

LevelOne

WNC-0300

54Mbps Wireless PCI Adapter

User's Manual

Version 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	5
Product Features	5
SYSTEM REQUIREMENTS	6
GETTING STARTED	7
GETTING TO KNOW LEVELONE WNC-0300 54MBPS WIRELESS PCI ADAPTER.	7
The LED indicators	7
SETTING UP THE WIRELESS NETWORK	7
Setting Up Ad-Hoc Network	7
Setting Up Infrastructure Network	8
INSTALLING YOUR 54MBPS WIRELESS NETWORK PC CARD	9
Installation and Setup	9
Installation and Setup	
CONFIGURING LEVELONE WNC-0300 WIRELESS PCI ADAPTER.	13
Link Info. Page	13
CONFIGURATION PAGE	14
SECURITY PAGE	16
SITESURVEY PAGE	
About Page	19
APPENDIX A: TROUBLESHOOTING	20
APPENDIX B: NETWORKING BASIS	25
USING THE WINDOWS XP NETWORK SETUP WIZARD	25
CHECKING IP ADDRESS OF YOUR COMPUTER IN WINDOWS XP	
DYNAMIC IP ADDRESS V.S. STATIC IP ADDRESS	
Dynamically Assigned IP Address	
Static IP Address	
WIRELESS NETWORK IN WINDOWS 2000	35
WIRELESS NETWORK IN WINDOWS 98 AND WINDOWS ME	
APPENDIX C: 802.1X AUTHENTICATION SETUP	
802.1x Authentication Infrastructure	
SUPPLICANT: WIRELESS NETWORK PCI ADAPTER	40
TLS Authentication	

APPENDIX E: TECHNICAL SPECIFICATION	79
APPENDIX D: GLOSSARY	74
For MD5 Authentication (Steps 39 ~ 54)	69
For TLS Authentication Setup (Steps 34 ~ 38)	66
RADIUS SERVER: WINDOW2000 SERVER	55
AUTHENTICATOR: WIRELESS NETWORK ACCESS POINT	54
MD5 Authentication	51
TLS Authentication – Download Digital Certificate from Server	45

INTRODUCTION



LevelOne WNC-0300 wireless PCI Adapter

is designed to meet the needs of wireless clients who connect to 2.4GHz standard network products. With the Dual-Standard capability, LevelOne WNC-0300 Wireless PCI Adapter automatically switches to the proper modulation, i.e. OFDM, CCK and etc., supported by one of the two standards, IEEE

802.11b or g(draft), that the corresponding wireless networking device is using. LevelOne WNC-0300 Wireless PCI Adapter offers unbeatable performance of data rates up to 54 Mbps for 802.11g(draft) and 11 Mbps for 802.11b, while maintaining wide range of area coverage. Wireless network security is protected with standard WEP encryption and Wi-Fi Protected Access (WPA), and further enhanced with 802.1x authentication security. With drivers and utility available for most commonly used Windows OS including Windows XP, the setup and installation can be easily managed. LevelOne WPC-0300, 2.4GHz 802.11g/b Wireless Network PCI Adapter, is a truly solid-design networking device that provides you with the ultimate freedom of wireless networking anywhere.

Product Features

- Fully IEEE 802.11g (draft) and 802.11b standards compliant.
- Highly efficient design mechanism to provide unbeatable performance achieving data rate up to 54Mbps for 802.11g (draft) and 11Mps for 802.11b wide range coverage.
- Strong network security with 802.1x available in Windows XP, Wi-Fi Protect Access (WPA), which be available by Q2 '03, and WEP encryption.
- Auto-switch between the two standards, IEEE 802.11b and g (draft) that the corresponding networking device is using.
- Driver/Utility support most commonly used operating systems including Windows 98SE/ME/200/XP.

System Requirements

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

GETTING STARTED

Getting To Know LevelOne WNC-0300 54Mbps Wireless PCI Adapter

The LED indicators

Power LED

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

Setting Up The Wireless Network

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

Setting Up Ad-Hoc Network



The idea of Ad-Hoc Network is rather simple. All the wireless station are set to use the same BSS ID and channel to establish communication linkage with each other to form a point-to-point network for data transmission and reception.



Setting Up Infrastructure Network

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

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

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

Installing Your LevelOne WNC-0300



Installation and Setup

Before insert PCI Adapter into the PCI slot of your computer, please install the Utility Program first.



NOTE:

All the captured images of installation mentioned in this user's manual were based on Windows XP operating system. For installation on other Windows OS, e.g. Windows 98 SE, all the procedures remains the same.

Click on the " Install "		LevelOne 54Mbps WLAN Installation
button on the selection		Install Uninstall User Manual CD Contents
menu.		
	WPC-0300	┝━┥──┝━┥
	WNC-0300	
		Exit



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

54Mbps Wireless LAN Adapter Setup	
Choose Destination Location Select folder where Setup will install files.	NZA.
Setup will install 54Mbps Wireless LAN Adapter in the following folder.	
To install to this folder, click Next. To install to a different folder, click Browse another folder.	e and select
Destination Folder C:\Program Files\54Mbps Wireless LAN Adapter	Browse
nstallShield	Cancel

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

54Mbps Wireless LAN Adapter Setup



NOW.

2

- 1. Turn off your computer, and remove the power cord from your PC.
- 2. Open up the cover of your PC.
- 3. Remove the PCI slot cover from PC case.
- 4. Insert the 54Mbps Wireless Network PCI Adapter into the empty PCI slot.
- 5. Place the computer case back on and plug the power cord.
- 6. Turn on your computer.
- 7. Continue with **Installation setup**.



