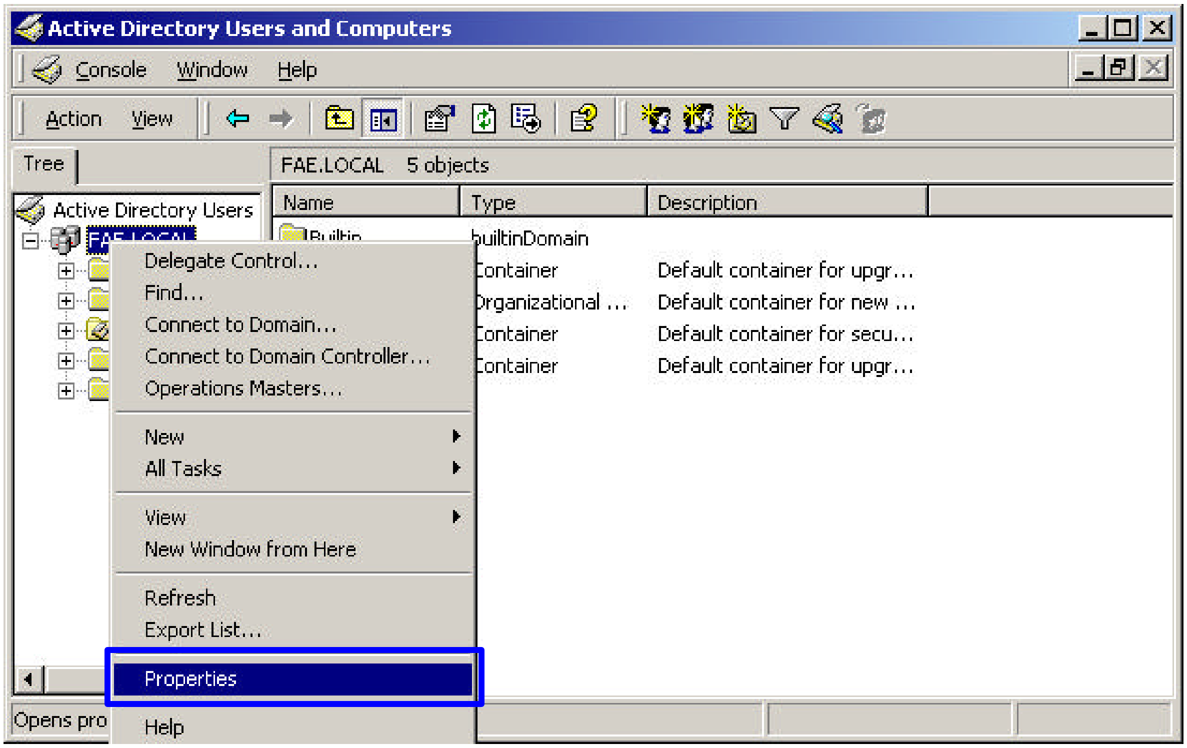
□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

For MD5 Authentication (Steps 39 ~ 54)

