



LevelOne

WAP-0003

54Mbps Wireless Access Point

User's Manual

V. 1.0

Manufacturer's Disclaimer Statement

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

FCC STATEMENT

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

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

FCC Radiation Exposure Statement

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

Table of Contents

INTRODUCTION.....	4
Product Features	4
System Requirements.....	4
GETTING STARTED	5
Getting To Know The Wireless Network Access Point.....	5
WIRELESS NETWORK ACCESS POINT'S PORTS	5
WIRELESS NETWORK ACCESS POINT'S LEDS.....	5
Connecting The Wireless Network Access Point	5
Setting Up The Wireless Network Access Point	6
CONFIGURING YOUR WIRELESS ACCESS POINT	7
Configuration Menu	8
<i>Getting Started With Setup Wizard</i>	10
<i>Status Page</i>	12
<i>Basic Setting</i>	14
<i>IP Setting</i>	16
<i>Advanced Setting</i>	18
<i>Security</i>	20
802.1x.....	23
Tools	25
Using AP 54M U tility for Management.....	27
Installing AP 54M Utility	27
Manage and Configure Access Point with 54M AP Utility	31
<i>Link Information</i>	32
<i>AP Settings</i>	33
<i>IP Settings</i>	35
<i>WEP Settings</i>	36
802.1x Settings	37
APPENDIX A: TROUBLESHOOTING.....	38
APPENDIX B: NETWORKING BASIS	43
APPENDIX C: 802.1x Authentication Setup.....	57
802.1x Authentication Infrastructure	57
Supplicant: Wireless Network PC Card	58
Authenticator: Wireless Network Access Point	76
Radius Server: Window2000 Server.....	77
APPENDIX D: GLOSSARY	99
APPENDIX E: TECHNICAL SPECIFICATION	104

INTRODUCTION

LevelOne WAP-0003 54Mbps Wireless Access Point is designed to meet the needs of wireless clients who use 2.4GHz 802.11b/g(draft) compliant wireless networking devices such as PC Card. With the Dual-Standard capability, not only seamless but also simultaneous wireless data transmission between AP and all wireless clients using both 802.11b and g (draft) can be sustained. Device network setup can be installed by the simple setup wizard that is provided as part of the web management utility or by manually configured for the advanced settings. SNMP management is also supported to make central network management an easy task for corporation IT personnel. Wireless network protection can be ensured by WEP encryption, Wi-Fi Protected Access (WPA) and 802.1x authentication to achieve maximum level of security. LevelOne WAP-0003, 2.4GHz 802.11g/b Wireless Access Point ,offers unbeatable performance for both data throughput and range coverage, which is an ideal device to be deployed not only in complex Enterprise corporation networking infrastructure and metropolitan area but also in simple SOHO and home environments.

Product Features

- ◆ Fully IEEE 802.11g (draft) and 802.11b standards compliant.
- ◆ High-speed data transfer of IEEE 802.11b/g(draft)
- ◆ Highly efficient design mechanism to provide unbeatable performance achieving data rate up to 54 Mbps for 802.11g(draft) and 11 Mbps for 802.11b with wide range coverage.
- ◆ Strong network security with 802.1x, Protected Access (WPA) and WEP encryption.
- ◆ Auto-select and use the least crowded channel by Dynamic Channel Selection Function.
- ◆ Quick and easy setup with Web-based management configuration utility.

System Requirements

- ◆ Windows 95, 98, 98SE, Millennium, 2000 and XP computers
- ◆ Internet Explorer 5.5 or higher
- ◆ One CD-ROM drive
- ◆ At least one 10/100Mbps Ethernet network adapter installed

GETTING STARTED

Getting To Know LevelOne 54Mbps Wireless Access Point

LevelOne WAP-0003 WIRELESS 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.

LevelOne WAP-0003 WIRELESS ACCESS POINT'S LEDS

- ◆ Power LED
 - ON when the unit is powered up
- ◆ WLAN LED
 - ON indicates WLAN is working; blink indicates wireless activity
- ◆ LAN LED
 - ON indicates LAN connection; blink indicates LAN activity

Connecting LevelOne WAP-0003 Wireless 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 LevelOne WAP-0003 Wireless Access Point

LevelOne 54mbps 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 LevelOne Access Point setup.

CONFIGURING LevelOne 54Mbps

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 versions.
2. The Ethernet network adapter must be working properly. Please refer to Troubleshooting section for details.
3. If you are connecting LevelOne 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 LevelOne 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 LevelOne 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 LevelOne Access Point is powered.

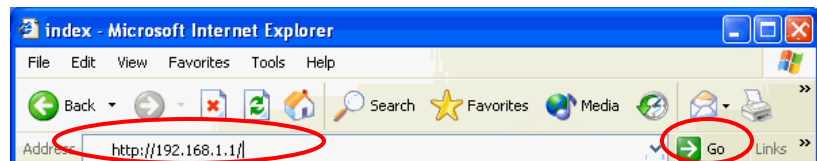
The Default Settings of LevelOne 54Mbps Wireless Access Point:

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 webbrowser window, and type in the IP address of LevelOne 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"

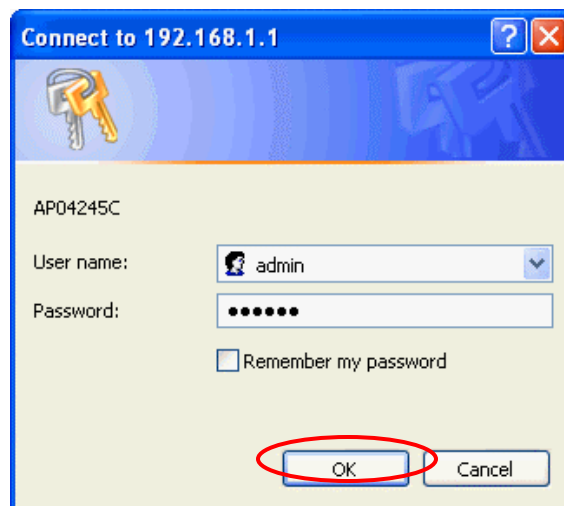


NOTE:

The IP address shown above is the default IP address for LevelOne 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"



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 LevelOne Access Point by going through each tab. Here **Status** page is displayed.



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 LevelOne Access Point configured and ready for running in 4 easy steps by clicking on the “**Wizard**” button on the function menu. The following screen will appear. Please click “**Next**” to continue.



Step 1: Set Password

LevelOne 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.



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.

The screenshot shows the 'Setup Wizard' window for a '54Mbps Access Point'. The title bar says '54Mbps Access Point Setup Wizard'. The main heading is 'Set Wireless LAN Connection'. Below this, a text box says: '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.' There are two input fields: 'SSID' with the text 'accounting' and 'Channel' with a dropdown menu showing '6'. At the bottom right, there are three buttons: 'back' (circular arrow), 'next' (green arrow), and 'exit' (exit icon).

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.

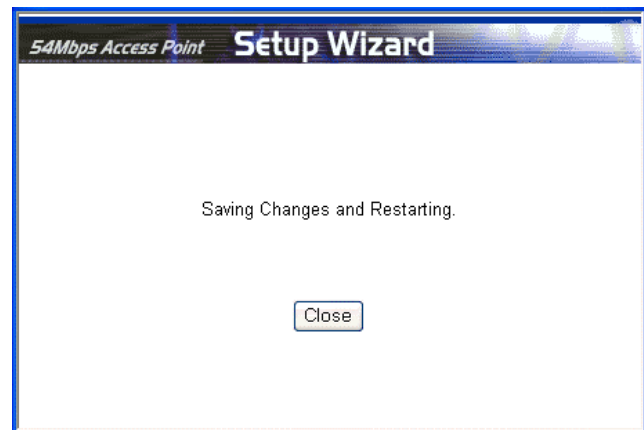
The screenshot shows the 'Setup Wizard' window for a '54Mbps Access Point'. The title bar says '54Mbps Access Point Setup Wizard'. The main heading is 'Set WEP Encryption'. Below this, a text box says: 'You may enable WEP security for data encryption by selecting Enabled. Select one of the WEP encryption 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.' There are three input fields: 'Wep' with radio buttons for 'Enabled' (selected) and 'Disabled'; 'Wep encryption' with a dropdown menu showing '64Bit'; and 'Key' with a text box containing '0000000000'. Below the key text box, it says 'Input 10 HEX characters(HEX is 0~9, A~F or a~f)'. At the bottom right, there are three buttons: 'back' (circular arrow), 'next' (green arrow), and 'exit' (exit icon).

Step 4: Restart

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

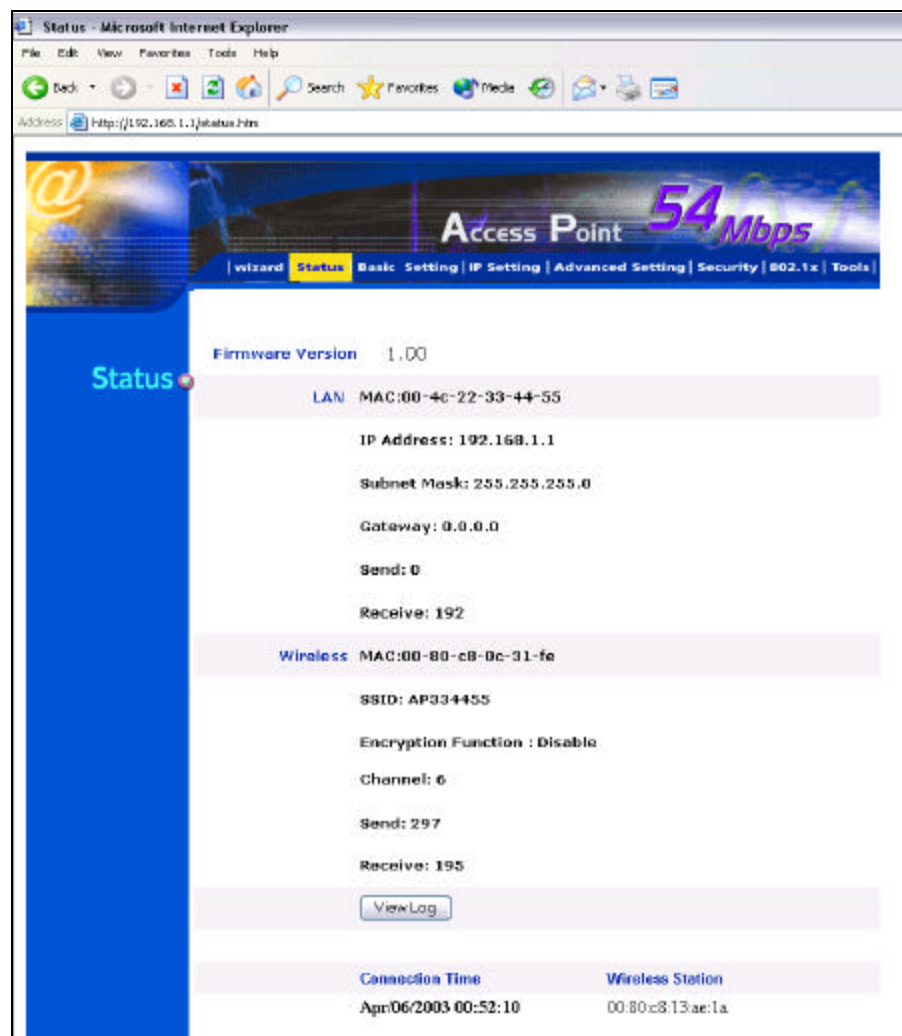
The screenshot shows the 'Setup Wizard' window for a '54Mbps Access Point'. The title bar says '54Mbps Access Point Setup Wizard'. The main heading is 'Setup Completed'. Below this, a text box says: 'The Access Point setup is now completed. If you want to change any setup settings, click Back to go back to the previous pages. Click Restart to reboot the Access Point for the new settings to take effect.' At the bottom right, there are three buttons: 'back' (circular arrow), 'restart' (circular arrow with a refresh symbol), and 'exit' (exit icon).

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



Status Page

This page displays the following information.

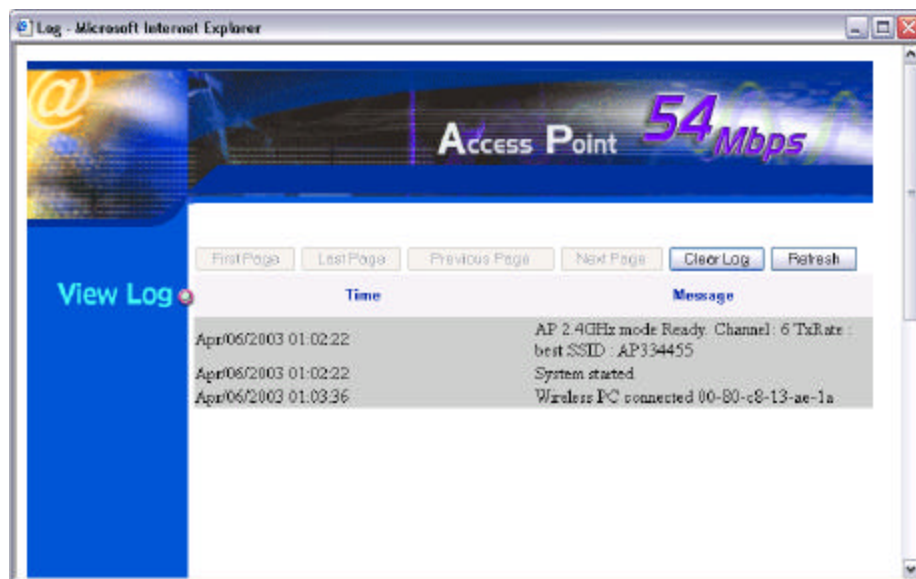


Firmware Version: Shows the current firmware version

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.



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 LevelOne 54Mbps Wireless Access Point with the minimum amount of effort to adjust a secure wireless network.

The screenshot shows the 'Basic Setting' page of a LevelOne 54Mbps Wireless Access Point configuration interface. The browser window is titled 'Basic Setting - Microsoft Internet Explorer' and the address bar shows 'http://192.168.1.1/basic.html'. The page has a blue sidebar with 'Basic Setting' and a main content area with a banner that says 'Access Point 54Mbps'. The main content area contains the following settings:

- AP Name:** Text box containing 'AP334455'.
- SSID:** Text box containing 'AP334455'.
- Channel:** Dropdown menu showing '6' and '(Domain: USA)'.
- WEP Key:** Radio buttons for 'Disable' (selected), '64bits', and '128bits'.
- Mode:** Dropdown menu showing 'HEX'.
- WEP Keys:** Four numbered text boxes (1, 2, 3, 4) for entering WEP keys.
- Buttons:** 'Apply', 'Cancel', and 'Help' buttons at the bottom.

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.

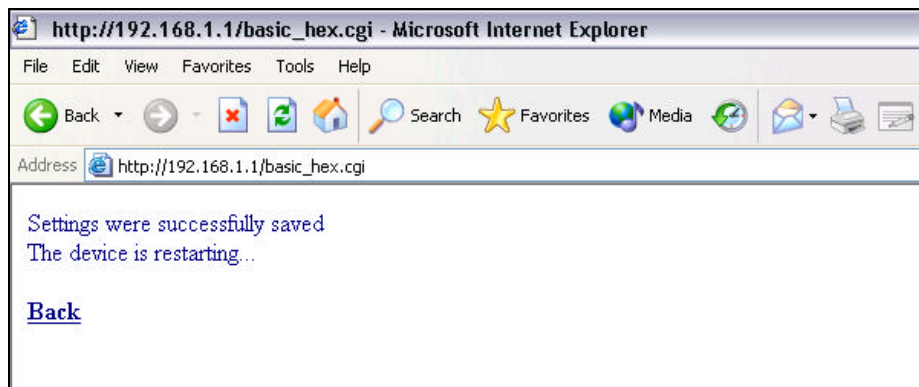
SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

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 2 type of WEP keys to choose from, 64bits and 128bits. When one of the 2 WEP key options is selected, you must enter the value 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".



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 LevelOne Access Point.

IP Setting - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://192.168.1.1/tp.html

Access Point 54Mbps

wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools

IP Setting

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

Apply Cancel Help

The default IP address of LevelOne 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.

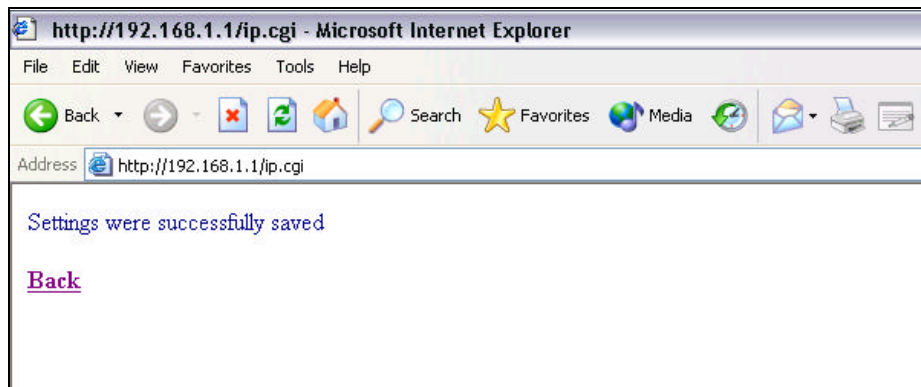
You can also set the Access Point to obtain the IP from a DHCP server, but it is not recommended. Once set, it will be difficult to determine the dynamic IP assigned to the Access Point. Select the option "Obtain IP Automatically" and click "**Apply**" button for the changes to be effective.

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.



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 Forward Stop Reload Search Favorites Media

Address: http://192.168.1.1/advanced.html

Access Point 54Mbps

Wizard Status Basic Setting IP Setting **Advanced Setting** Security 802.1x Tools

AP Mode ☒ AP

☐ AP Client Remote AP BSS ID: 000000000000

☐ Wireless Bridge Remote Bridge MAC:

☐ Multiple Bridge

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

RTS Threshold: 2432 (range: 256~2432, default: 2432)

Fragmentation Threshold: 2346 (range: 256~2346, default: 2346, even number only)

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

Authentication Type ☐ Open System ☐ Shared Key ☒ Both

SSID broadcast ☒ Enable ☐ Disable

TX Rates: Auto (Mbps)

11g Only Mode ☐ Enabled ☒ Disabled

Apply Cancel Help

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 field: 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.

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.

TX Rate: Select the data rate for data transmission.

11g Only Mode: Select **Enable** or **Disable** IEEE 802.11g (drag) only mode.

Security

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

The screenshot shows a web browser window titled "Security - Microsoft Internet Explorer". The address bar displays "http://192.168.1.1/security.html". The page features a navigation bar with links: "wizard", "Status", "Basic Setting", "IP Setting", "Advanced Setting", "Security" (highlighted), "802.1x", and "Tools". The main content area is titled "Security" and includes the following fields and options:

- Password** section:
 - Administrator Id:
 - AP Password New:
 - Confirm:
 - Buttons: , ,
- MAC Filter** section:
 - Radio buttons: ☐ Enabled, ☒ Disabled
 - Options:
 - ☐ Only **deny** PCs with MAC listed below to access device
 - ☒ Only **allow** PCs with MAC listed below to access device
 - MAC list header: 10
 - MAC 1: - - - - -
 - MAC 2: - - - - -

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 SiteSurvey utilities, such as zero configuration utility provided in Windows XP.

MAC Filter

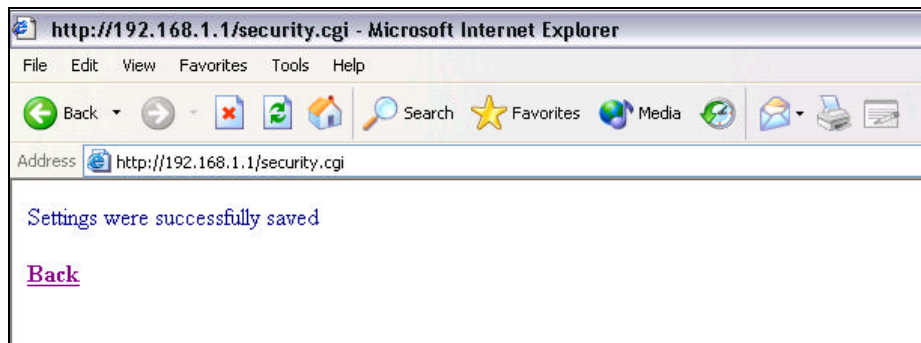
MAC Filter function controls the MAC of the network devices that are listed in this table for access authorization or denial. When MAC Filter is enabled, by selecting the “**Enabled**” radio box, select one of two choices:

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

The screenshot shows the MAC Filter configuration window. The 'MAC Filter' label is circled in red. Below it, the 'Enabled' radio button is selected. The window contains a table with 10 rows for MAC addresses (MAC1 to MAC10), each with six input fields. At the bottom are 'Apply', 'Cancel', and 'Help' buttons.

The screenshot shows the MAC Filter configuration window with the 'Only allow PCs with MAC listed below to access device' radio button selected. The dropdown menu for the first MAC address (MAC1) is open, showing a list of MAC address ranges: 1~10, 1~10, 11~20, 21~30, 31~40, and 41~50. The dropdown menu is circled in red.

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.



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. LevelOne 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.

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

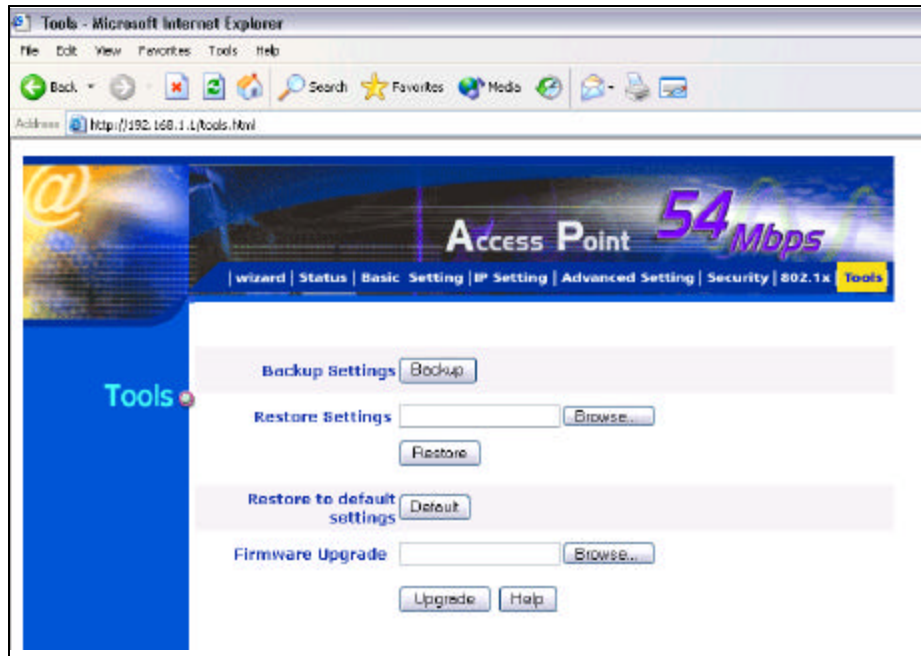
6. Click "**Apply**" button for the 802.1x settings to take effect after Access Point reboots itself.

NOTE:

As soon as 802.1x security is enabled, all the wireless client stations that are connected to LevelOne 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.



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 LevelOne Access Point re-operates after it restarts.