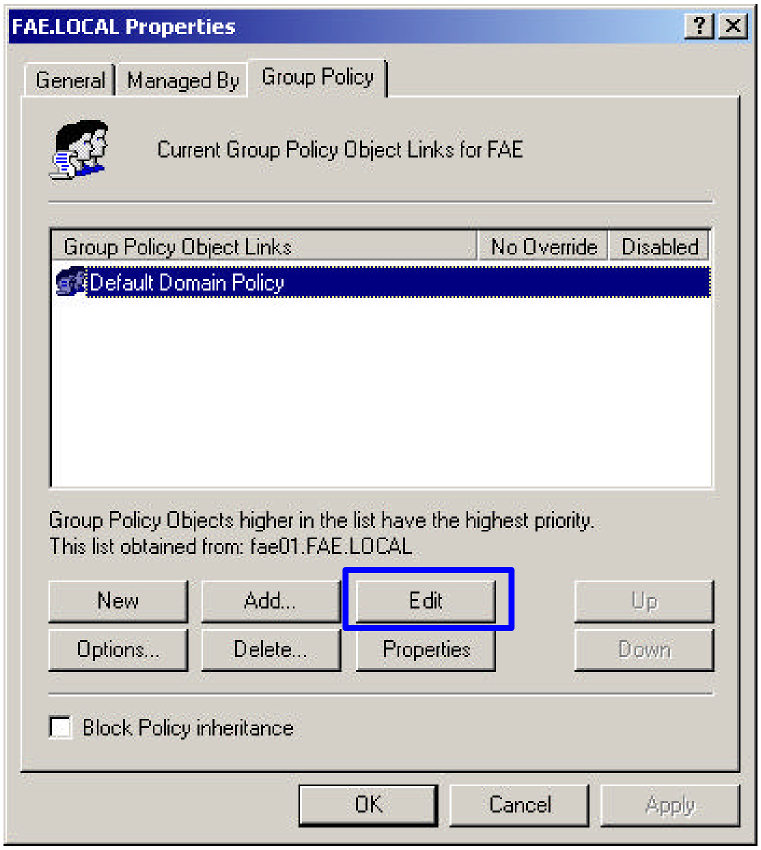
39. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers.**
40. Right click on the domain, and select "**Properties**"



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.



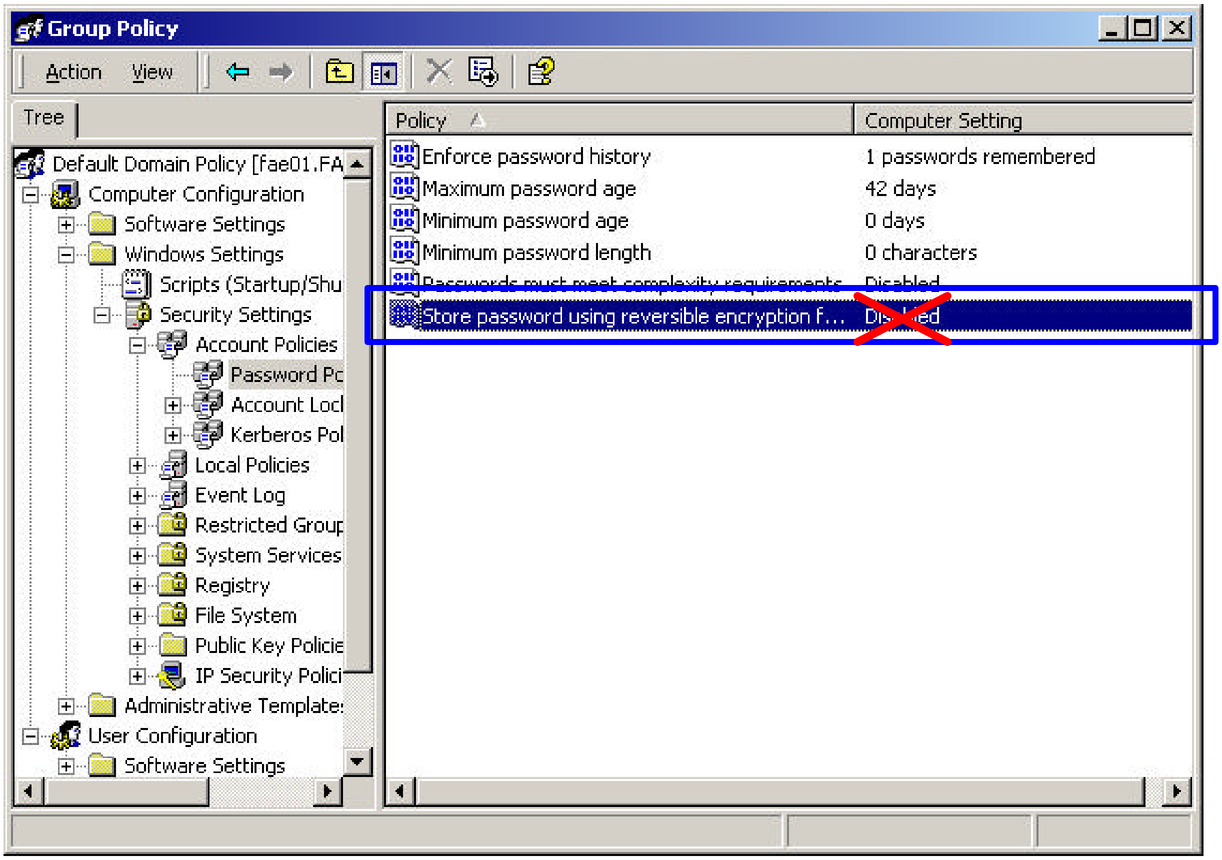
Current Group Policy Object Links for FAE