Restore to default settings:

Click on “**Default**” button to restore LevelOne 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 LevelOne Access Point re -operates after it restarts.

Using AP 54M Utility for Management

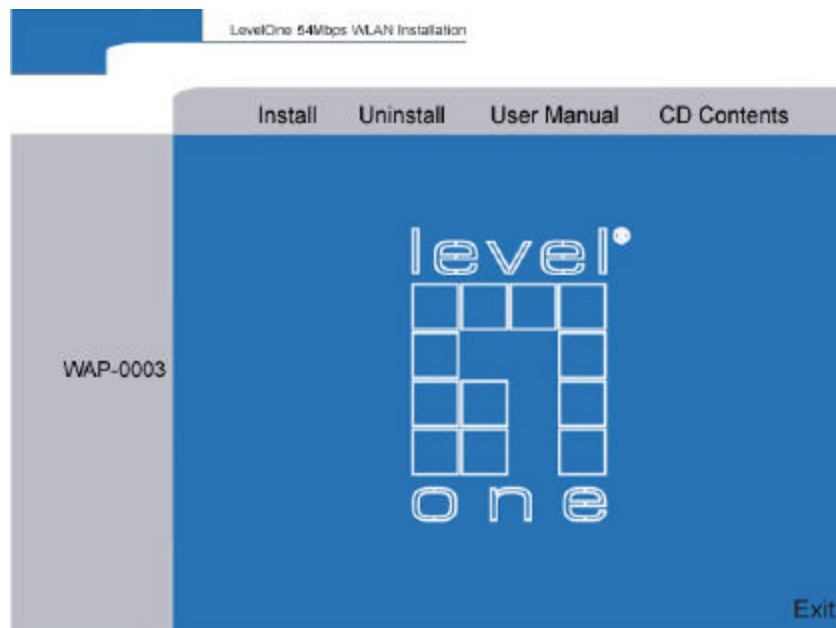
Installing AP 54M Utility

The AP 54M Utility is a program that runs on your PC, which offers easy management for all existing 54Mbps Access Points in the same network domain. Please follow the steps below for installation and refer to “Manage and Configure AP with AP 54M Utility” session Access point configuration.

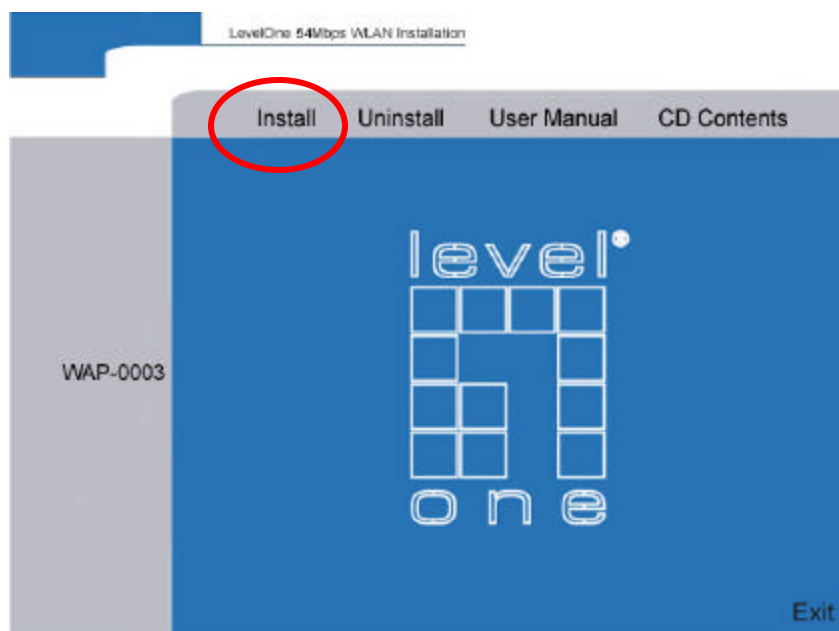
NOTE:

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

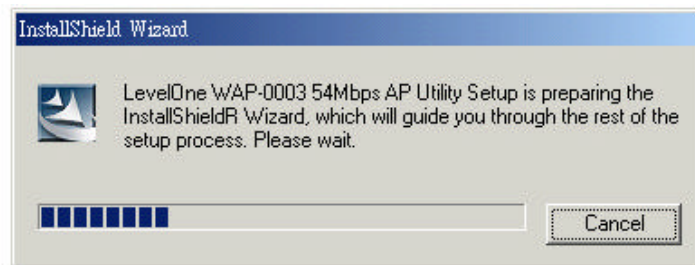
1. Turn on your PC
2. After Windows starts up, insert the 54Mbps Access Point Product CD into the CD tray of the CD-ROM
3. The following screen would appear.



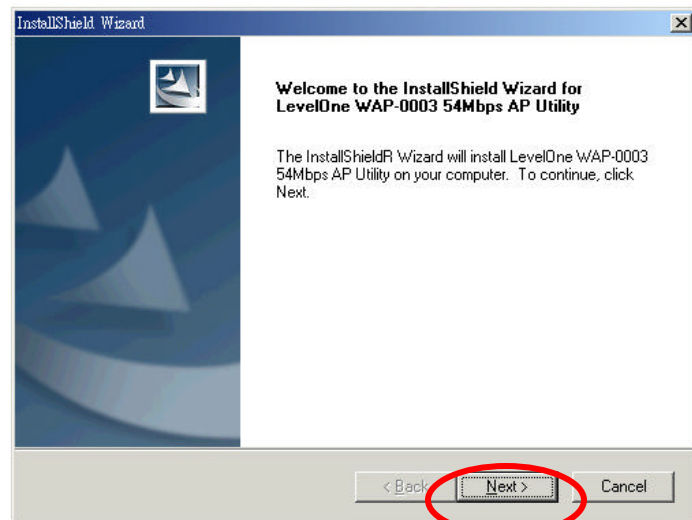
4. Click "**Install**" on the menu bar to proceed with 54M AP installation.



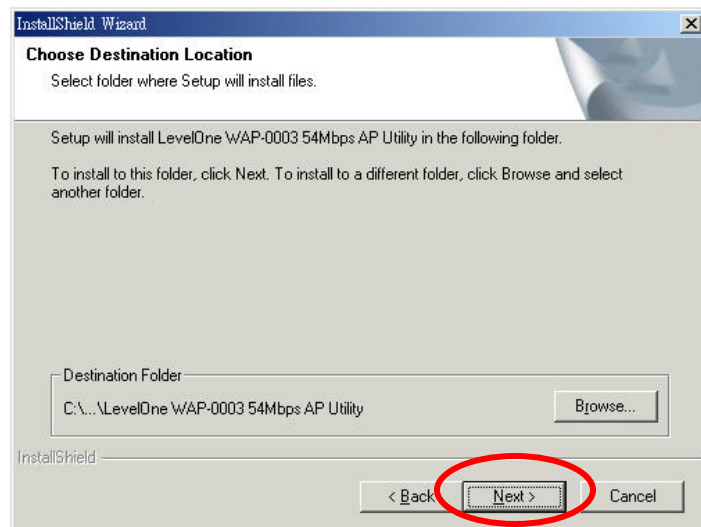
The 54M AP Utility loads the Install wizard for installation.



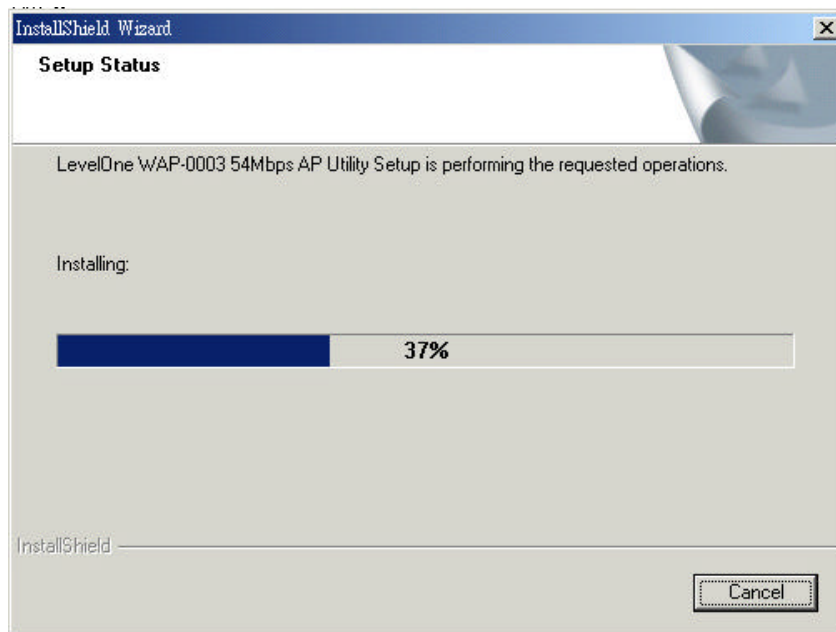
Click **"Next"** to start installation.



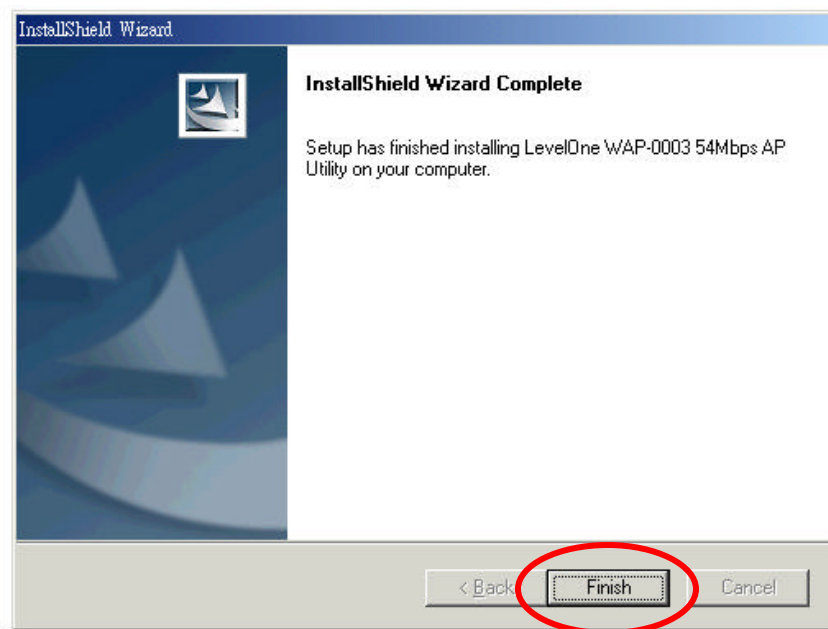
Click **"Next"** to install in default folder or Click **"Browse"** to install in a different folder.



Installation wizard copies the utility program files in your PC.



5. Click "**Finish**" to complete the installation.



6. The 54M AP Utility icon would then appear on your desktop for easy access.



Manage and Configure Access Point with 54M AP Utility

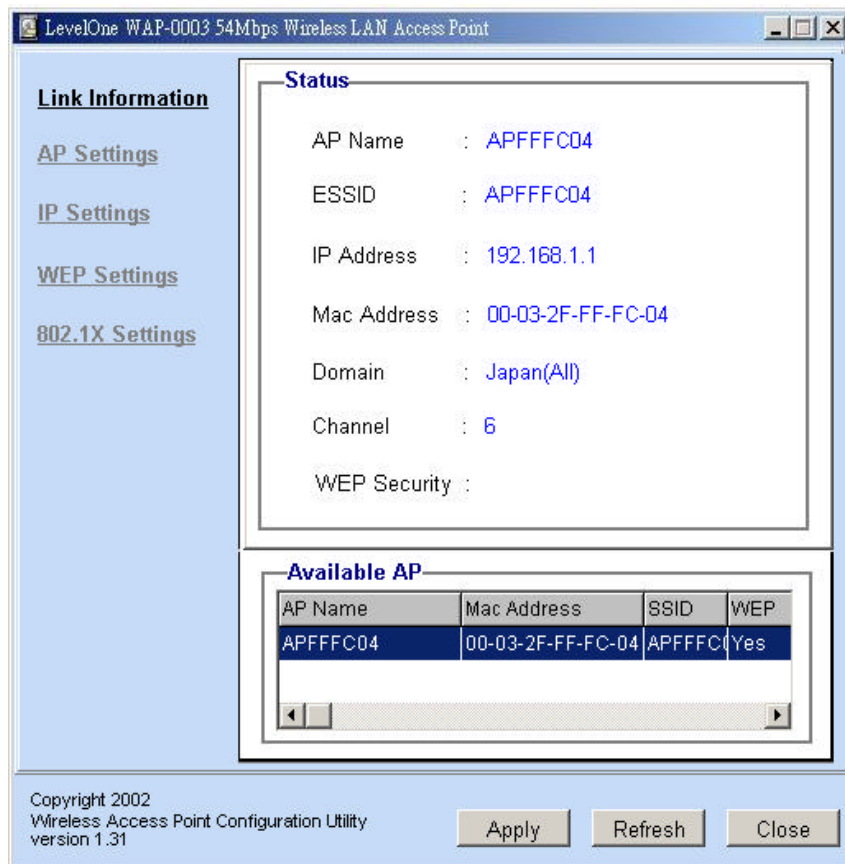
LevelOne AP 54M Utility can be useful in away that allows you to configure one AP to another to save the trouble of logging into the web configuration utility of each AP. However, all the Access Points that you wish to configure using 54MAP Utility must be in the same network domain as your PC's.

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.

```
C:\WINNT\System32\command.com
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 54M AP Utility starts up.



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

Available AP – lists all the 54Mbps 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.

LevelOne WAP-0003 54Mbps Wireless LAN Access Point

Link Information

AP Settings

IP Settings

WEP Settings

802.1X Settings

1 Basic Setting

ESSID: APFFFC04

Channel: 6

AP Name: APFFFC04

2 Mode Setting

☒ Access Point Remote MAC Address

☐ Access Point Client

☐ Wireless Bridge

☐ Multiple Bridge

3 Advanced Setting

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

Apply Refresh Close

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. Please refer to Appendix C, Glossary for the definitions of these 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.

The 'Login Management' dialog box has a title bar with standard window controls. Inside, there's a 'Login' section with two text input fields: 'UserName' and 'Password'. Both fields are currently empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

Enter "UserName" and "Password" for the Access Point

Click "OK" button

The 'Login Management' dialog box is shown again, but now the 'UserName' field contains the text 'admin'. The 'Password' field contains a series of asterisks (*****). The 'OK' and 'Cancel' buttons remain at the bottom right.

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

The 'LevelOne WAP-0003 54Mbps Wireless LAN Access Point' configuration utility window is displayed. It has a sidebar on the left with links: 'Link Information' (selected), 'AP Settings', 'IP Settings', 'WEP Settings', and '802.1X Settings'. The main area is divided into two sections: 'Status' and 'Available AP'.

Status Section:

- 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 Section:

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

At the bottom of the window, there is a footer with copyright information: 'Copyright 2002 Wireless Access Point Configuration Utility version 1.31'. To the right of the footer are 'Apply', 'Refresh', and 'Close' buttons.

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.

Copyright 2002
Wireless Access Point Configuration Utility
version 1.31

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

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"

LevelOne WAP-0003 54Mbps Wireless LAN Access Point

Link Information

AP Settings

IP Settings

WEP Settings

802.1X Settings

☒ 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

Apply Refresh Close

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

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

LevelOne WAP-0003 54Mbps Wireless LAN Access Point

Link Information

AP Settings

IP Settings

WEP Settings

802.1X Settings

☒ 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

Apply Refresh Close

802.1x Settings

The screenshot shows the 'LevelOne WAP-0003 54Mbps Wireless LAN Access Point' configuration window. On the left is a sidebar with links: 'Link Information', 'AP Settings', 'IP Settings', 'WEP Settings', and '802.1X Settings' (which is highlighted). The main area is titled '802.1X Setting'. It contains a checkbox for '802.1X Function' which is checked. Below it are 'Encryption Key Length' (set to '64 bits') and 'Lifetime' (set to '1 Day'). There are two sections for RADIUS servers. 'RADIUS Server 1' has fields for 'Port' (1812), 'IP Address' (0.0.0.0), and 'Shared Secret'. 'RADIUS Server 2(Optional)' has fields for 'Port' (0), 'IP Address' (0.0.0.0), and 'Shared Secret'. Below these is an 'Available AP' section with a table:

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

At the bottom of the window, there is a copyright notice: 'Copyright 2002 Wireless Access Point Configuration Utility version 1.31'. To the right of the notice are three buttons: 'Apply', 'Refresh', and 'Close'.

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 802.1 x 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 LevelOne 54Mbps Wireless Access Point. Please read through the following to solve your problems.

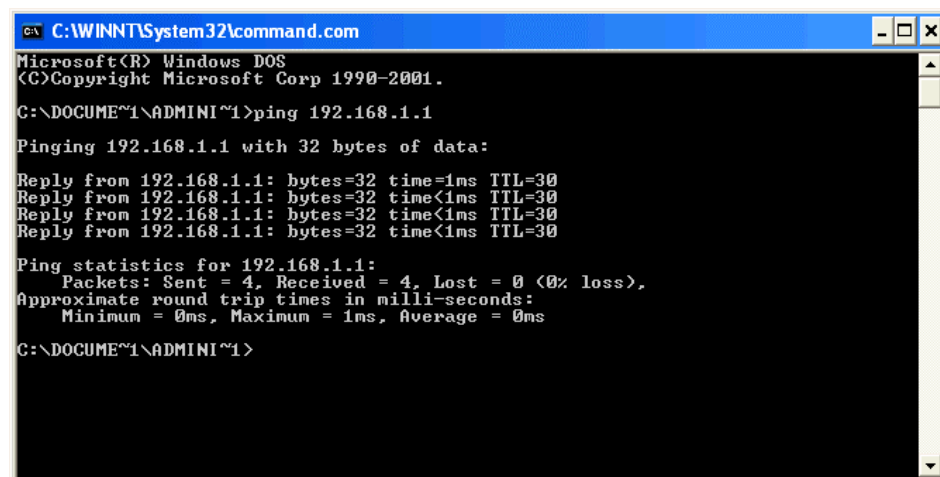
1. The computer connected to LevelOne Wireless Access Point through Ethernet network cannot access the configuration menu.

- ◆ 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 LevelOne 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.

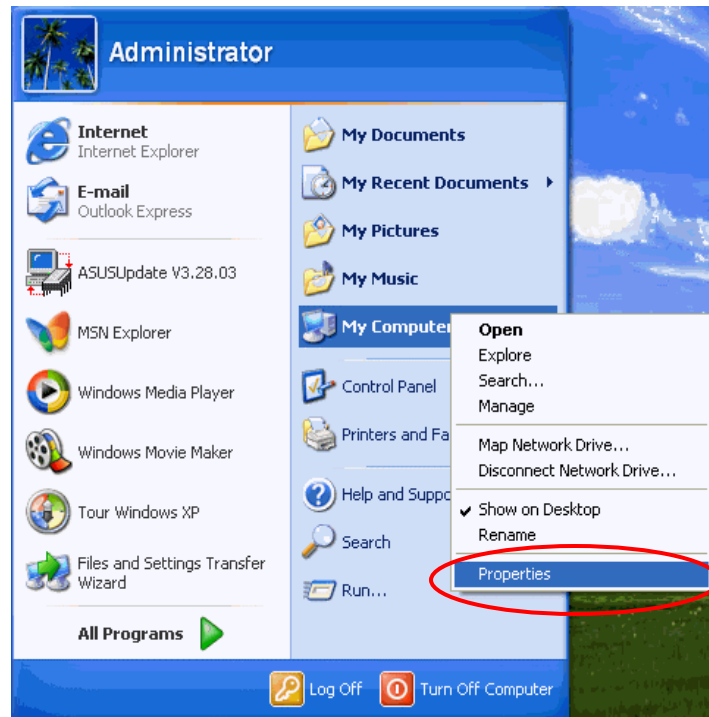