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

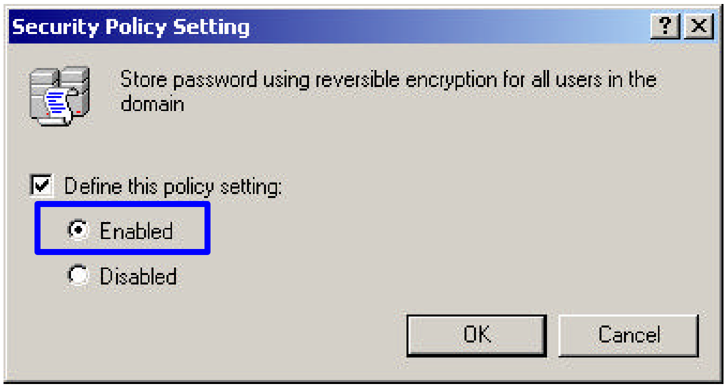
□ Block Policy inheritance

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.



Store password using reversible encryption for all users in the domain

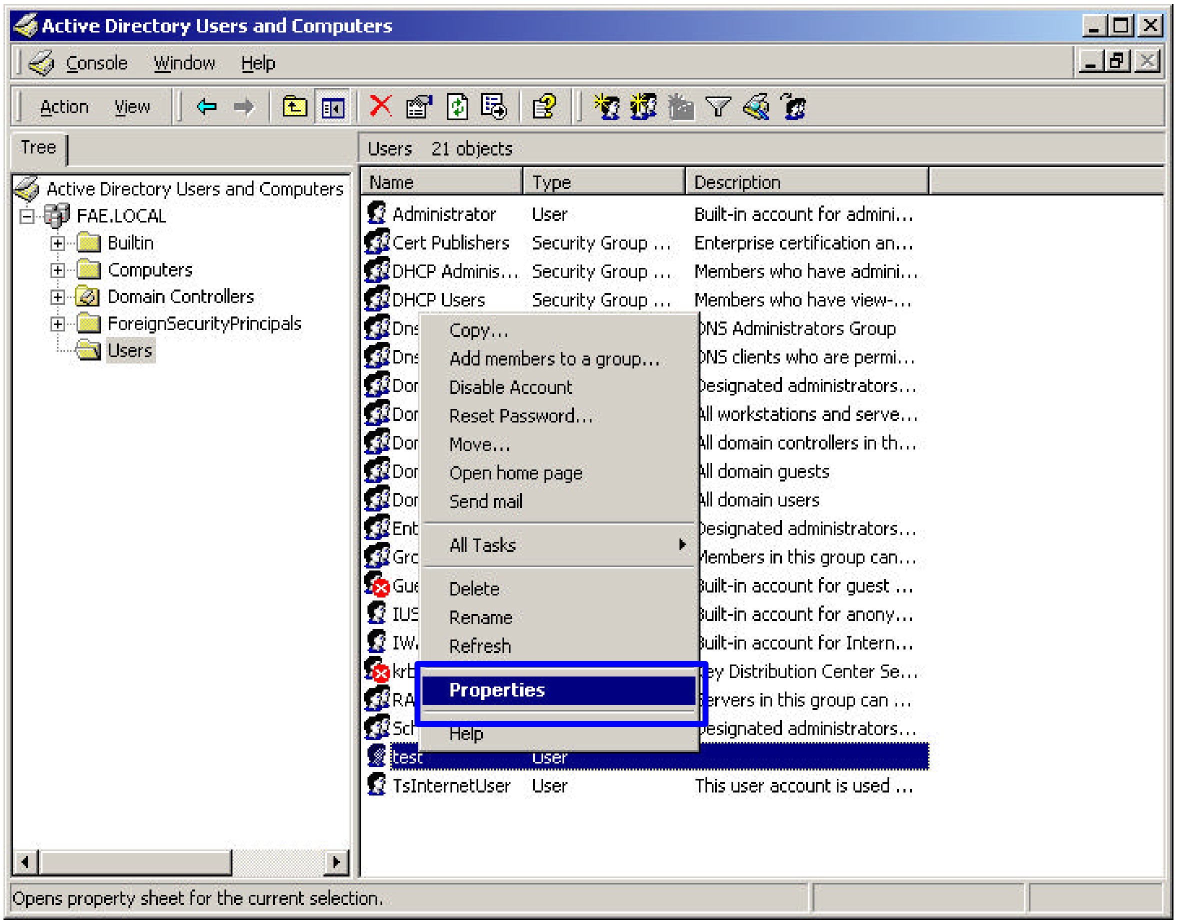
☑ Define this policy setting:

● 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**"

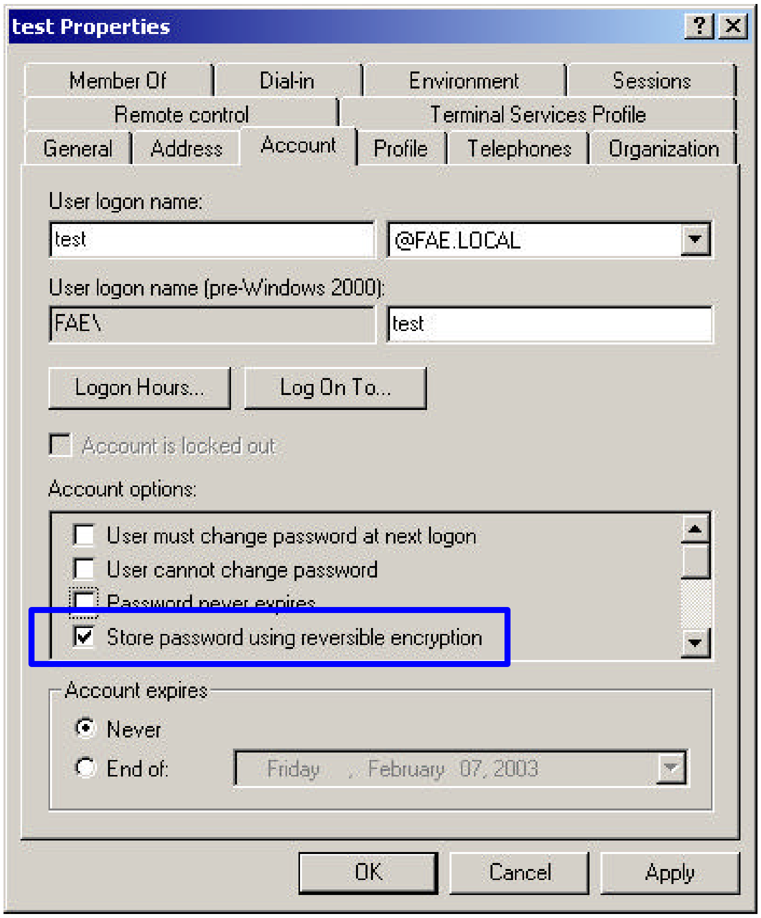


Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Enterprise certification an...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
Dns		NS Administrators Group
Dns		NS clients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

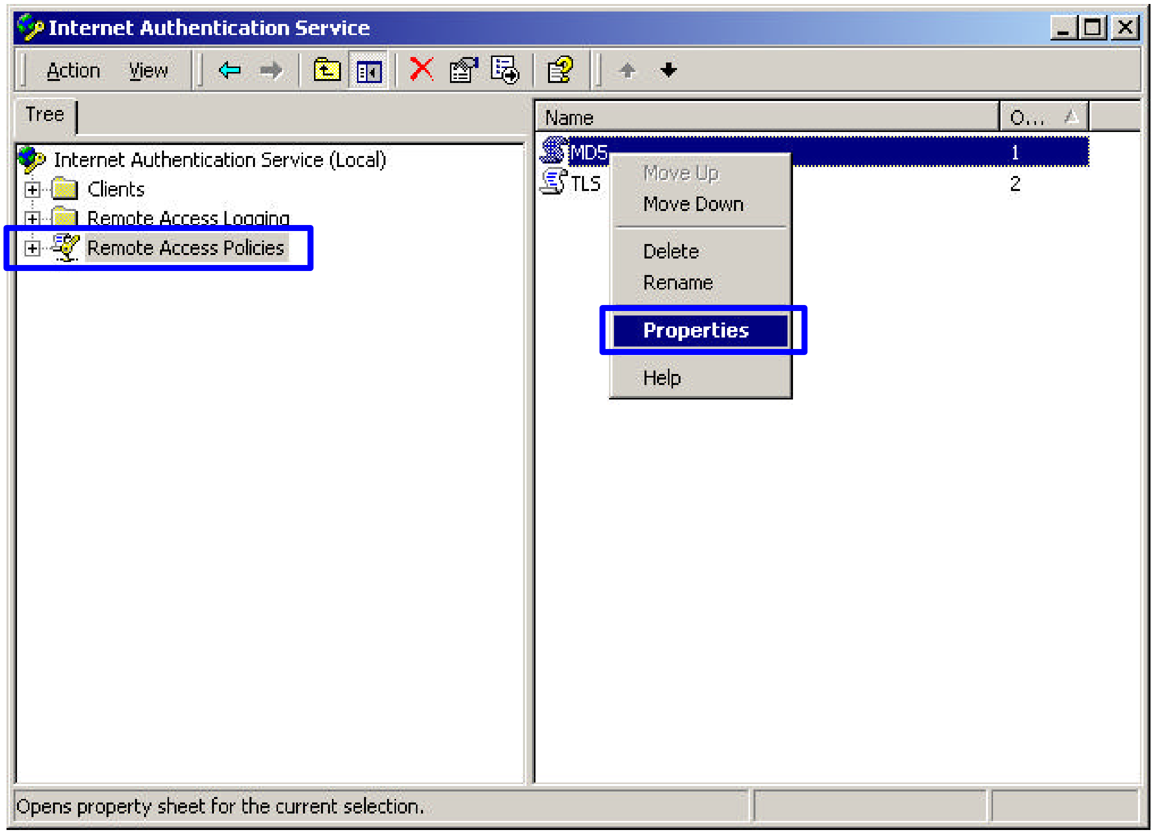
○ End of: Friday , February 07, 2003

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**”