```
C:\WINNT\System32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\DOCUME~1\ADMINI~1>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=30
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30
Reply from 192.168.1.1: 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>
```

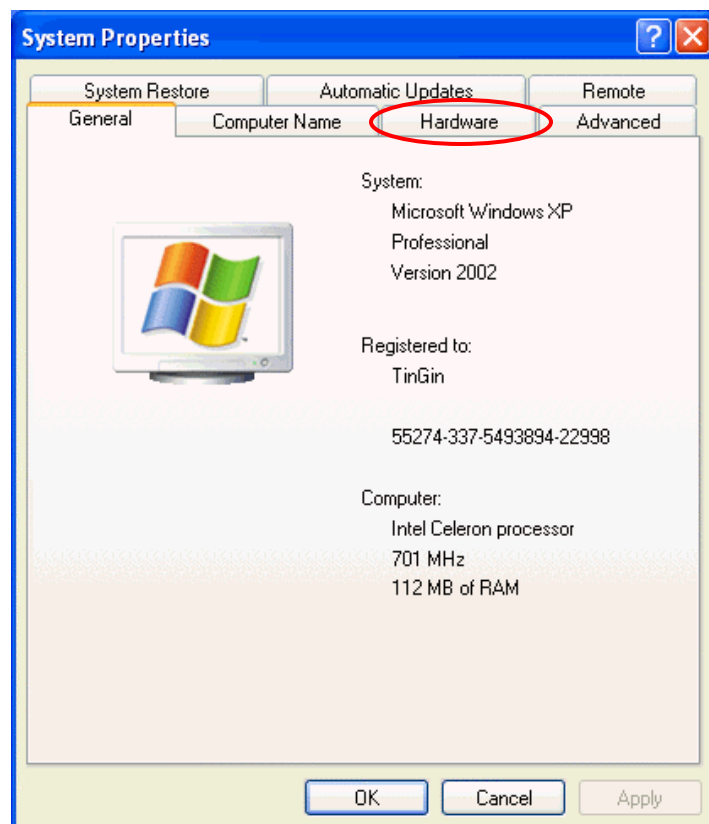
2. The wireless clients cannot access the network in the infrastructure mode.

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

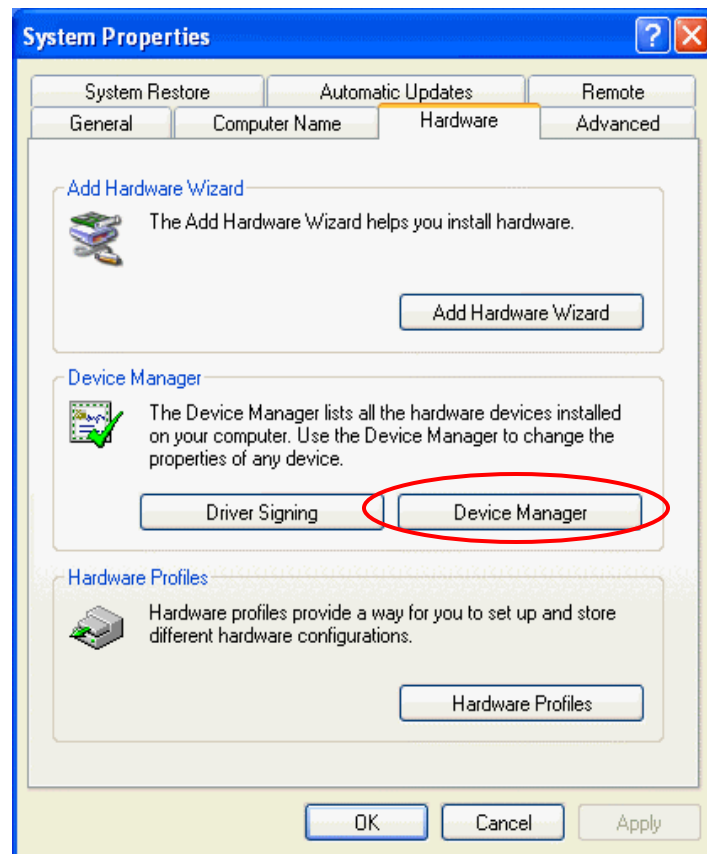
Go to "Start" >
Right mouse click
on "My Computer"
> "Properties"



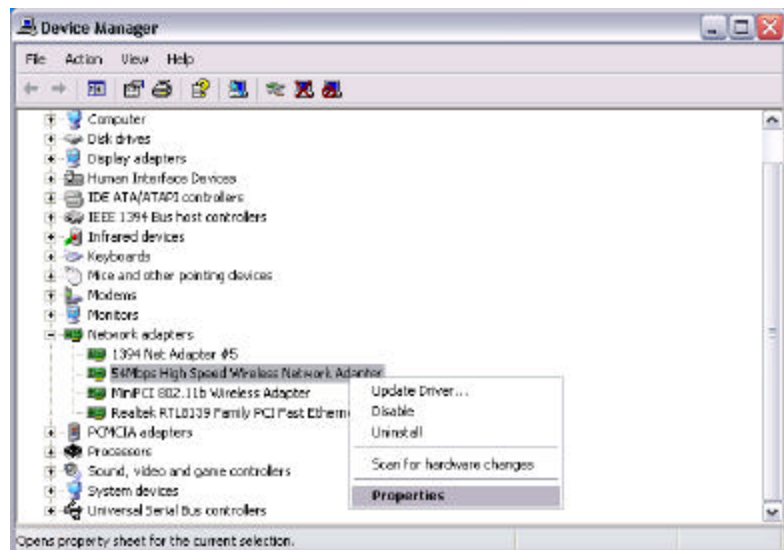
Go to "Hardware"



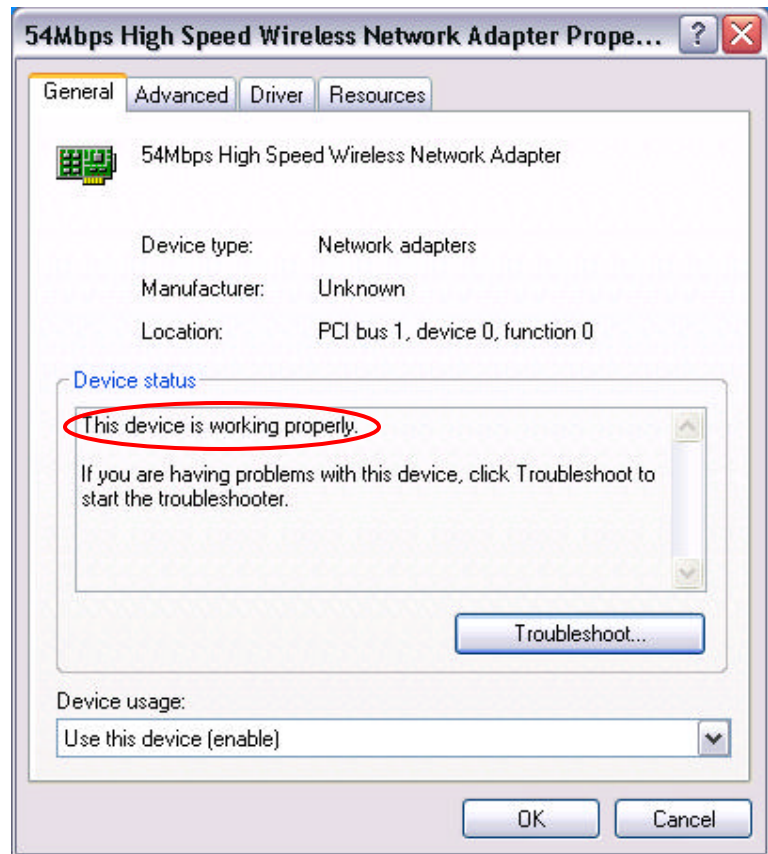
Go to "Device Manager"



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



Check and make sure that the network adapter is working properly



3. Resetting LevelOne 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 LevelOne 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 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.

6. 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.

7. What is WEP?

Wired Equivalent Privacy (WEP) is a type of data encryption mechanism described in the IEEE 802.11 standard. The 54Mbps Wireless Access Point supports 64/128 bit shared key for WEP.

8. 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.

9. 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.

APPENDIX B: NETWORKING BASIS

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

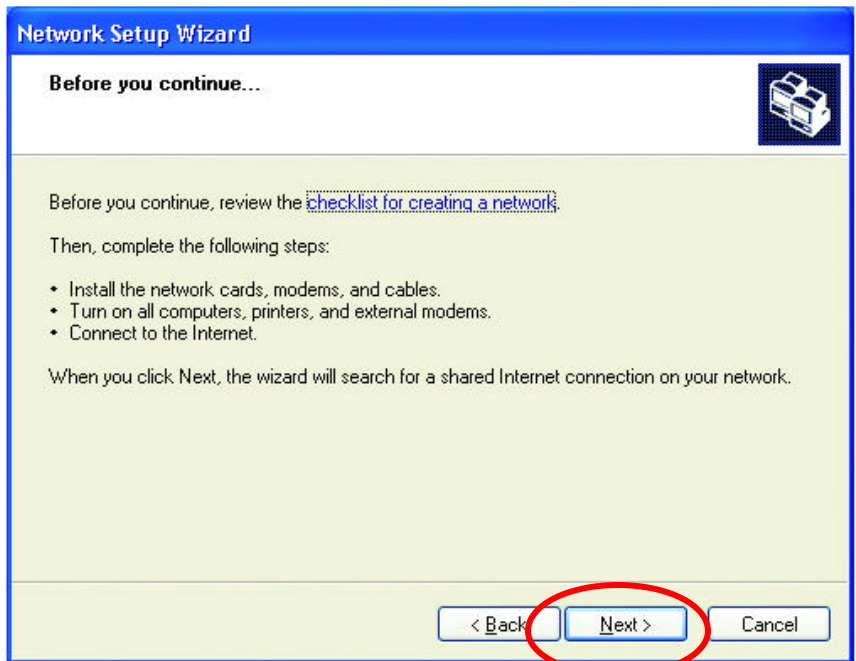
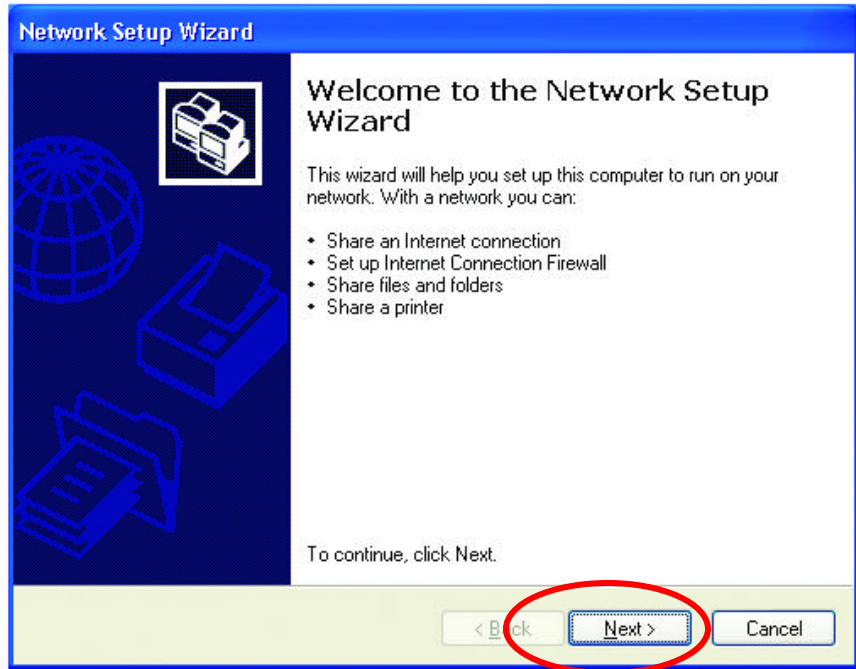
Using the Windows XP Network Setup Wizard

Go to Start menu >
Control Panel >
Network
Connections

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

Click **"Next"** to proceed

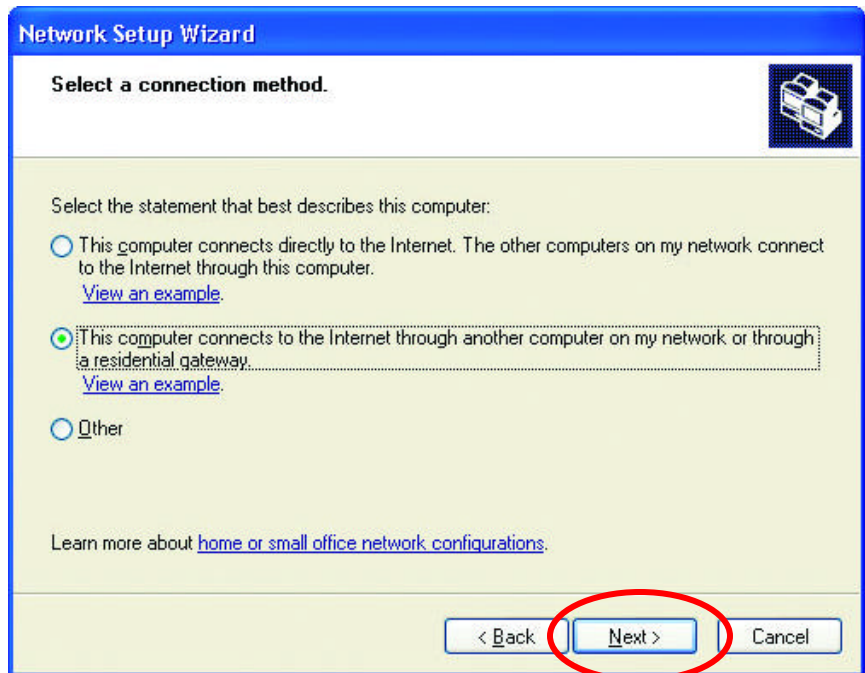
Click **"Next"** to continue



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

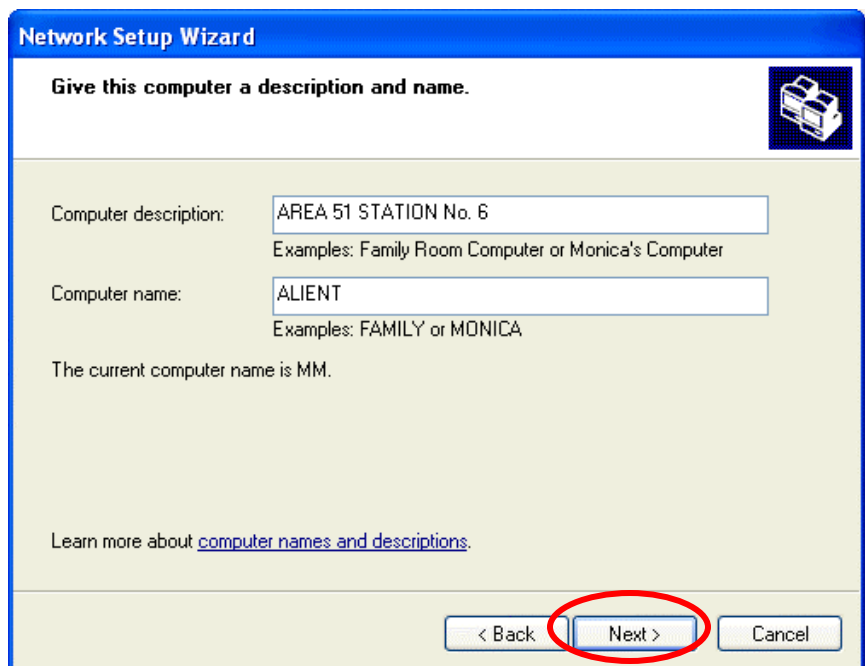
In the case of using router in the network, choose the second option.

Click "**Next**" to continue.



The screenshot shows the 'Network Setup Wizard' window with the title 'Select a connection method.' It contains three radio button options: 'This computer connects directly to the Internet...', 'This computer connects to the Internet through another computer on my network or through a residential gateway.', and 'Other'. The second option is selected. Below the options is a link to 'Learn more about home or small office network configurations.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is circled in red.

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.



The screenshot shows the 'Network Setup Wizard' window with the title 'Give this computer a description and name.' It has two text input fields: 'Computer description:' with the value 'AREA 51 STATION No. 6' and 'Computer name:' with the value 'ALIENT'. Below these fields are examples of names and a note about the current computer name. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is circled in red.

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:
Examples: HOME or OFFICE

< Back **Next >** Cancel

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:

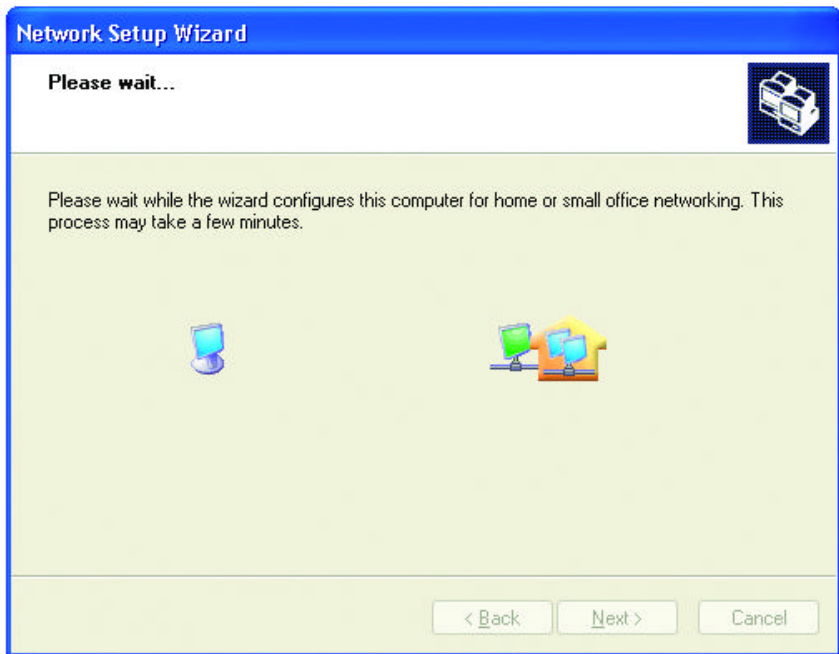
Internet connection settings:
Connecting through another device or computer.

Network settings:

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

To apply these settings, click Next.

< Back **Next >** Cancel



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

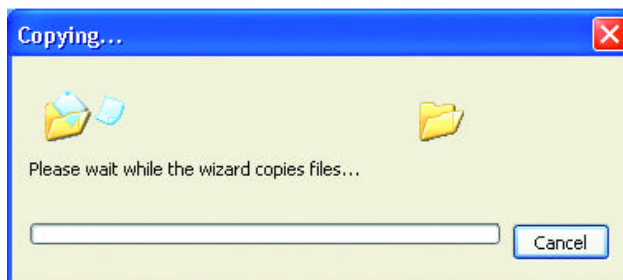
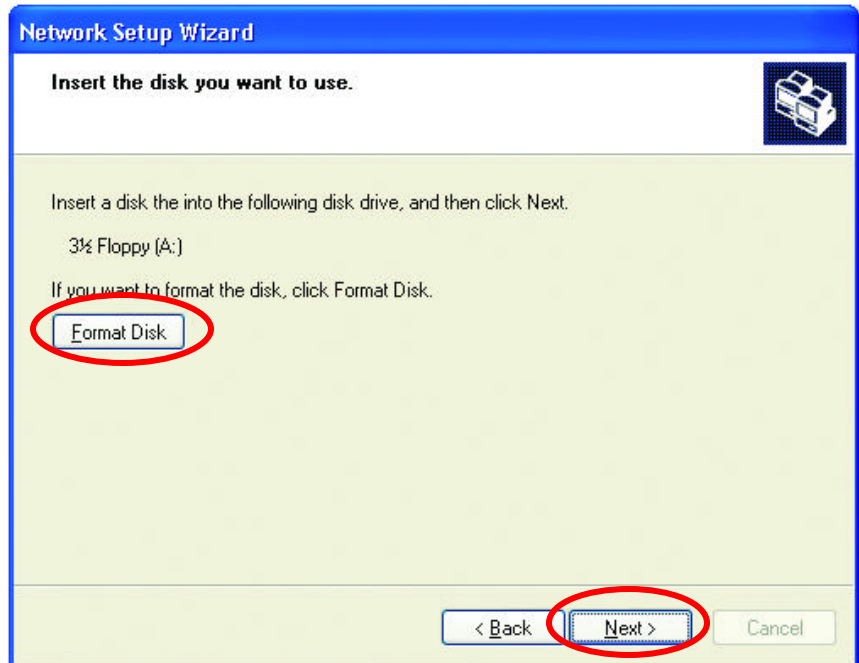
Select the first choice, and insert a floppy disk into your disk drive

Click "**Next**" to continue.

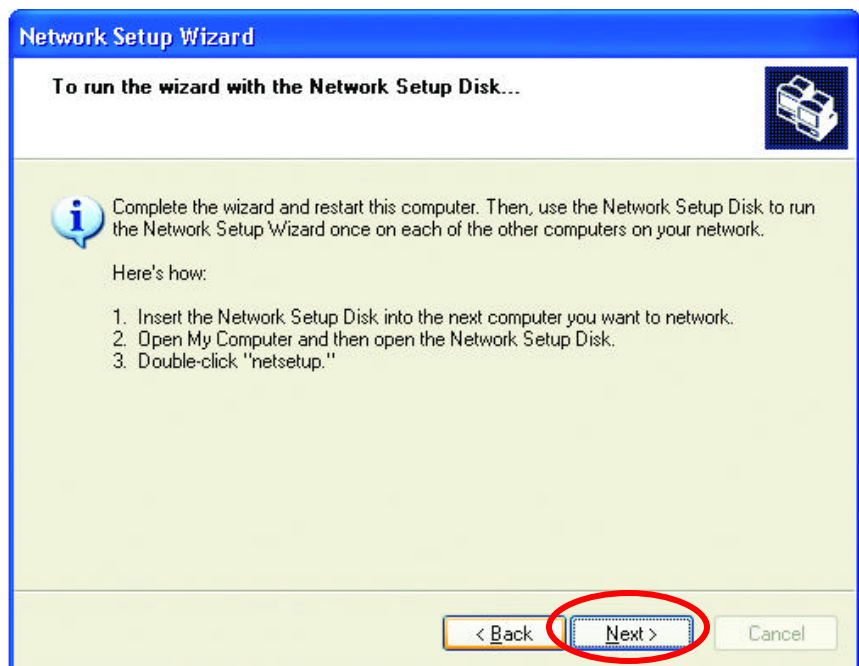


Click "**Format Disk**" if you wish to format the disk.

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



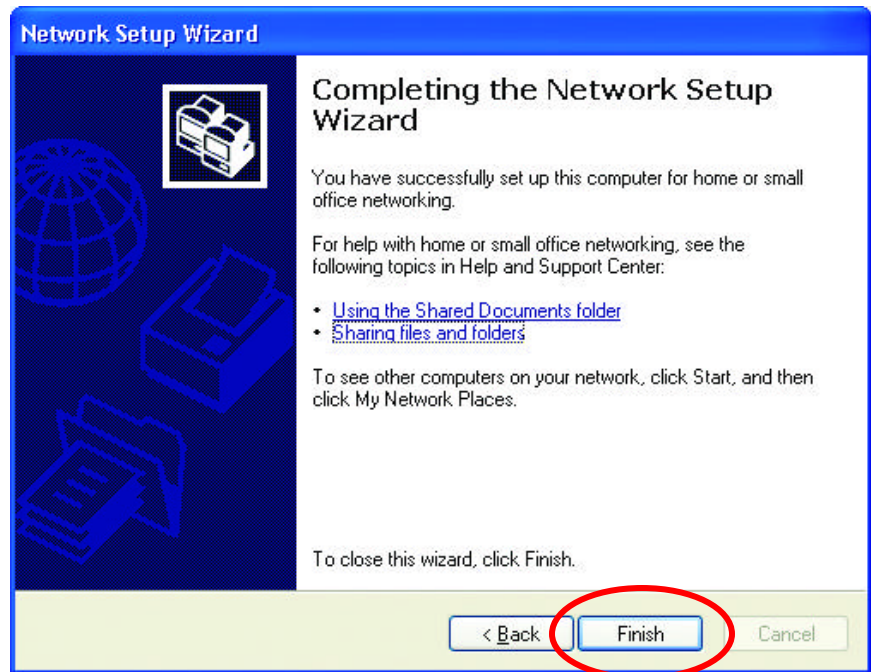
Click "**Next**" to continue with the Network Setup Wizard



NOTE:

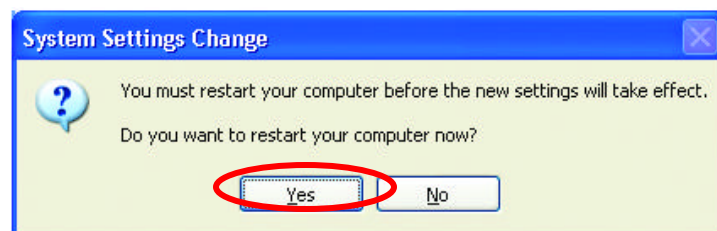
Now you may use the Network Setup Disk you just created in any PCs in your network that you wish to setup. Simply insert the Network Setup Disk into the disk drive of a PC, and open to browse the content of the disk with "My Computer" or "Windows File Manager". Double-click and run the file "netsetup"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

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



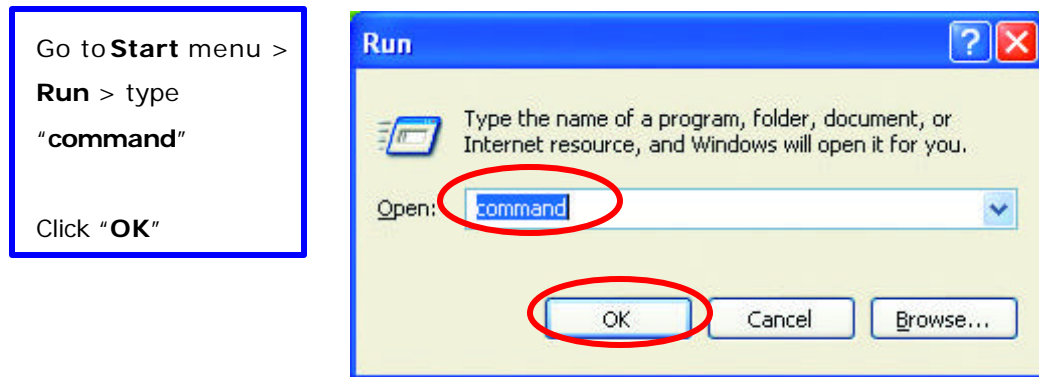