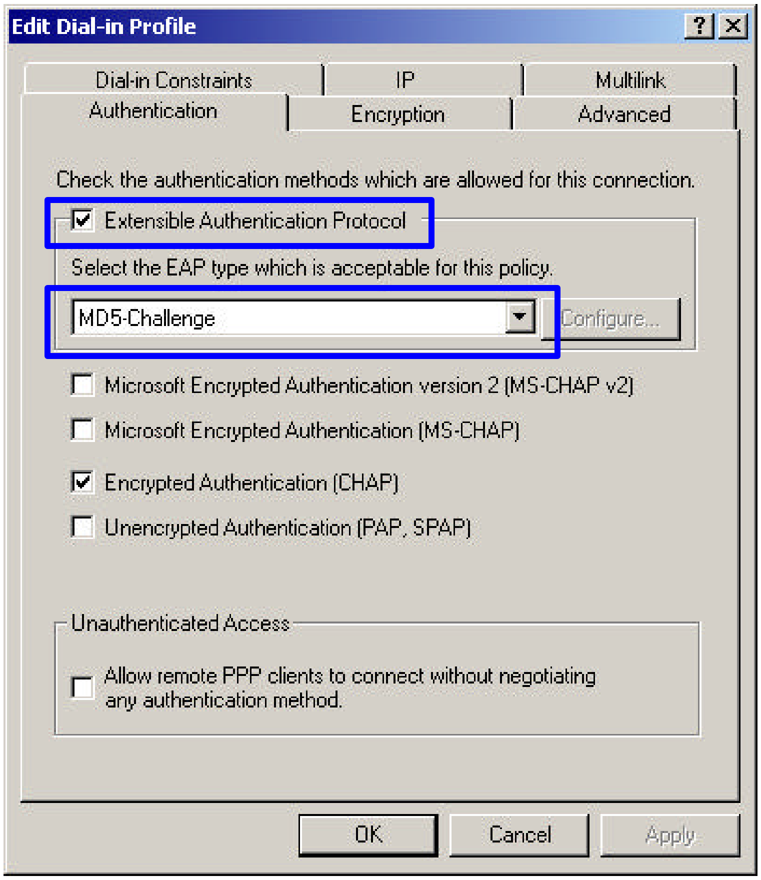


Opens property sheet for the current selection.

52. Go to “**Authentication**” tab

53. Enable “**Extensible Authentication Protocol**”

54. Select “**MD5-Challenge**” for EAP type.



Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

MD5-Challenge

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

□ Microsoft Encrypted Authentication (MS-CHAP)

☑ Encrypted Authentication (CHAP)

□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

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

APPENDIX D: GLOSSARY

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

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

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

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

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

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

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

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

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

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

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

Browser ? An application program that enables one to read the content and interact in the World

Wide Web or Intranet.

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

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

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

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

DHCP ? Dynamic Host Configuration Protocol, which is a protocol that lets network 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.

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

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

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

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

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

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

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

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

PLCP ? Physical layer convergence protocol

PPDU ? PLCP protocol data unit

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

PSDU ? PLCP service data unit

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

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

RTS Threshold ? Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this "Hidden Node Problem". If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

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

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

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

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

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

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

APPENDIX E: TECHNICAL SPECIFICATION

Standard	802.11b compliant (wireless)
	802.3, 802.3u for LAN
Data Rate	1 / 2 / 5.5 / 11 / 22 mbps
Interface	4 x 100BaseTX with Automatic MDI/MDIX feature
	Power Jack: 2.5 mm (inner dimension)
	Default Reset button
Emission Type	Direct Sequence Spread Spectrum (DSSS)
Data Modulation	1 Mbps – BPSK
	2 Mbps – QPSK
	5.5 / 11 Mbps – CCK
	5.5 / 11 / 22 Mbps - PBCC
RF Frequency	2412 MHz – 2462 MHz (North America)
	2412 MHz – 2472 MHz (General Europe)
	2412 MHz – 2484 MHz (Japan)
Operating Channel	11 Channels (North America)
	13 Channels (Europe)
	14 Channels (Japan)
RF Output Power	16 ~ 18 dBm (typical)
Sensitivity	22MHz PBCC -80 dBm (Typically @25? ±5?)
	11MHz PBCC - 85 dBm (Typically @25? ±5?)
	11MHz CCK - 82 dBm (Typically @25? ±5?)
Security	Wired Equivalent Privacy (WEP) 64 / 128 / 256 bit
Antenna Type	Dipole Antenna with Diversity, 2dBi Antenna Gain
Memory	SDRAM 4 Mbyte
	FLASH 1 Mbyte
Power Consumption	Operation max. 1.2 A
	600mA ± 50mA
Power Supply	DC 5 Volt ± 5% / 2.4A, AC Adapter AC 100V-240V