System will now have to restart in order for the new settings to be effective.

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

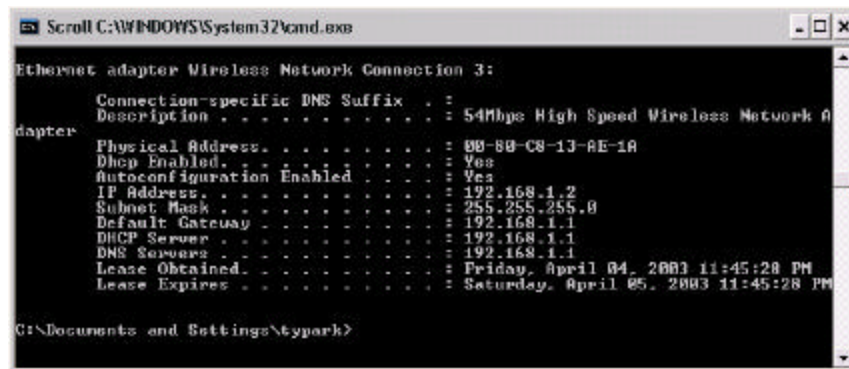


Checking IP Address of Your Computer In Windows XP

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

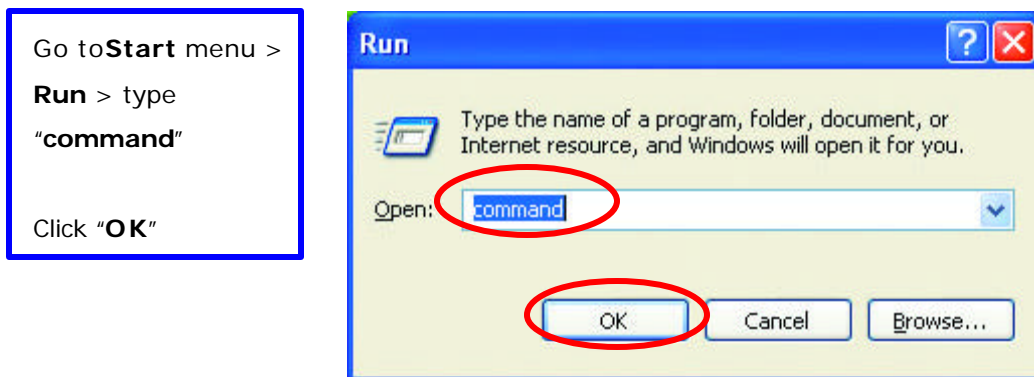


When the command prompt window appears, type command "ipconfig /all" and press Enter. This command will display the IP addresses of all the network adapters in your computer.

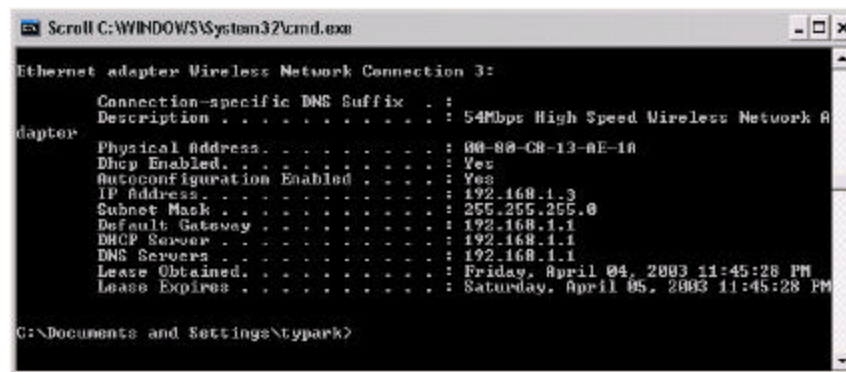


In this case, the IP address of your network adapter is 192.168.1.2 which means your Access Point must have an IP address of 192.168.1.xxx in order for you to be able to access it.

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



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



In this case, the IP address that we acquired is 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.

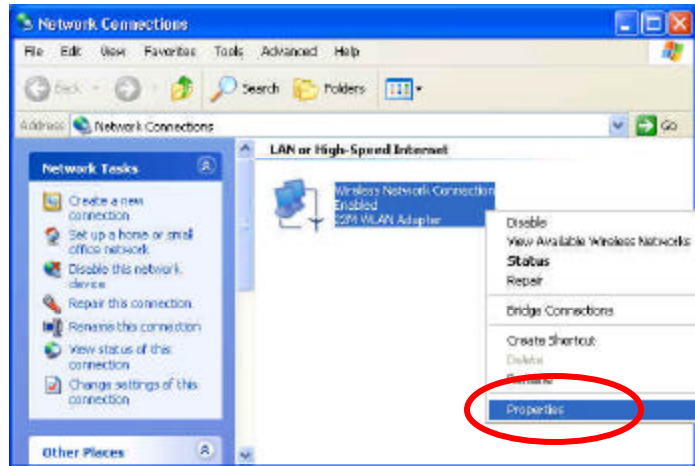
If the above methods for IP renew fail, you will have to try and restart the computer, which will reinitializes the network adapter settings during startup including renewing IP address. If you still have problems getting an IP address after computer restarts, you will have to consult with your MIS in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

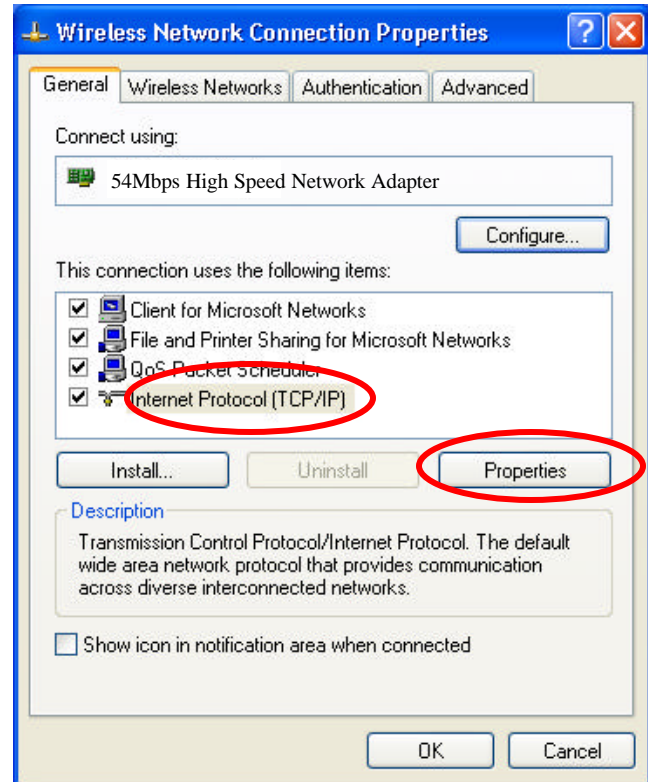


NOTE:

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 window would appear.

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

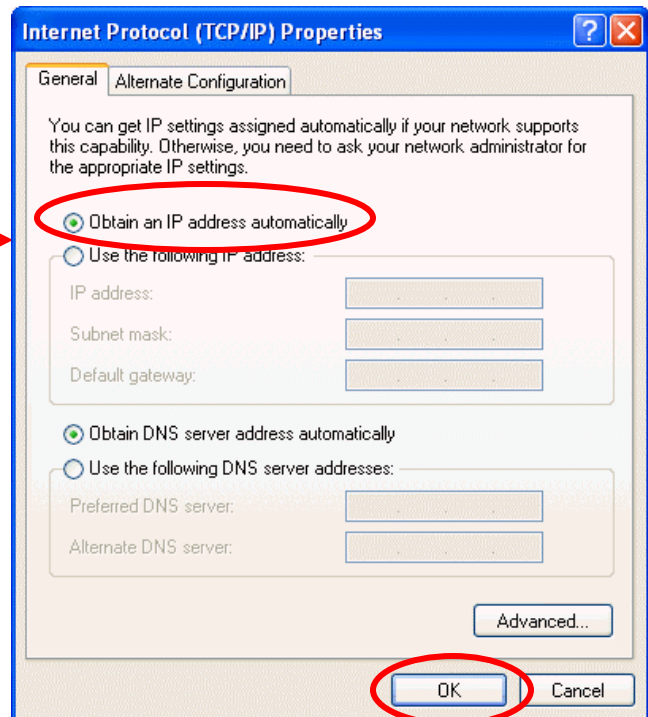


Dynamically Assigned IP Address

The TCP/IP Properties window appears.

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

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



Static IP Address

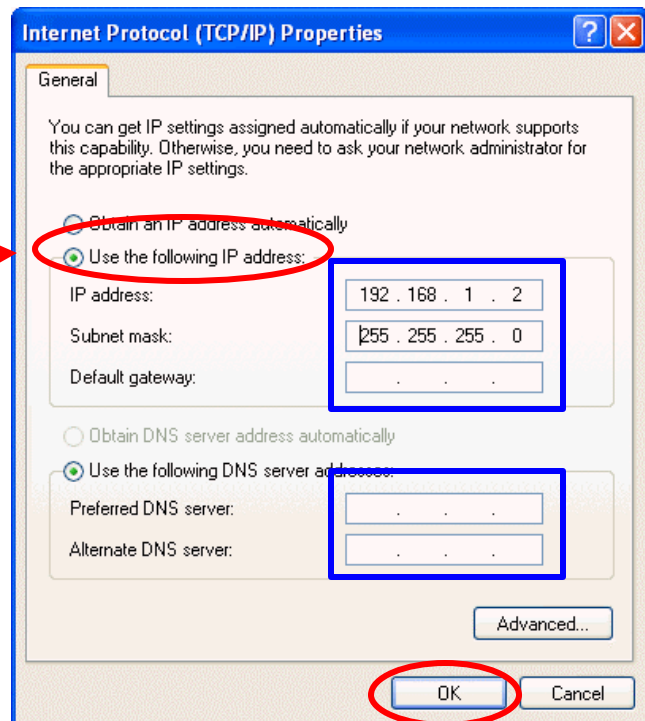
Select "**Use the following IP address**"

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

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

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

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



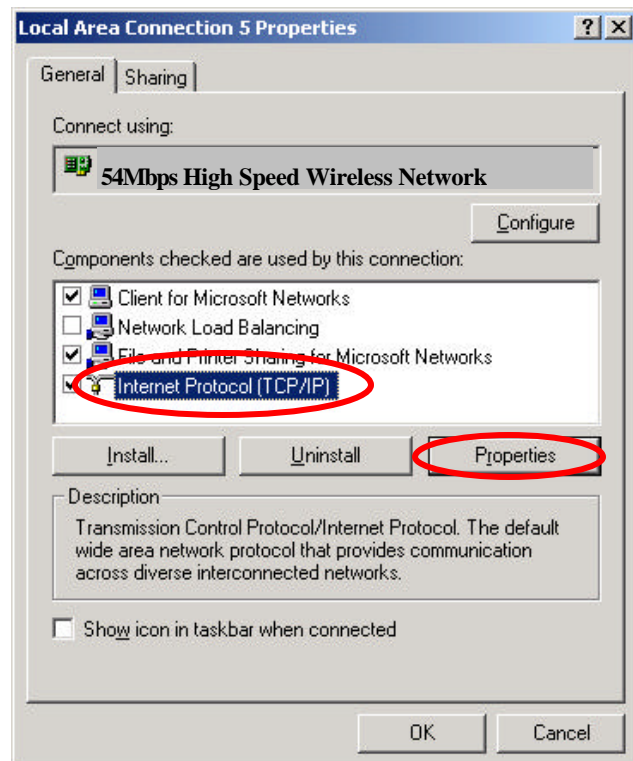
NOTE:

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

Wireless Network in Windows 2000

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

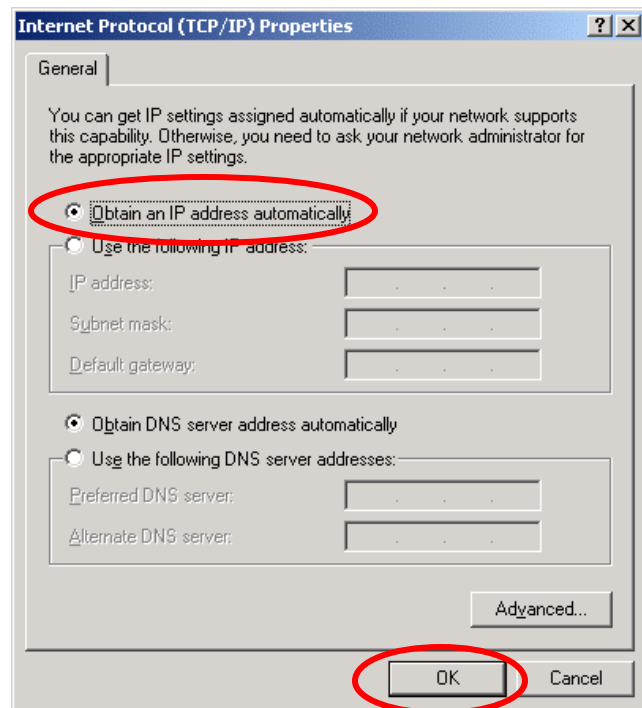
Select "**Internet Protocol (TCP/IP)**" and click "**Properties**"



The TCP/IP Properties window appears.

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

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



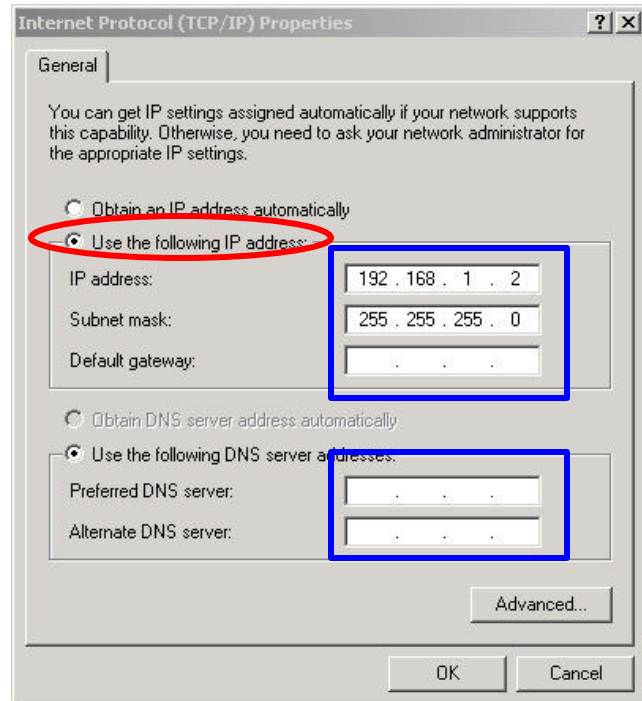
Select "**Use the following IP address**"

Enter the IP address and subnet mask fields.

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

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

Click "**OK**" to close the window



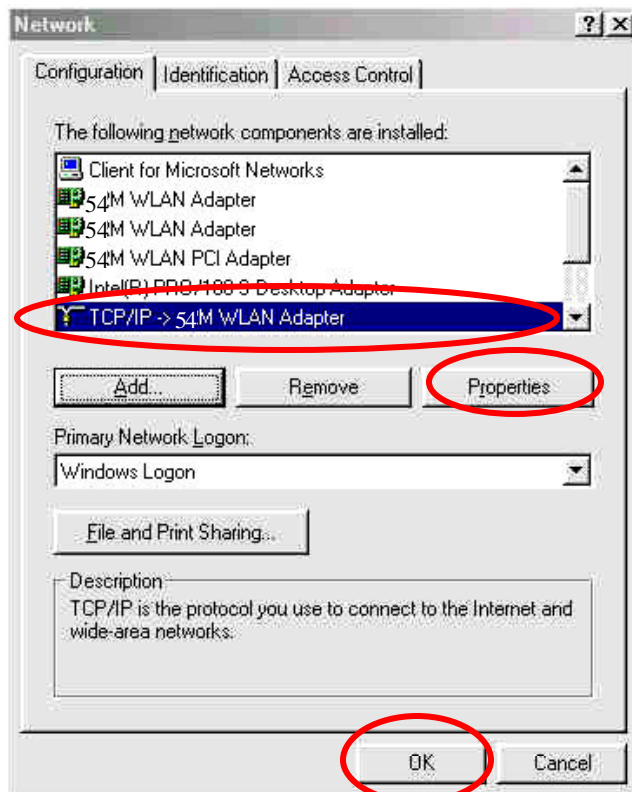
Wireless Network In Windows 98 and Windows ME

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

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

Click "**Properties**" to
continue

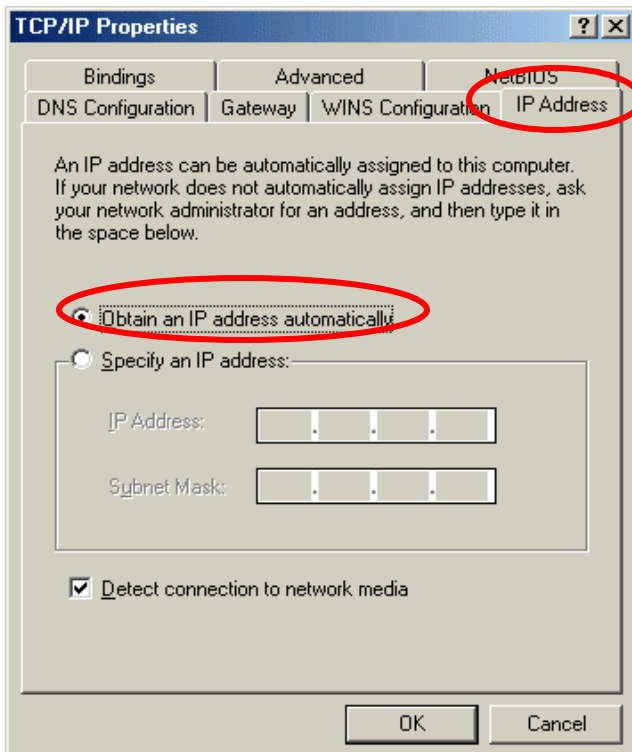
The Access Point restarts
itself, and the screen will
switch back to startup page–
Link Information



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



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

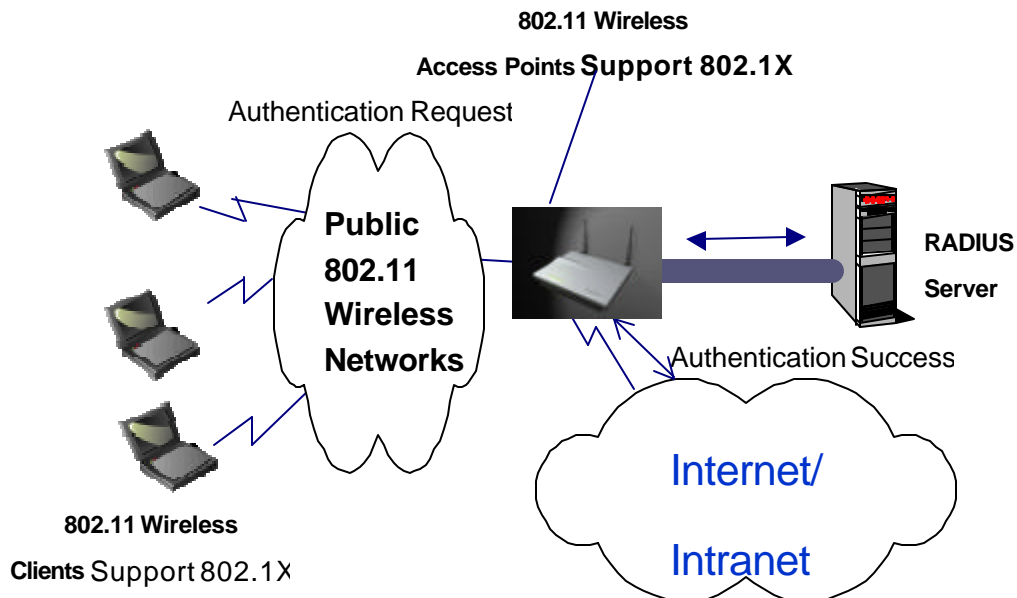
(2) Enter the IP address of the Router in the **DNS server** field



APPENDIX C: 802.1x Authentication Setup

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

802.1x Authentication Infrastructure



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

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

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

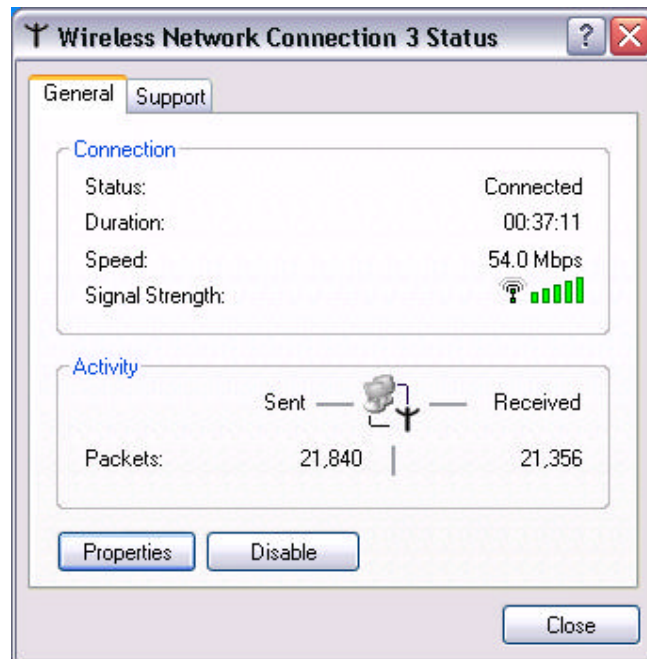
Supplicant: Wireless Network PC Card

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

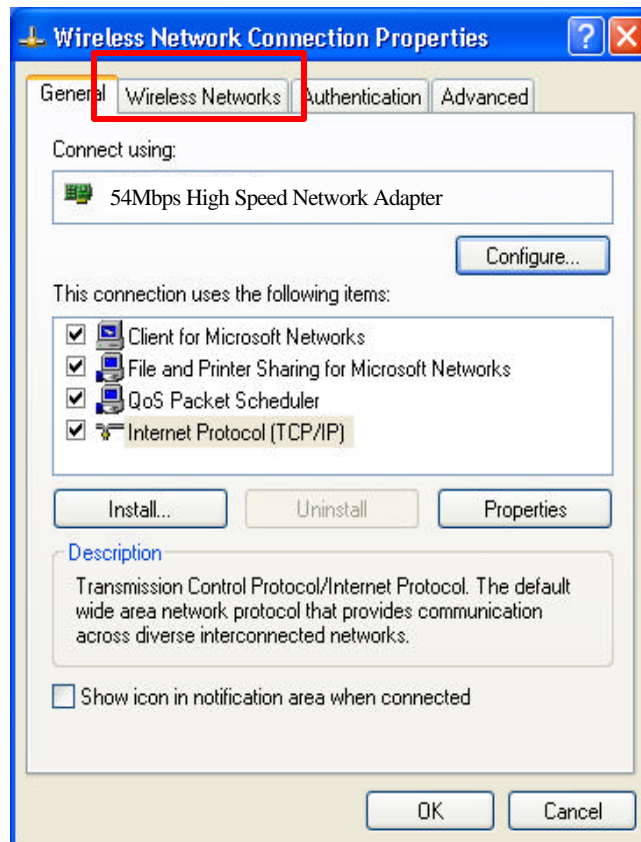
Please note that the setup illustration is based on our 54Mbps wireless PC Card.

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 54Mbps wireless PC Card.

- Click **"Properties"** to open up the Properties setting window.

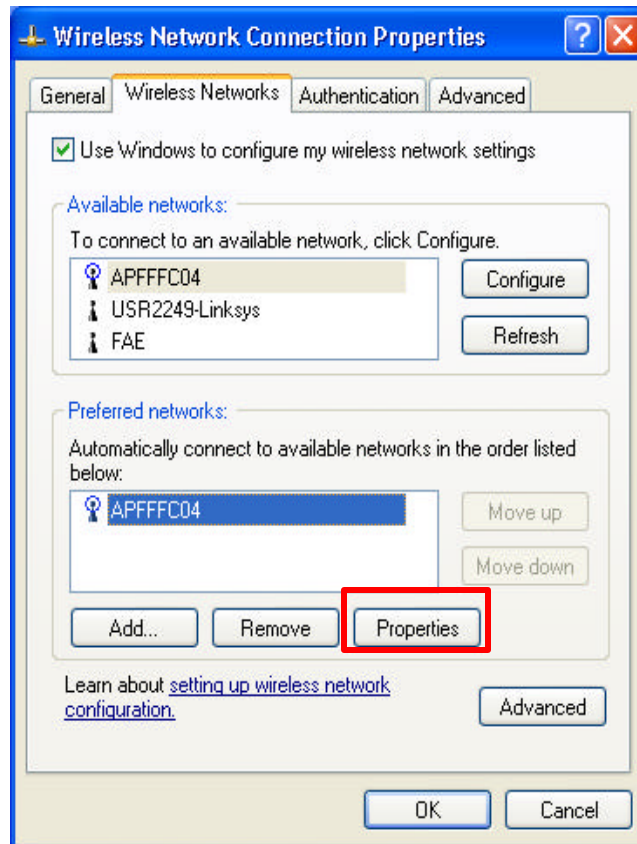


- Click on the **"Wireless Network"** tab.



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

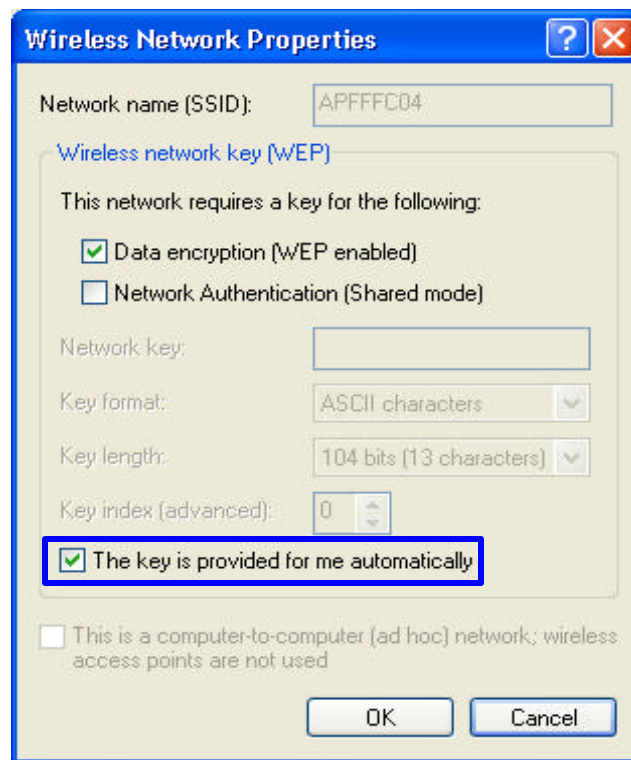
Please note that if you are going to change to a different 802.1x authentication EAP method, i.e. switch from using MD5 to TLS, you must remove the current existing wireless network from your Preferred networks first, and add it in again.



To configure for using TLS authentication method, please follow steps 7 ~ 25.
Please follow steps 26 ~ for using MD5 authentication method.

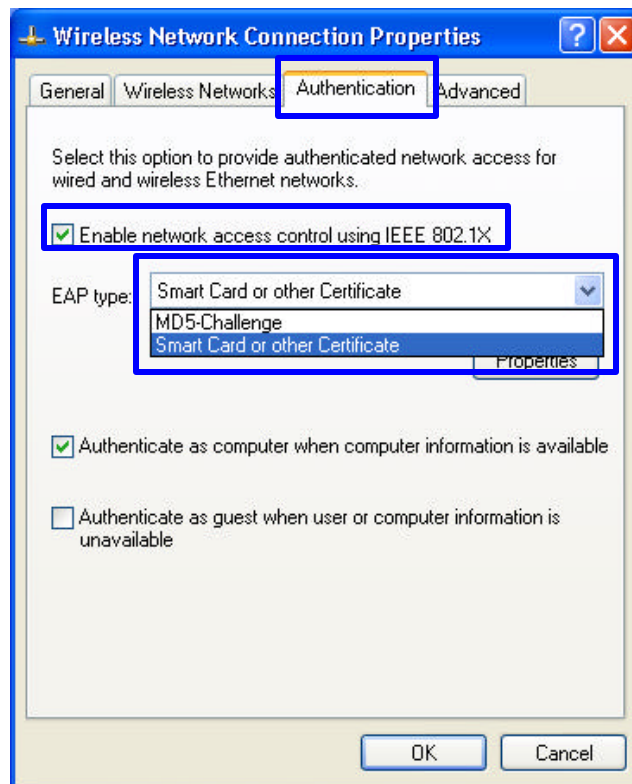
TLS Authentication

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



8. Click "**OK**" to close the Wireless Network Properties window.
9. Click "Authentication" tab
10. Select "**Enable network access control using IEEE 802.1x**" option to enable 802.1x authentication.

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



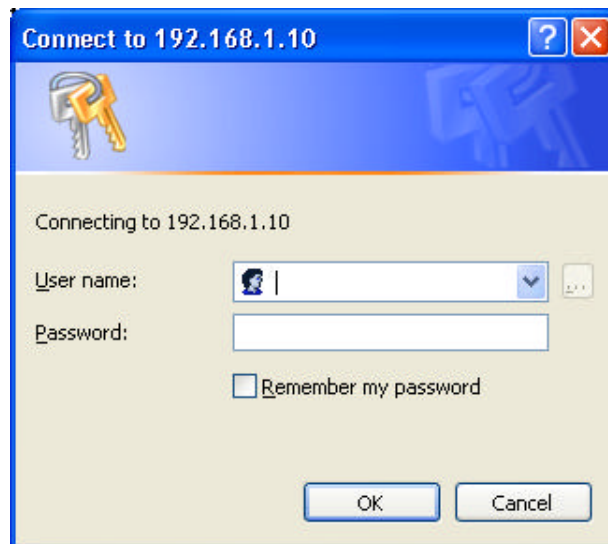
12. Click "**OK**" to close the Wireless Network Connection Properties window, thus make the changes effective.

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

TLS Authentication – Download Digital Certificate from Server

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

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

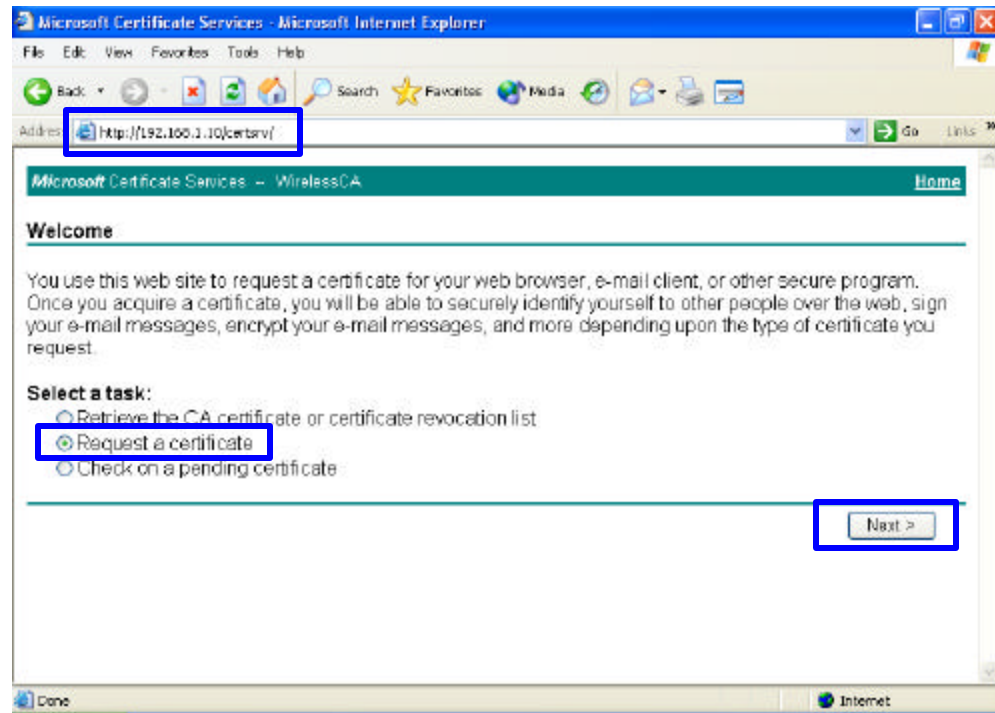


Please note that we use IP addresses for connection with the server for our illustration, and the IP of the server is 192.168.1.10.

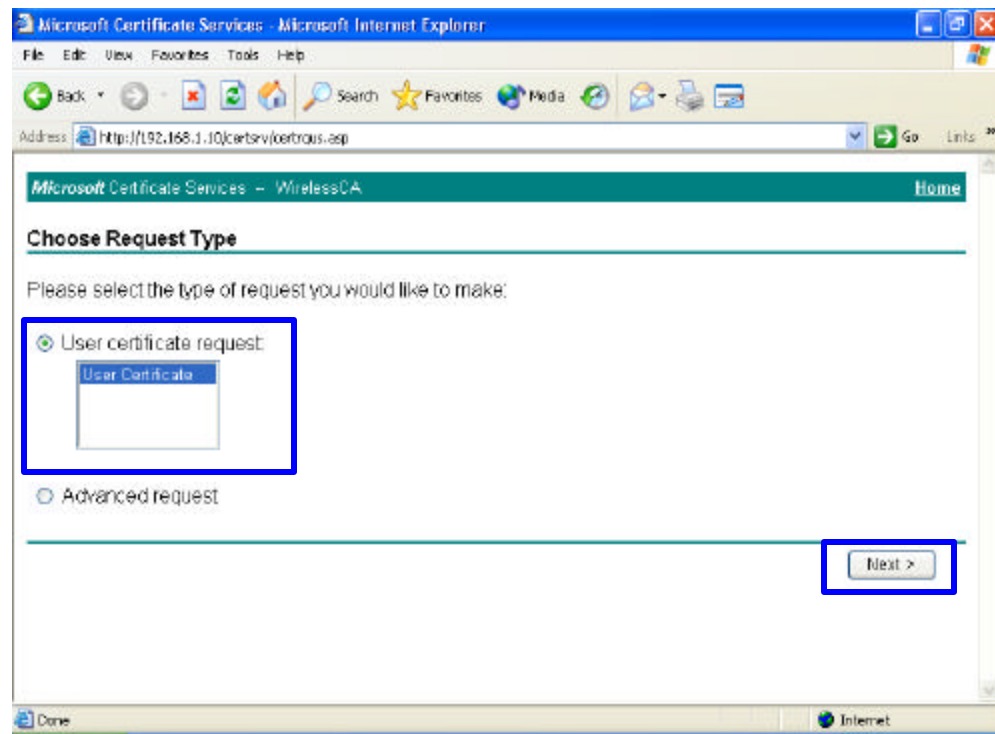
15. After successful login, open up your Internet Browser, and type the following in the address field.
http://192.168.1.10/certsrv

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

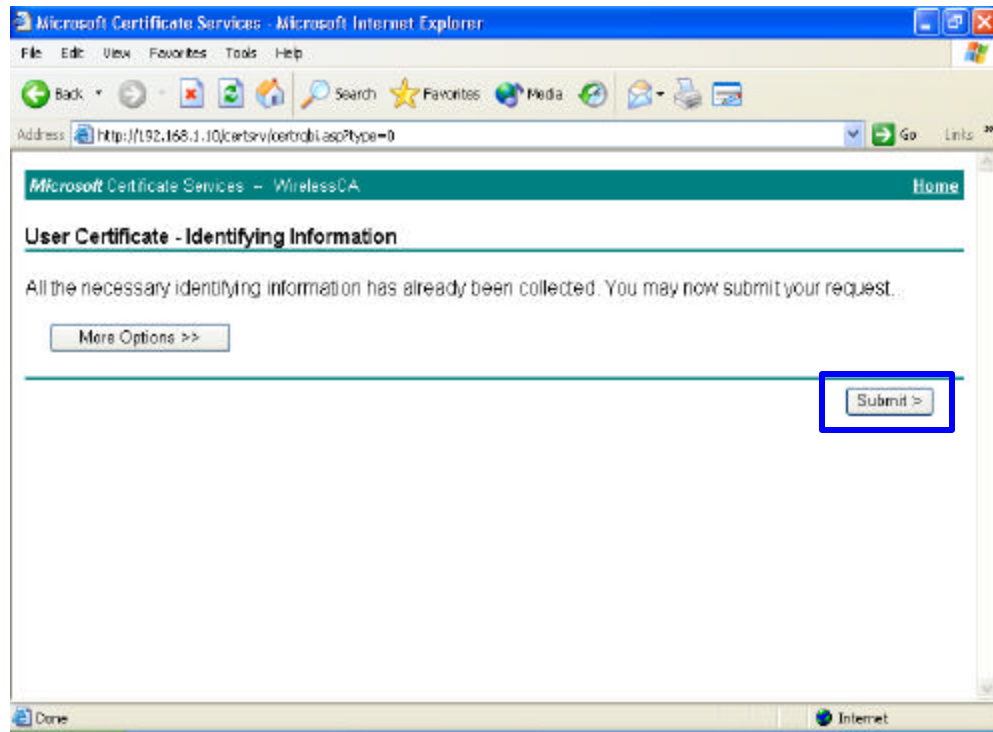
16. Now we are connected to the Certificate Service. Select **"Request a certificate"**, and click **"Next"** to continue.



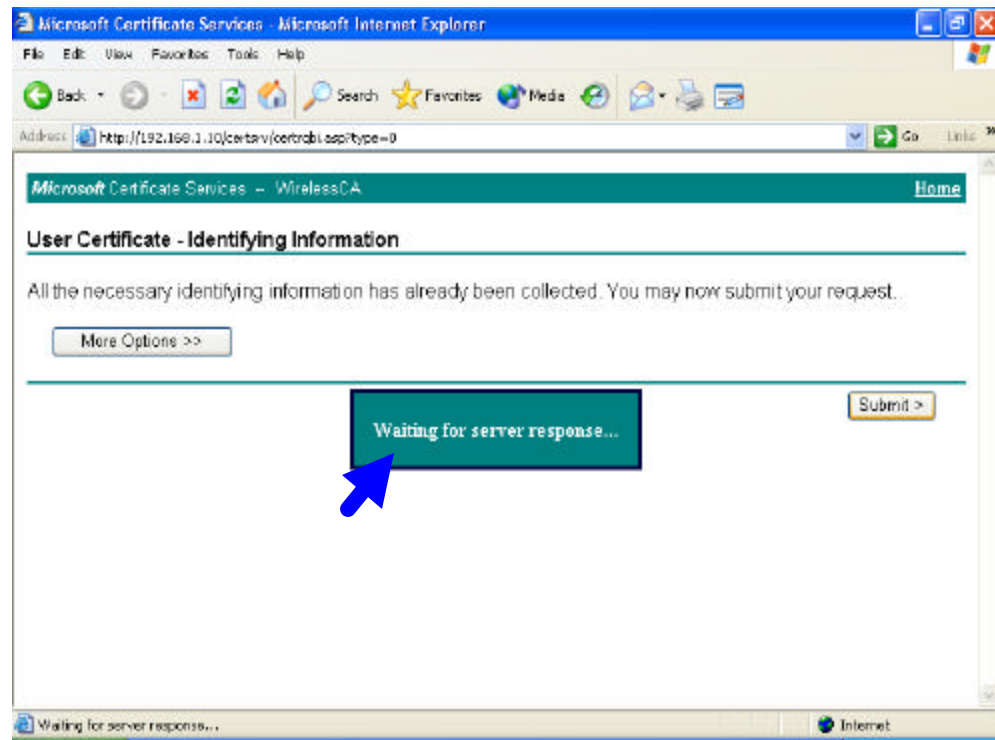
17. Select **"User Certificate request"**, and click **"Next"** to continue.



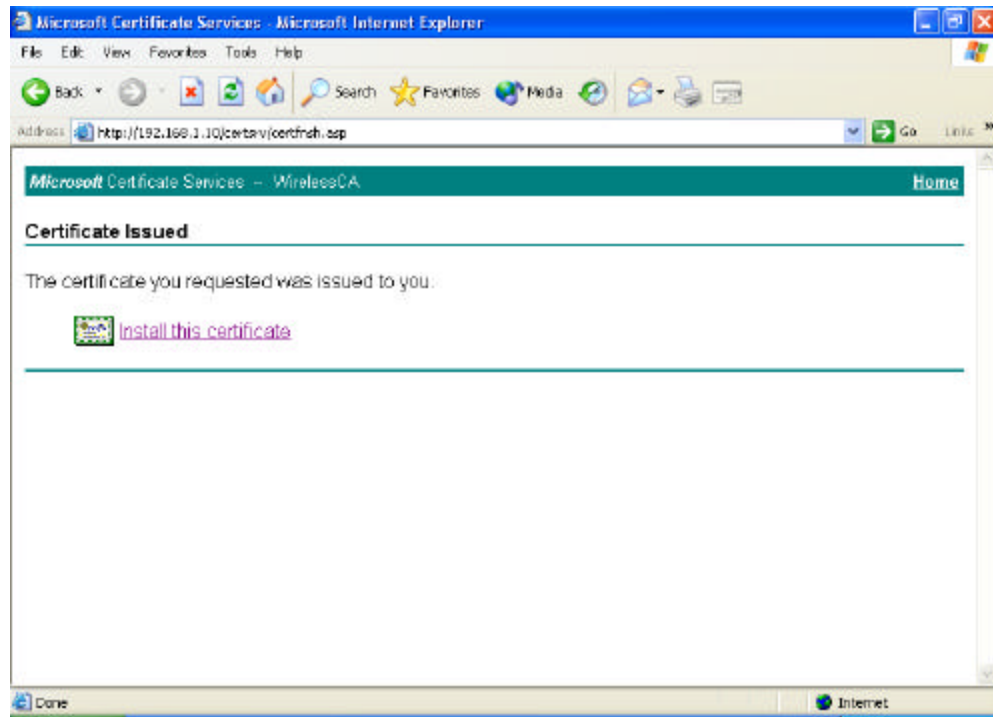
18. Click "**Submit >**" to continue.



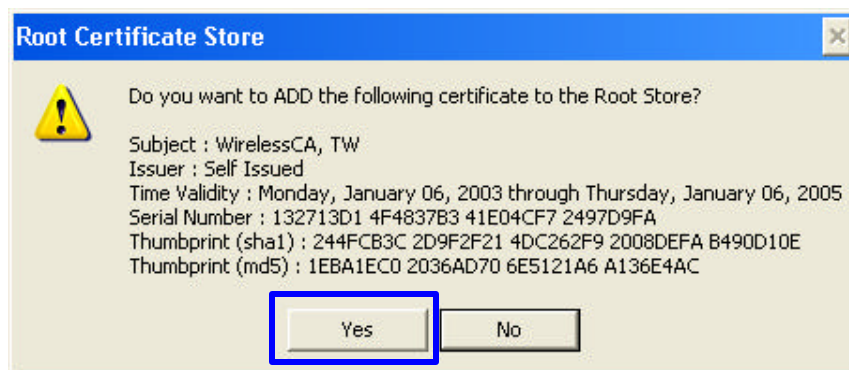
19. The Certificate Service is now processing the certificate request.



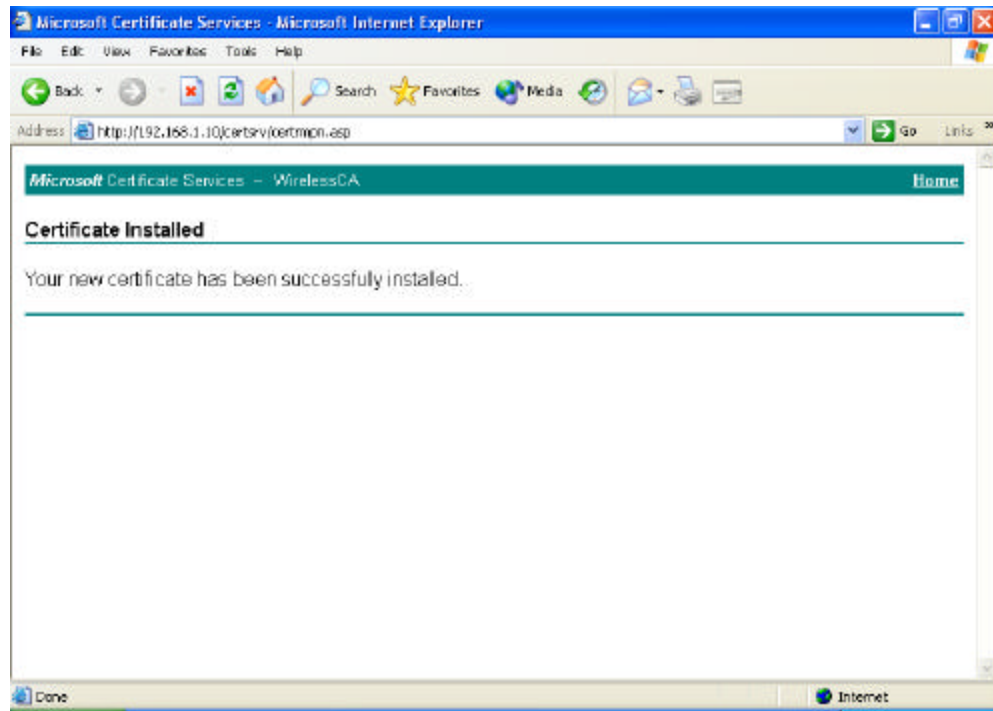
20. The certificate is issued by the server, click "**Install this certificate**" to download and store the certificate to your local computer.



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

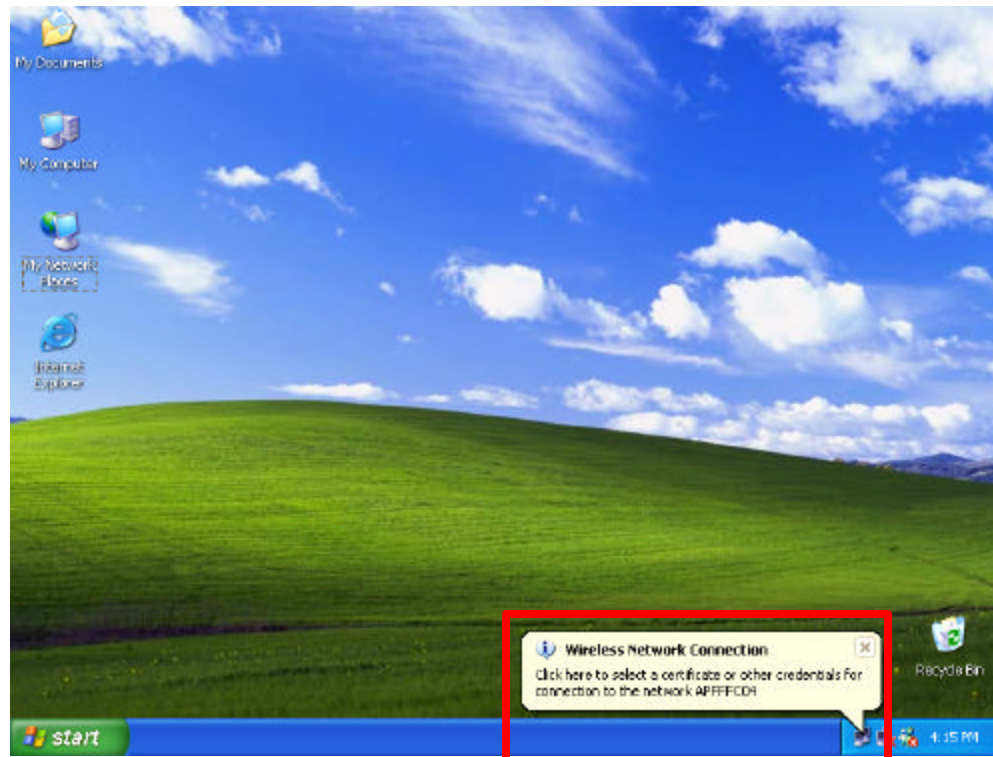


22. Certificate is now installed.

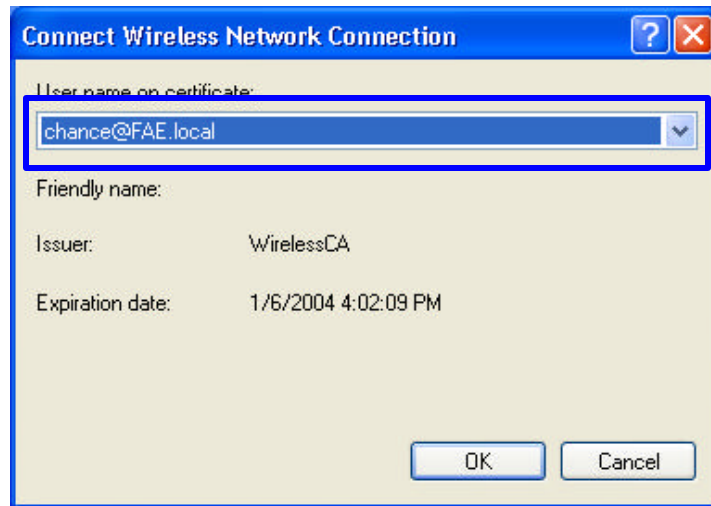


All the configuration and certificate download are now complete. Let's try to connect to the Access Point using 802.1x TLS Authentication.

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



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

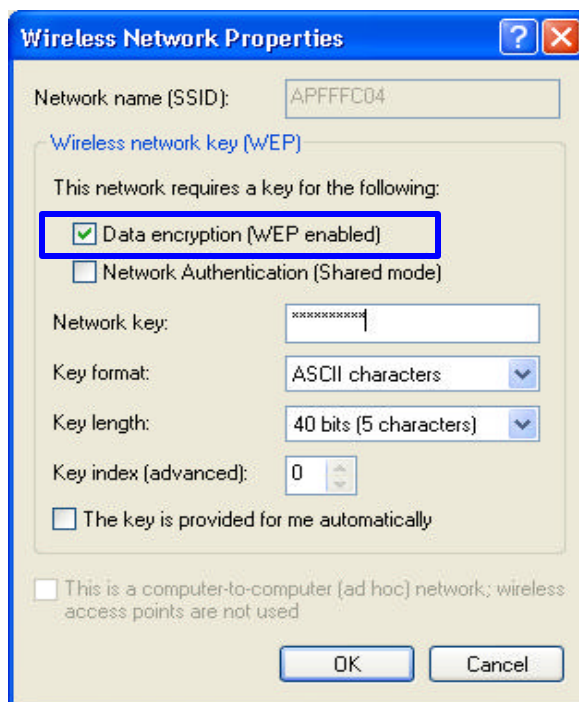


25. Check the server to make sure that it's the server that issues certificate, and click **"OK"** to complete the authentication process.



MD5 Authentication

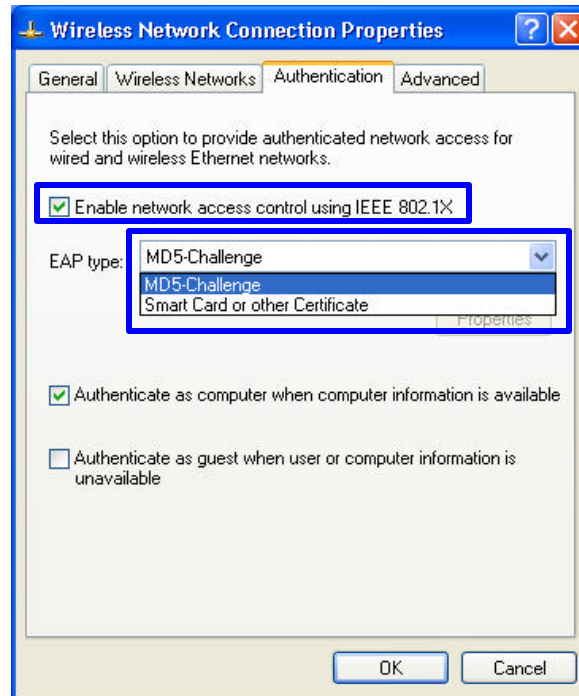
26. Select "**Data encryption (WEP enabled)**" option, but leave other option unselected.
27. Select the key format that you want to use to key in your Network key.
ASCII characters: 0~9, a~z and A~Z
HEX characters: 0~9, a~f
28. Select the **key** length that you wish to use
40 bits (5 characters for ASCII, 10 characters for HEX)
104 bits (13 characters for ASCII, 26 characters for HEX)
29. After deciding the key format and key length that you wish to use for network key. Enter the network key in "**Network key**" text box.



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

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

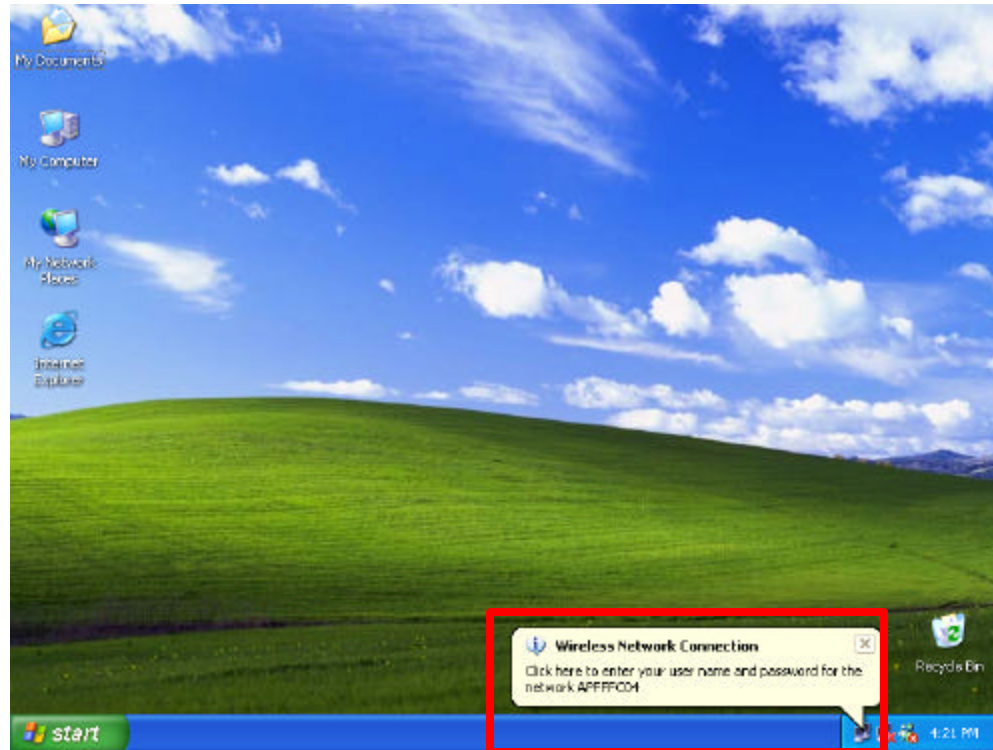
31. Select "**Authentication**" tab.
32. Select "**Enable network access control using IEEE 802.1X**" to enable 802.1x authentication.
33. Select "**MD-5 Challenge**" from the drop-down list box for EAP type.



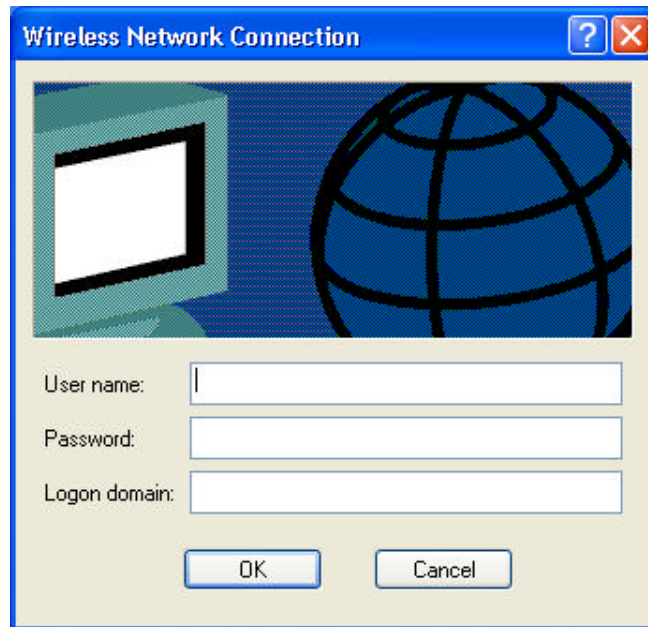
34. Click "**OK**" to close Wireless Network Connection Properties window, thus make all the changes effective.

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

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



36. Enter the user name, password and the logon domain that your account belongs if you have one or more network domain exist in your network.
37. Click **“OK”** to complete the validation process.



Authenticator: Wireless Network Access Point

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

The screenshot shows the web configuration interface for a LevelOne Access Point. The top navigation bar includes links for 'wizard', 'Status', 'Basic Setting', 'IP Setting', 'Advanced Setting', 'Security', '802.1x', and 'Tools'. The '802.1x' tab is currently selected. On the left side, there is a blue vertical bar with the text '802.1x' and a small icon. The main configuration area is titled '802.1x' and contains the following settings:

- 802.1x** ☒ Enabled ☐ Disabled
- Encryption Key Length** ☒ 64 bits ☐ 128 bits ☐ 256bits
- Lifetime** 30 Minutes (dropdown menu)
- RADIUS Server 1**
 - IP**: [0] [0] [0] [0]
 - Port**: 1812
 - Shared Secret**: [text input field]
- RADIUS Server 2 (optional)**
 - IP**: [0] [0] [0] [0]
 - Port**: [0]
 - Shared Secret**: [text input field]

At the bottom of the configuration area are three buttons: 'Apply', 'Cancel', and 'Help'.

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

Select the **Lifetime of the Encryption Key** from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.

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

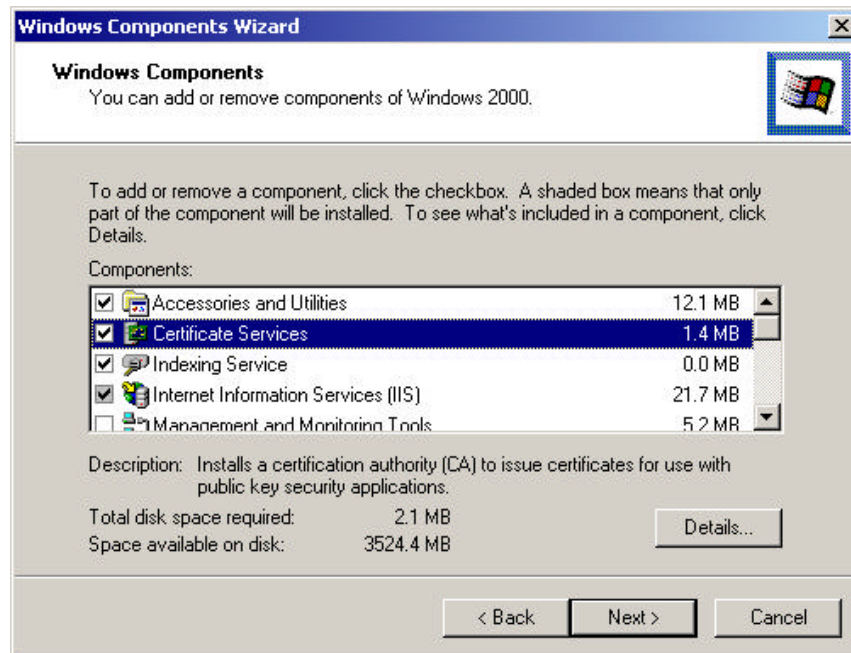
NOTE:

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

Radius Server: Window2000 Server

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

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



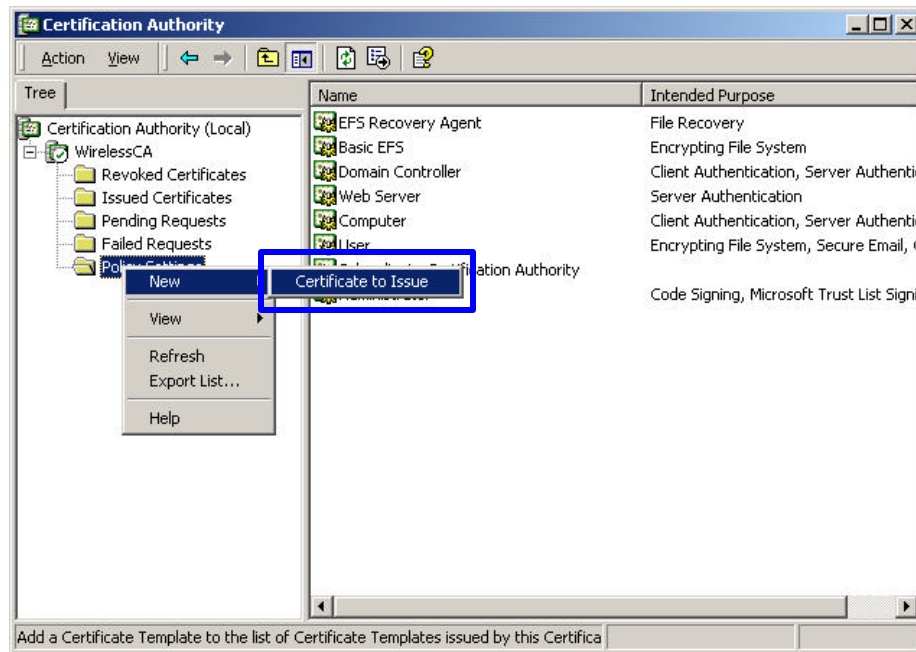
5. Select **“Enterprise root CA”**, and click **“Next”** to continue.

The screenshot shows the 'CA Identifying Information' window of the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The subtitle is 'CA Identifying Information' with the instruction 'Enter information to identify this CA'. The window contains several text input fields: 'CA name' (filled with 'WirelessCA'), 'Organization', 'Organizational unit', 'City', 'State or province', 'Country/region' (filled with 'US'), 'E-mail', and 'CA description'. There is also a 'Valid for' section with a spinner set to '2' and a dropdown set to 'Years', and an 'Expires' date field filled with '1/8/2005 12:15 PM'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

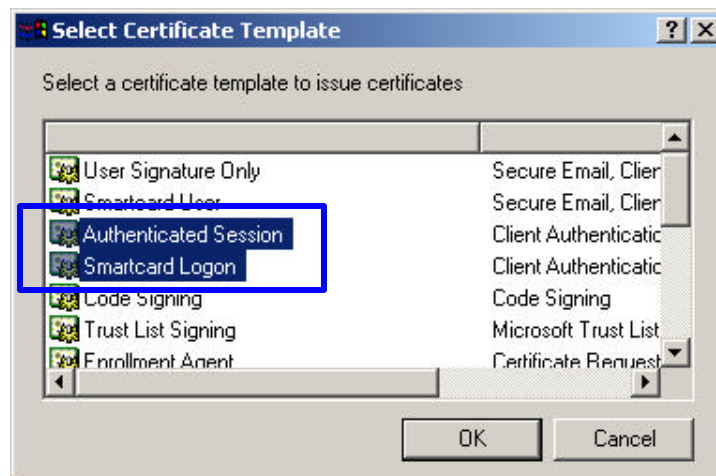
6. Enter the information that you want for your Certificate Service, and click **“Next”** to continue.

The screenshot shows the 'Certification Authority Type' window of the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The subtitle is 'Certification Authority Type' with the instruction 'There are four types of certification authorities.' The window contains a list of 'Certification Authority types' with radio buttons: 'Enterprise root CA' (selected), 'Enterprise subordinate CA', 'Stand-alone root CA', and 'Stand-alone subordinate CA'. To the right is a 'Description' text box containing the text: 'The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.' At the bottom left is a checkbox for 'Advanced options'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

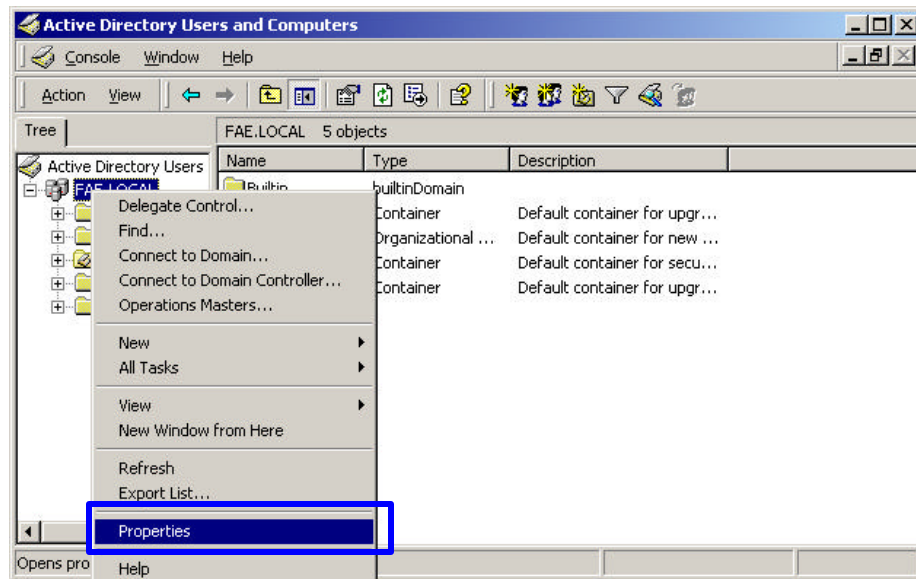
7. Go to Start > Program > Administrative Tools > **Certificate Authority**
8. Right-click on the "**Policy Setting**", select "**new**"
9. Select "**Certificate to Issue**"



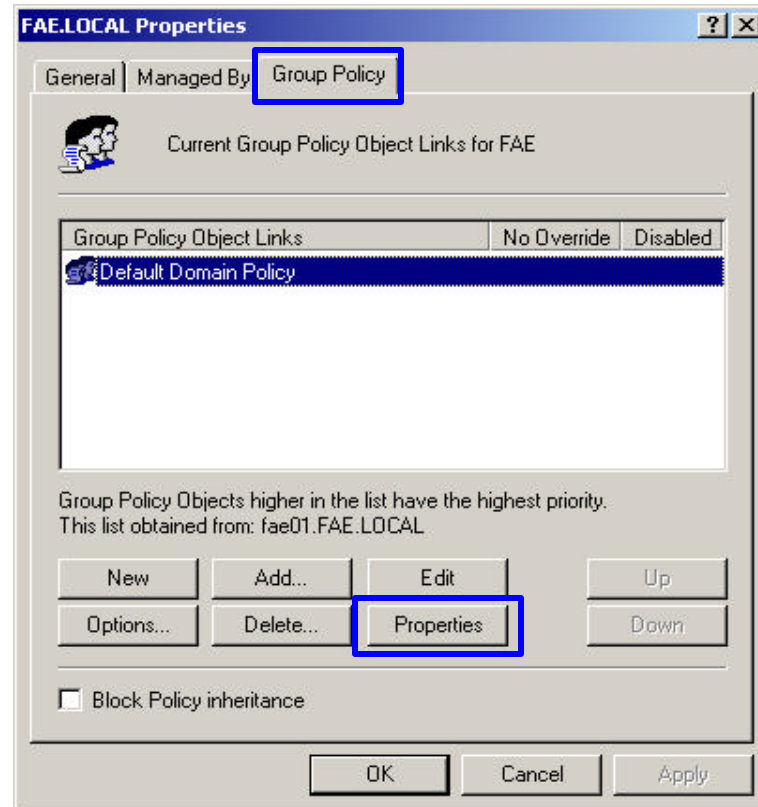
10. Select "**Authenticated Session**" and "**Smartcard Logon**" by holding down to the Ctrl key, and click "**OK**" to continue.



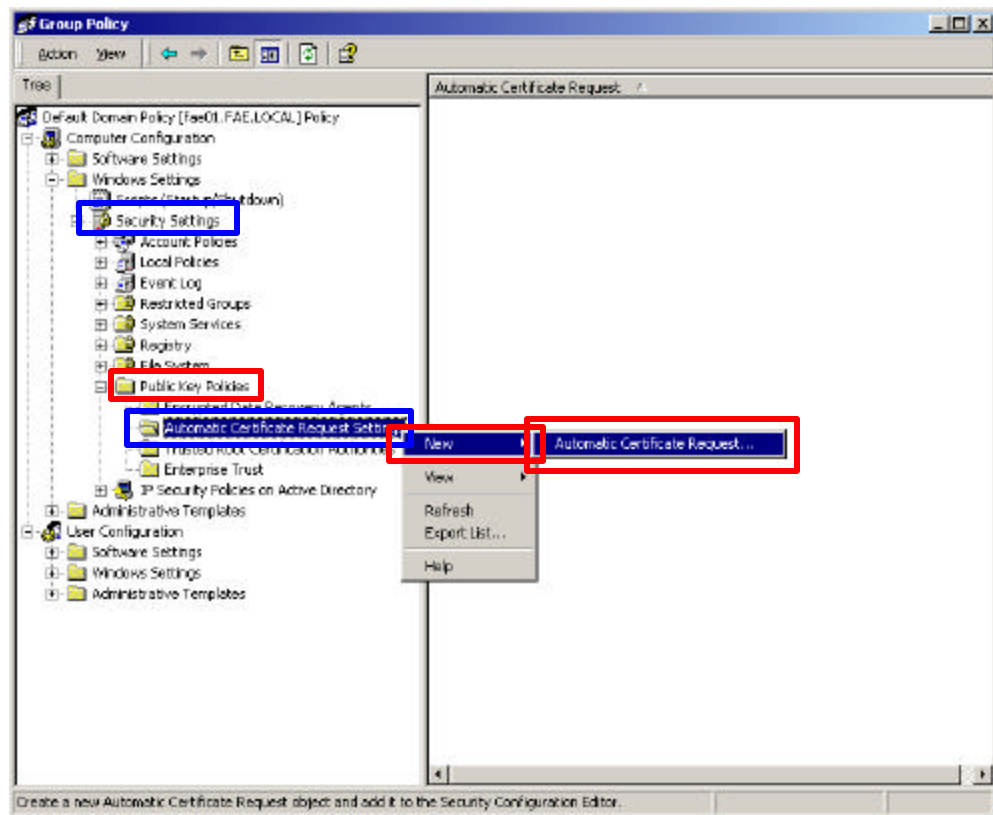
11. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.
12. Right-click on domain, and select "**Properties**" to continue.



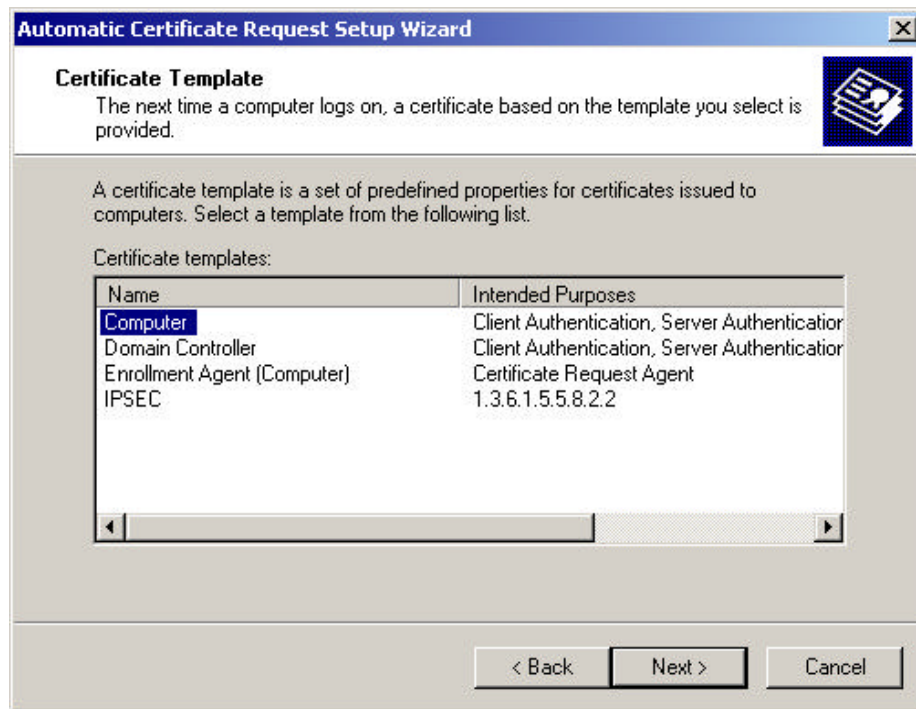
13. Select "**Group Policy**" tab and click "**Properties**" to continue.



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

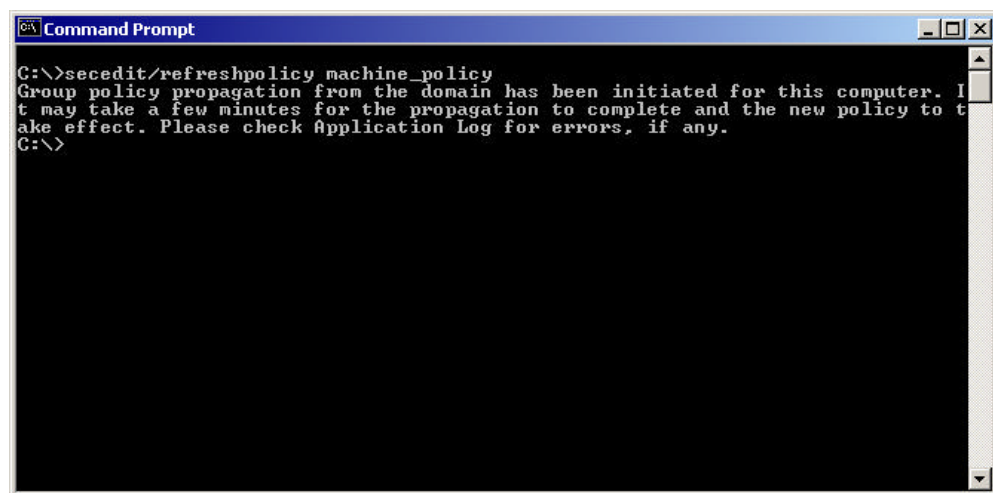


17. The Automatic Certificate Request Setup Wizard will guide you through the Automatic Certificate Request setup, simply click "**Next**" through to the last step.



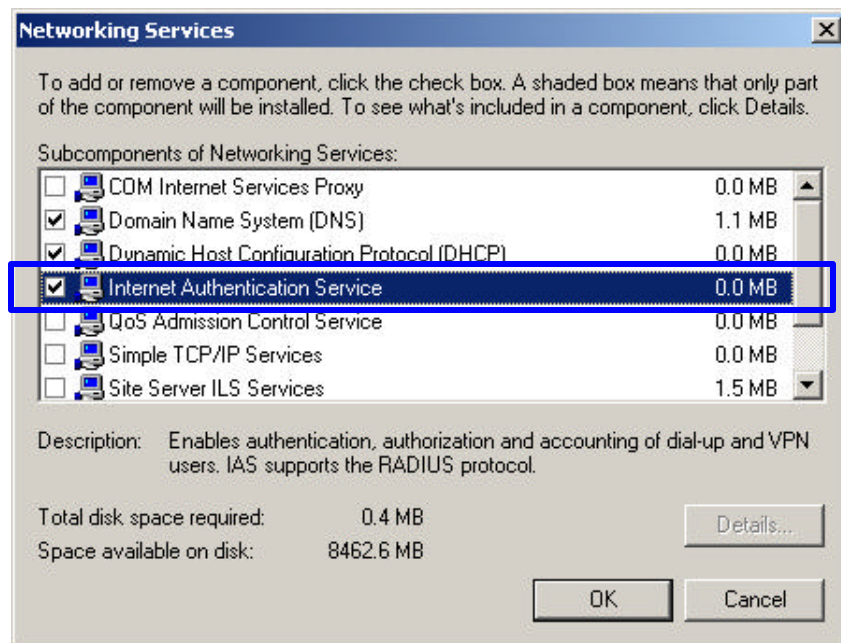
18. Click "**Finish**" to complete the Automatic Certificate Request Setup
19. Go to Start > **Run**, and type "**command**" and click "**Enter**" to open Command Prompt.
20. Type "secedit/refreshpolicy machine_policy" to refresh policy.

Adding Internet Authentication Service



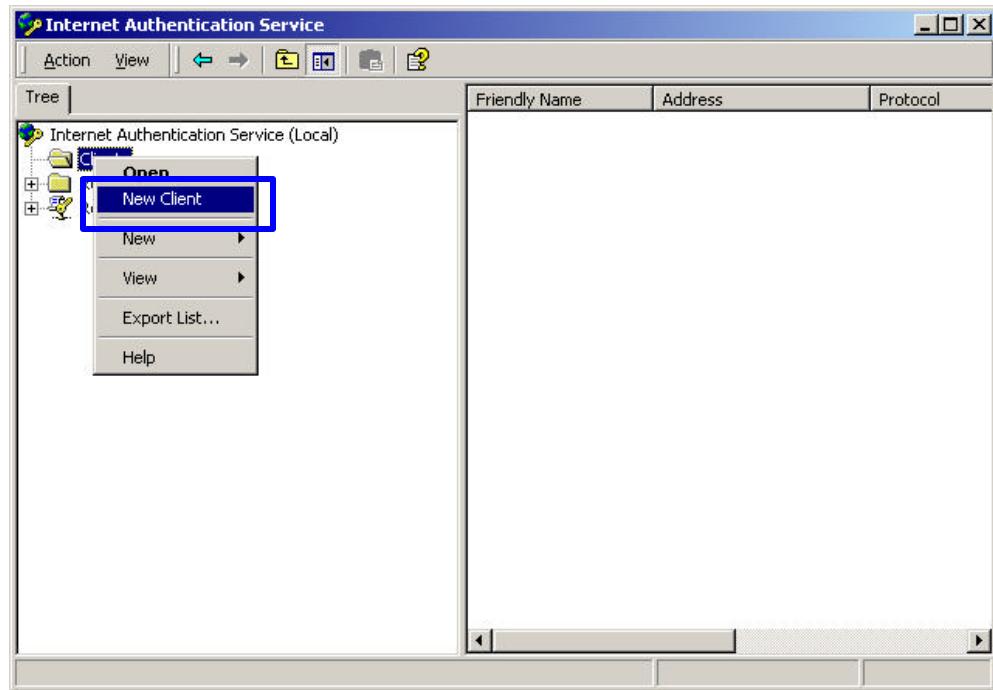
21. Go to Start > Control Panel > **Add or Remove Programs**
22. Select "**Add/Remove Windows Components**" from the panel on the left.

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

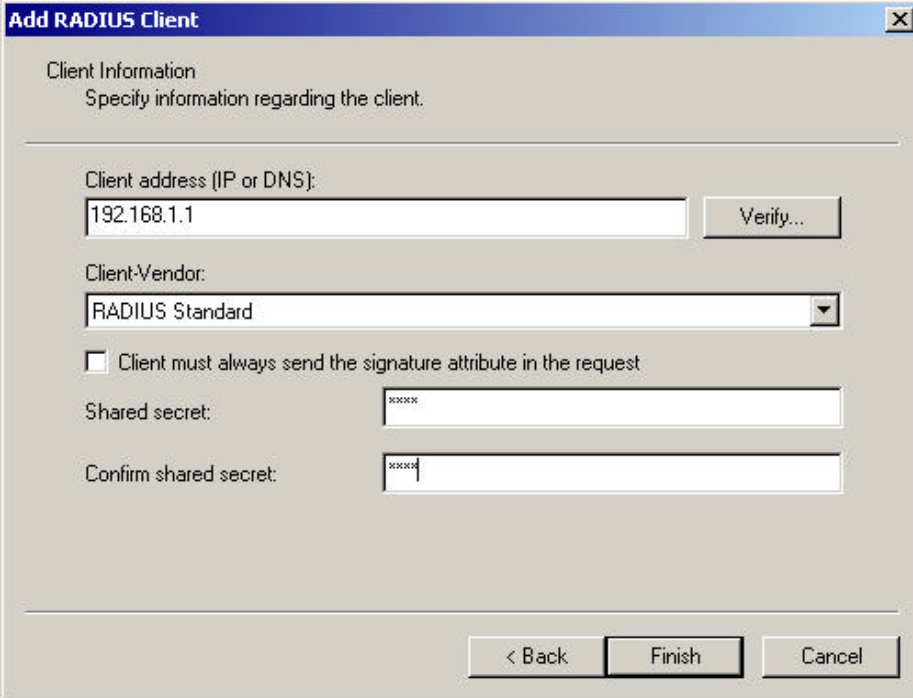


Setting Internet Authentication Service

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



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



The image shows a Windows-style dialog box titled "Add RADIUS Client". The dialog has a blue title bar with a close button (X) in the top right corner. Below the title bar, the text "Client Information" is followed by the instruction "Specify information regarding the client." A horizontal line separates this header from the input fields. The first field is labeled "Client address (IP or DNS):" and contains the text "192.168.1.1". To its right is a "Verify..." button. The second field is labeled "Client-Vendor:" and is a dropdown menu showing "RADIUS Standard". Below these is a checkbox labeled "Client must always send the signature attribute in the request", which is currently unchecked. The next two fields are "Shared secret:" and "Confirm shared secret:", both containing masked text represented by "x" characters. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):
192.168.1.1 Verify...

Client-Vendor:
RADIUS Standard

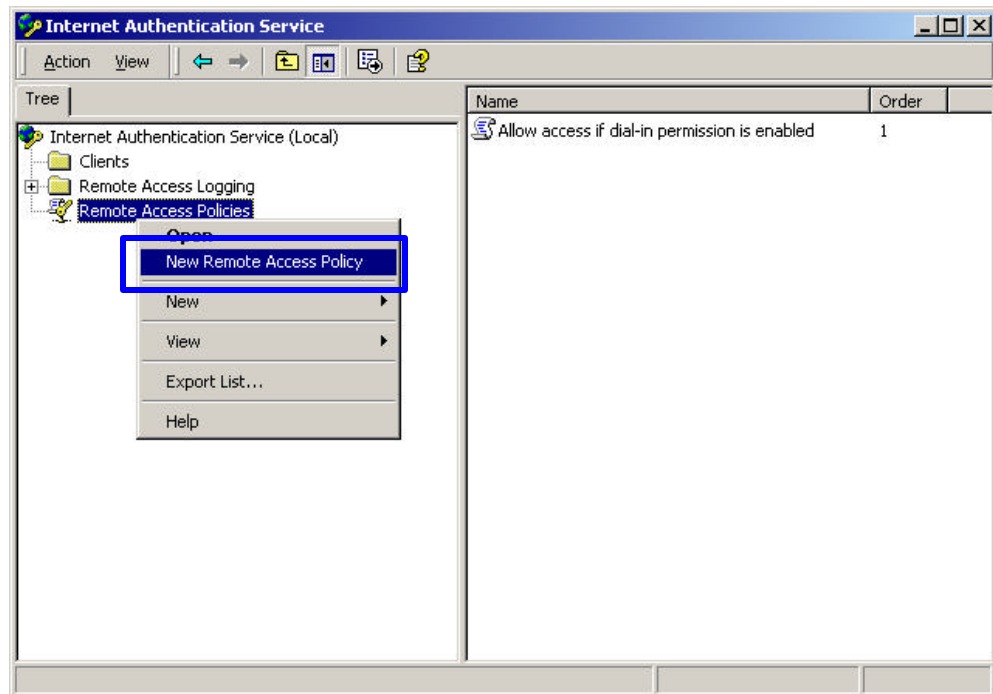
☐ Client must always send the signature attribute in the request

Shared secret: xxxxxx

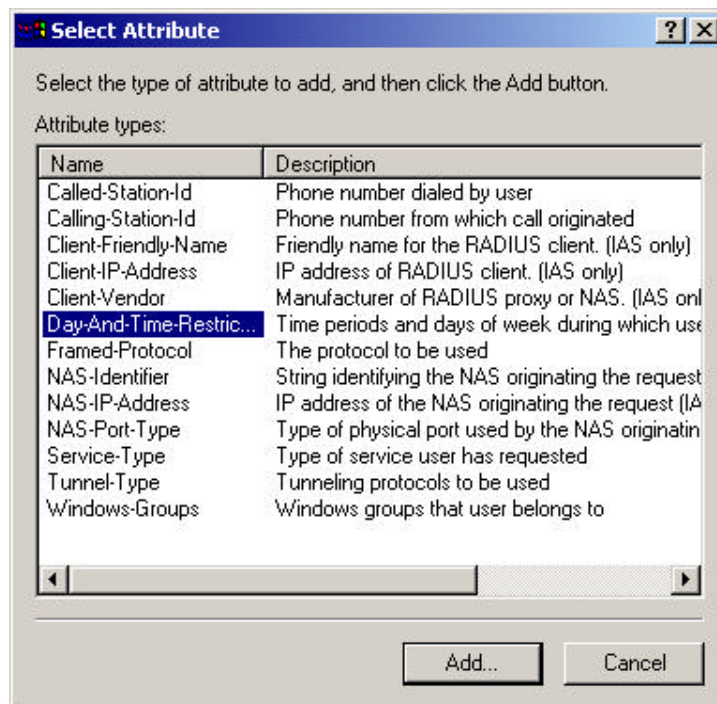
Confirm shared secret: xxxxxx

< Back Finish Cancel

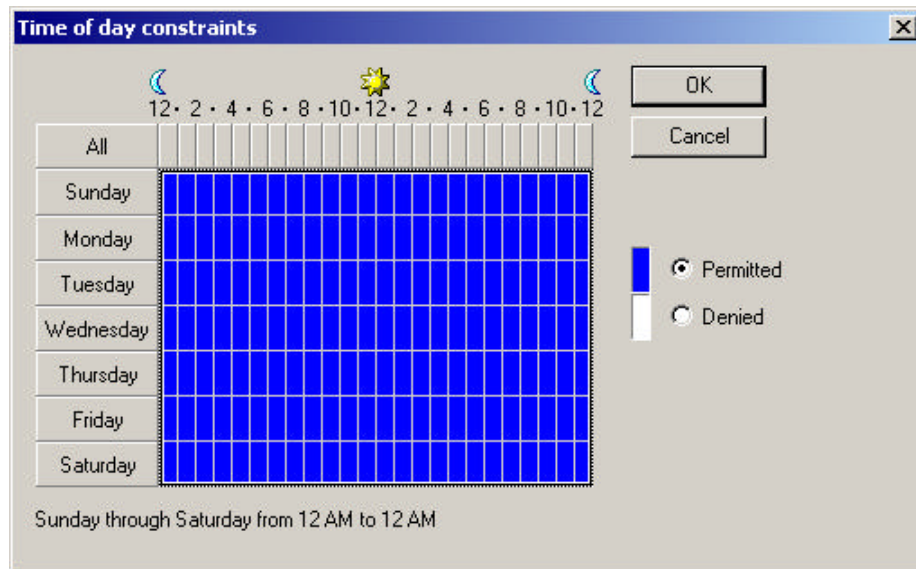
28. In the Internet Authentication Service, right-click "**Remote Access Policies**".
29. Select "New Remote Access Policy".



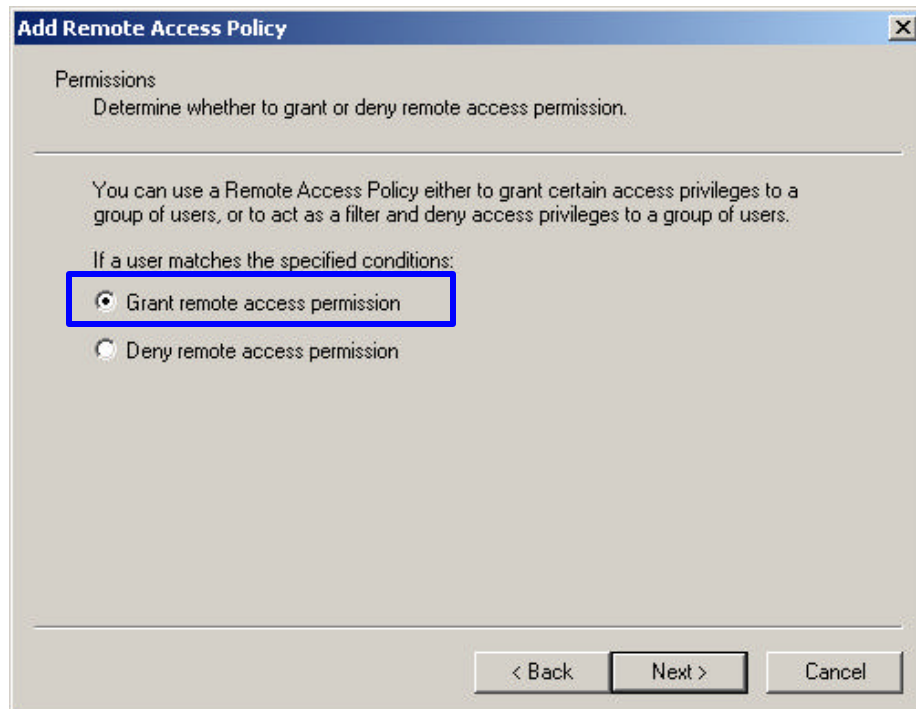
30. Select "**Day-And-Time-Restriction**", and click "**Add**" to continue.



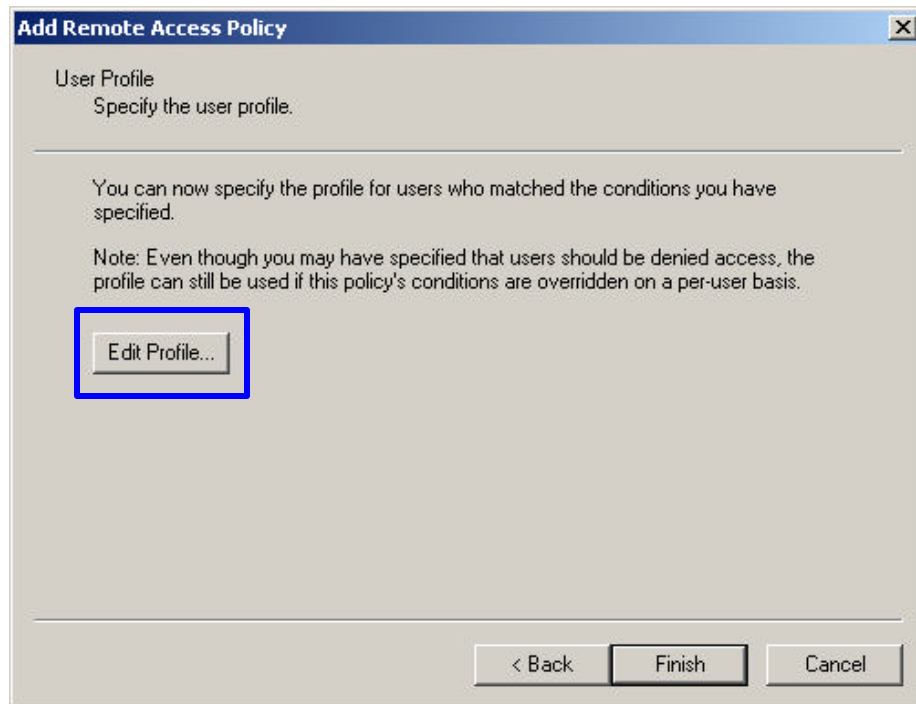
31. Unless you want to specify the active duration for 802.1x authentication, click **OK** to accept to have 802.1x authentication enabled at all times.



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

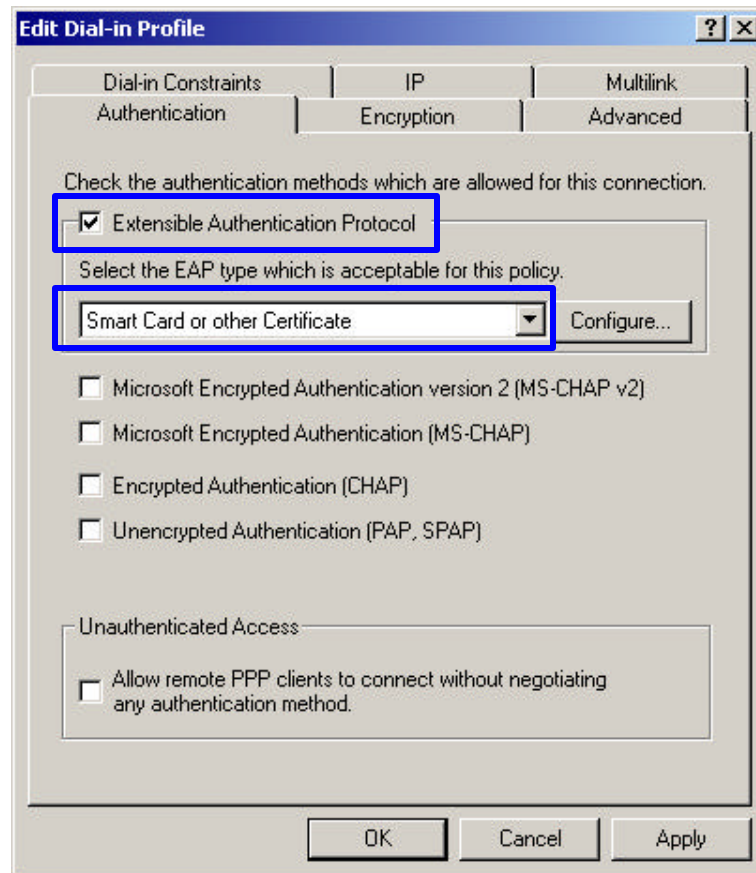


33. Click “Edit Profile” to open up

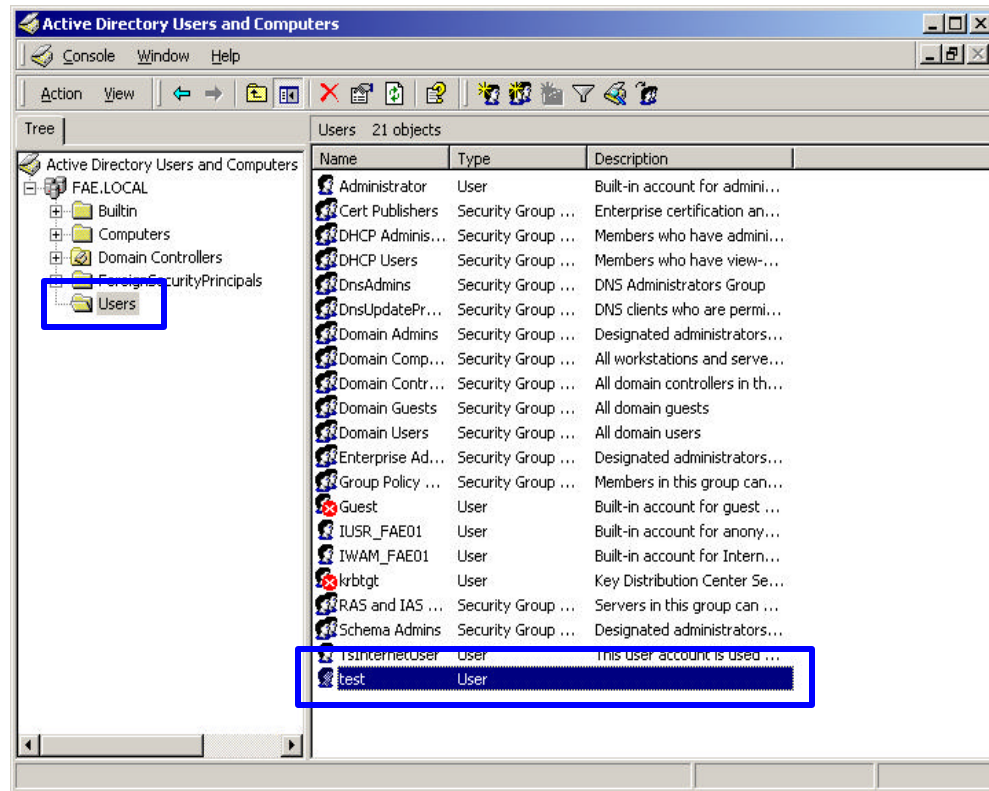


For TLS Authentication Setup (Steps 34 ~ 38)

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



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



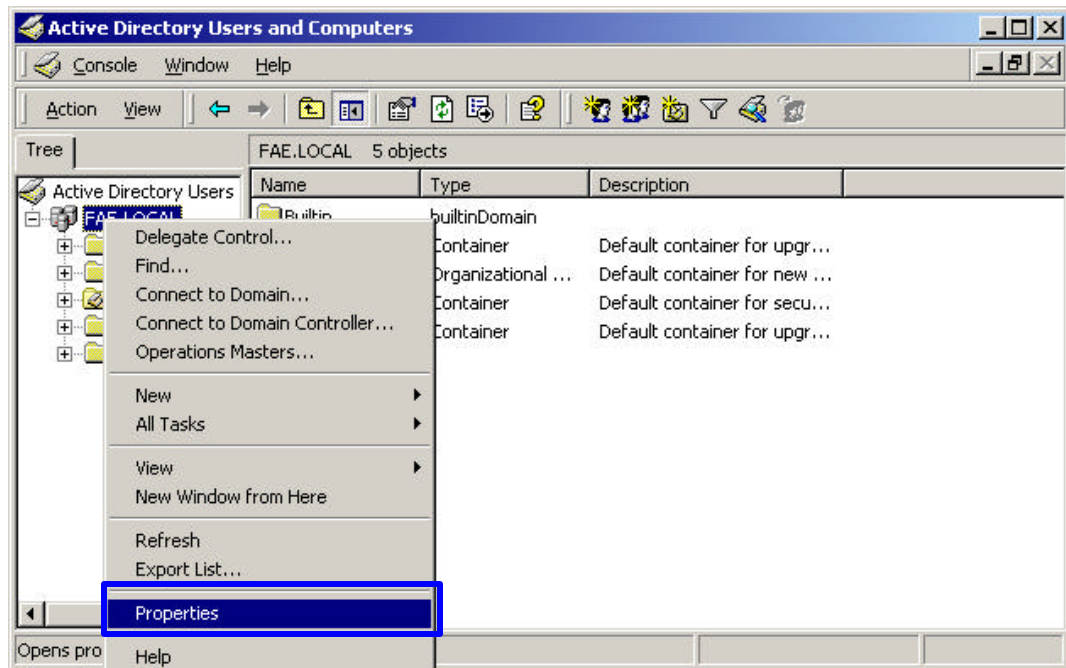
Please note that in this case, we have a user called, **test**, whose account/password are used to obtain the digital certificate from server.

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

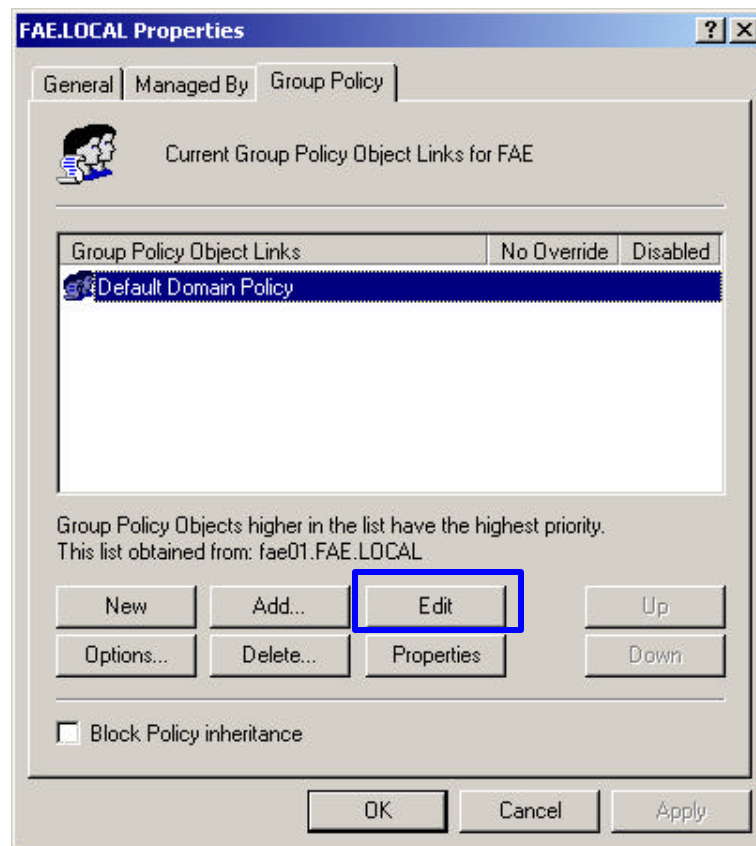
The screenshot shows the 'test Properties' dialog box with the 'Dial-in' tab selected. The 'Remote Access Permission (Dial-in or VPN)' section has three radio buttons: 'Allow access' (selected), 'Deny access', and 'Control access through Remote Access Policy'. A blue arrow points to the 'Allow access' radio button. The 'Callback Options' section has three radio buttons: 'No Callback' (selected), 'Set by Caller (Routing and Remote Access Service only)', and 'Always Callback to:'. A blue arrow points to the 'No Callback' radio button. Below the 'Callback Options' section, there are checkboxes for 'Verify CallerID:', 'Assign a Static IP Address', and 'Apply Static Routes'. The 'Static Routes' button is also visible. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

For MD5 Authentication (Steps 39 ~ 54)

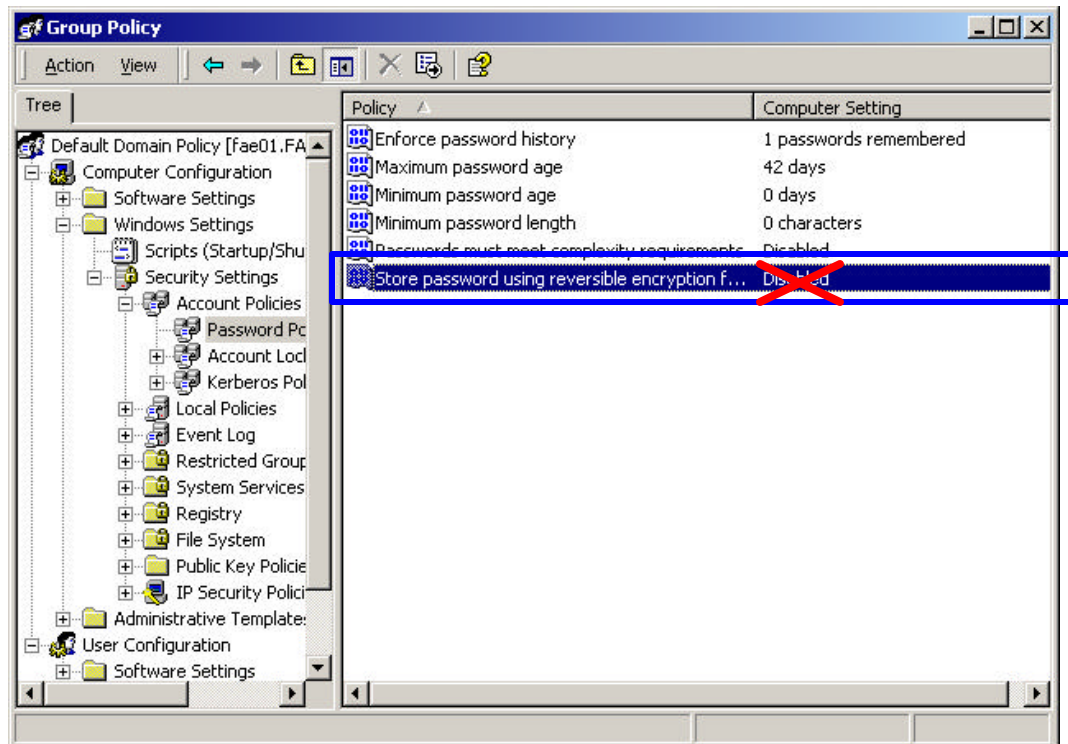
39. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.
40. Right click on the domain, and select "**Properties**"



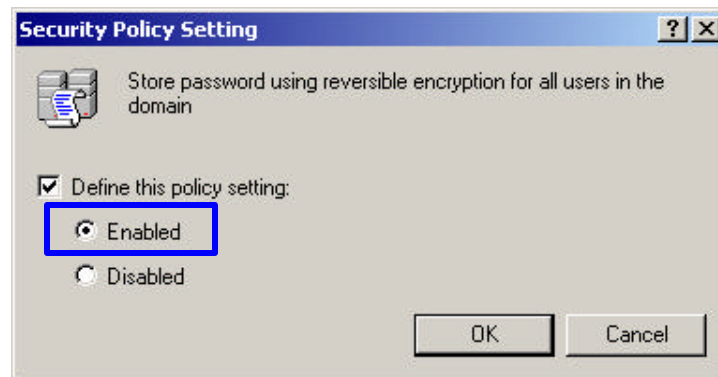
41. Select “**Group Policy**” tab, and click “**Edit**” to edit the Group Policy.



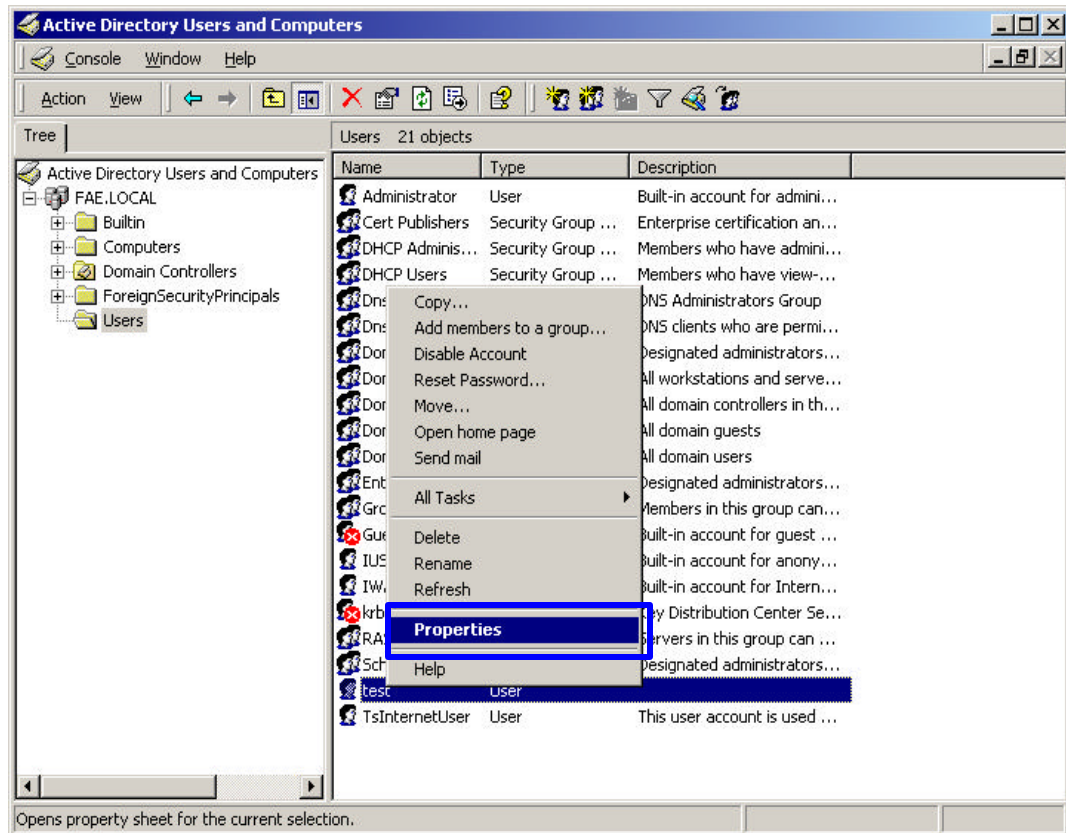
42. Go to “Computer Configuration” > “Windows Settings” > “Security Settings” > “Account Policies” > “**Password Policies**”



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



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



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

The screenshot shows the 'test Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'test' and the domain is '@FAE.LOCAL'. The 'User logon name (pre-Windows 2000)' is 'FAE\test'. The 'Account options' section contains four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Store password using reversible encryption' (checked). The 'Account expires' section has 'Never' selected. The 'OK' button is highlighted.

Member Of	Dial-in	Environment	Sessions
Remote control		Terminal Services Profile	
General	Address	Account	Profile
Telephones		Organization	

User logon name:
test @FAE.LOCAL

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

Logon Hours... Log On To...

☐ Account is locked out

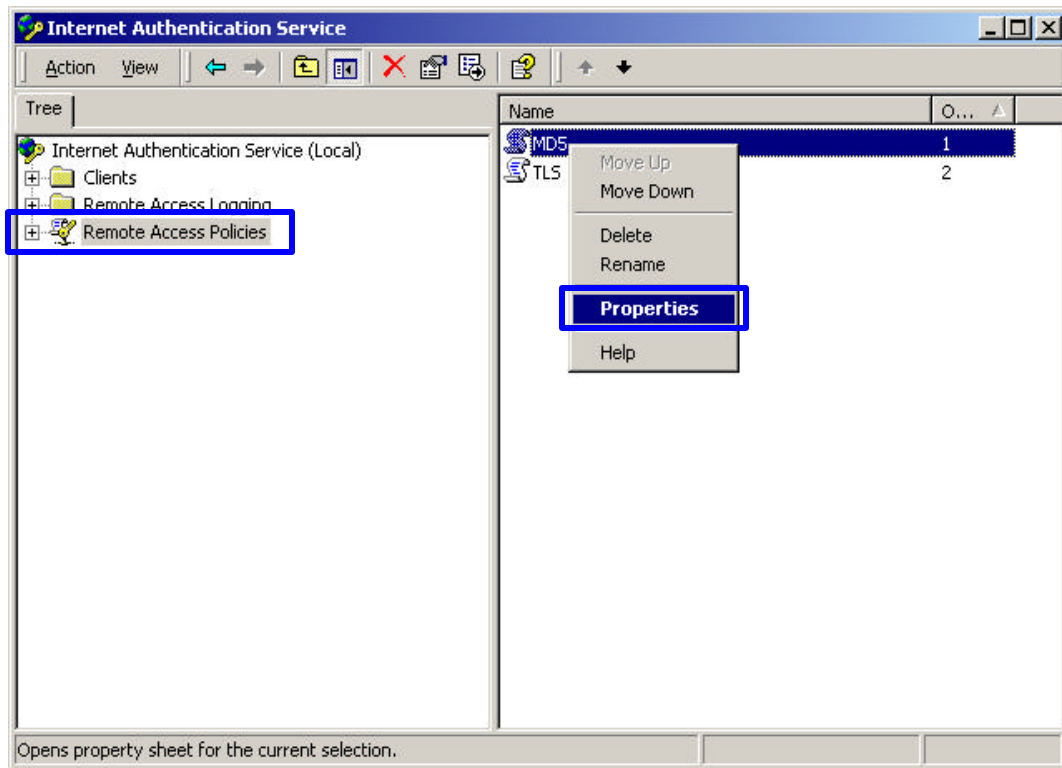
Account options:

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

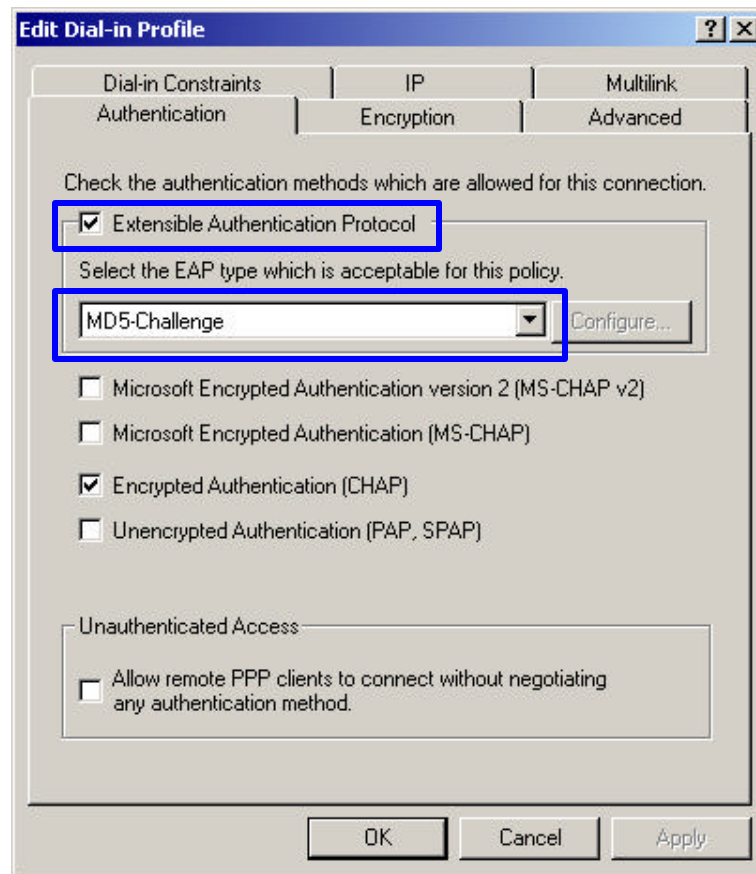
Account expires:
☒ Never
☐ End of: Friday, February 07, 2003

OK Cancel Apply

48. Go to Start > Program > Administrative Tools > **Internet Authentication Service**.
49. Go to **Remote Access Policies**
50. Make sure that **MD5** is moved up to Order 1
51. Right-click "**MD5**", and select "**Properties**"



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



APPENDIX D: GLOSSARY

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

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

AP Client – One of the additional AP operating modes offered by 54mbps 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:

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.

Shared Key : Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key or a member of those who does not.

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

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

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

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

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

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

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

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

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

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

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

DSSS ? Direct Sequence Spread Spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

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

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

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

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

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

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

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

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

IEEE ? The Institute of Electrical and Electronics Engineers, which is the largest technical professional society that promotes the development and application of electro technology 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 54mbps 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**esult **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 54Mbps 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

Item	Specification
Standard	<ul style="list-style-type: none"> Wireless: IEEE 802.11b, 802.11g (draft) Ethernet: IEEE 802.3/u (10/100BaseTX)
Data Rate	<ul style="list-style-type: none"> 802.11g (draft): Up to 54Mbps (6/9/12/18/24/36/48/54) 802.11b: Up to 11Mbps (1/2/5.5/11)
Interface	<ul style="list-style-type: none"> 1 x 100BaseTX with Automatic MDI/MDIX feature Power Jack: 2.5 mm (inner dimension) Default Reset button
Emission Type	<ul style="list-style-type: none"> Direct Sequence Spread Spectrum (DSSS)
Data Modulation	<ul style="list-style-type: none"> BPSK, QPSK, CCK and OFDM (BPSK/QPSK/16-QAM/64-QAM)
RF Frequency	<ul style="list-style-type: none"> 2412 MHz – 2462 MHz (North America) 2412 MHz – 2472 MHz (General Europe) 2412 MHz – 2484 MHz (Japan)
Operating Channel	<ul style="list-style-type: none"> 1 ~ 11 Channels (North America) 1 ~ 13 Channels (Europe) 1 ~ 14 Channels (Japan)
RF Output Power	<ul style="list-style-type: none"> 16 ~ 18 dBm (typical)
Sensitivity for 802.11b	<ul style="list-style-type: none"> 1, 2 Mbps (BPSK, QPSK): -90 dBm 5.5 Mbps (CCK): -86 dBm 11 Mbps (CCK): -82 dBm <p>(Typically @PER < 8% packet size 1024 and @25? ±5?)</p>
Sensitivity for 802.11g (draft)	<ul style="list-style-type: none"> 54 Mbps: -68 dBm 48 Mbps: -68 dBm 36 Mbps: -72 dBm 24 Mbps: -74 dBm 18 Mbps: -82 dBm 12 Mbps: -86 dBm 9 Mbps: -89 dBm 6 bps: -90 dBm <p>(Typically @PER < 8% packet size 1024 and @25? ±5?)</p>

Security	<ul style="list-style-type: none"> ♦ WEP 64/128 ♦ Password Protect ♦ 802.1x security (MD5 and TLS) ♦ Port-Isolation (TBD) ♦ MAC Filtering ♦ SSID Broadcast Disable function ♦ Wi-Fi Protected Access (TBD)
Antenna Type	<ul style="list-style-type: none"> ♦ 1 X 2.4GHz Dipole Antenna ♦ 1 X 2.4GHz Embedded Antenna
Memory	<ul style="list-style-type: none"> ♦ SDRAM: 8 MB (up to 16 MB) ♦ FLASH: 1 MB (up to 4MB)
Dimension	♦ 190 X 149 X 36 mm
Power	♦ Operation max. 1.2 A
Consumption	♦ 600mA \pm 50mA
Power Supply	♦ DC 5 Volt \pm 5% / 2.4A, AC Adapter AC 100V-240V

* Design and specifications are subject to change without notice.