Installation and Setup

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

Found New Hardware Wizard





Click "Finish" to

installation.

complete new hardware

Hardware Installation



After successful installation, a utility program icon will appear on your desktop screen. To launch the utility, simply double-click the icon.

	i- Link Info	54Mbps Wireless LAN Adapter Configuration Utility		
54Mbps Wireless LON	Configuration	Status Associated BSSID=00-4C-22-33-44-55		
Adapter Configuration	🔒 Advanced	SSID AP334455 Frequency 2437 MHz Wireless Mode Infrastructure		
Utility	<mark>⊪</mark> Site Survey	Encryption WEP Disable Tx Rate 48 Mbns		
	il- About	Channel 6 Rescan		
		Link Quality/Signal Strength Link Quality 100% Signal Strength 100% Data Rate Transmit 0 Kbps 1000 100 10 0 0		
		54Mbps Wireless LAN Adapter Configuration Utility		

Configuring Your LevelOne WNC-0300 Wireless PCI adpapter

Link Info. Page

The default page after you launch the Utility program.

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

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

Frequency: Shows the current frequency used for wireless network.

Wireless Mode: Shows the current wireless mode used for wireless communication.

Encryption: Shows the current encryption mode used for wireless network.

TxRate: Shows the current data rate used for transmitting.

Channel: Shows the current channel for communication.

Link Quality: Shows the link quality of the LevelOne WNC-0300 54Mbps wireless PCI Adapter with the Access Point when operating under Infrastructure mode.

Signal Strength: Shows the wireless signal strength of the connection between the 54Mbps wireless network PCI Adapter with the Access Point.

Data Rate: Shows the statistics of data transfer, and the calculation is based on the number of packets transmitted and received.

Data Rate: Displays the statistics of data transmitted and received.

📴 Link Info	54Mbps Wireless LAN Adapter Configuration Utility				
- Configuration	Status	Associated BSSID=00-4C-22-33-44-55			
- Advanced	Frequency	AP334455 2437 MHz			
	Wireless Mode Encryption	Infrastructure WEP Disable			
III Site Survey	Tx Rate	48	Mbps		
il- About	Channel	6		Rescan	
	Link Quality/Sig	nal Strength —— 100%		Signal Strength	100%
	Data Rate Transmit	C Kbps	10000 1000 100 10 0	Receive	0 Kbps
	54Mbps Wireless LAN Adapter Configuration Utility				

Configuration Page

- Link Info	54Mbps Wireless LAN Adapter Configuration Utility	X
. Configuration	SSID Any	
Advanced	Wireless Mode Infrastructure	
Site Survey	Tx Rate (11B/G) Auto	
i About		
	Power Mode Continuous Access Mode 💌	
	Preamble Short & Long Preamble 💌	
	Apply Cancel	
	54Mbps Wireless LAN Adapter Configuration Utility	

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

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

Wireless Mode: There are two types available for selection

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

AdHoc Band: There are two bands available for selection

- 11B allow user to set the 802.11b standard wireless network.
- 11G allow user to set the 802.11g (draft) standard 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 and 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain.

Tx Rate: Select the data rate for data transmission.

Power Mode: There are 3 modes to choose from

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

Preamble: Select **Long** or **Short** Preamble type. Preamble is a sequence of bits transmitted at 1Mbps that allows the PHY circuitry to reach steady-state demodulation and synchronization of bit clock and frame start. Two different preambles and headers are defined: the mandatory supported Long Preamble and header, which interoperates with the 1 Mbit/s and 2 Mbit/s DSSS specification (as described in IEEE Std 802.11), and an optional Short Preamble and header (as described in IEEE Std 802.11b). At the receiver, the Preamble and header are processed to aid in demodulation and delivery of the PSDU. The Short Preamble and header may be used to minimize overhead and, thus, maximize the network data throughput. However, the Short Preamble is supported only from the IEEE 802.11b (High-Rate) standard and not from the original IEEE 802.11. That means that stations using Short-Preamble cannot communicate with stations implementing the original version of the protocol.

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

i Link Info	54Mbps Wireless LAN Adapter Configuration Utility			
	Status Associated BSSID=00-4C-22-33-44-55			
	SSID AP334455			
Advanced	Frequency 2437 MHz			
	Wireless Mode Infrastructure			
Site Survey	Encryption WEP Disable			
	Tx Rate 48 Mbps			
I- About	Channel 6 Rescan			
	Link Quality/Signal Strength Link Quality 100% Signal Strength 100%			
	Data Rate O Kbps 10000 Receive O Kbps 1000 1000 1000 100)ps		
	54Mbps Wireless LAN Adapter Configuration Utility			

Security Page

This is the page where you configure Security settings of your LevelOne WMC-0300 54Mbps wireless PCI Adapter.

🅞 Link Info	54Mbps Wireless LAN Adapter Configuration Utili	ty 🗙
: Configuration	Encryption Disable	
i. Advanced	Auth. Mode	
II- Site Survey	Default Key Network Key	Key Length
	1	64 bits 🔽
il- About	2	64 bits 🔽
	3	64 bits 💌
	4	64 bits 💌
	Default Key 1	
	Key Format	
	Apply Cancel	
	54Mbps Wireless LAN Adapter Configuration Utili	ty

Encryption: Select Enable or Disable data encryption feature.

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

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

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

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

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

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

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

SiteSurvey Page

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

🖡 Link Info	54Mbps Wireless LAN Adapter Configuration Utility
i Configuration	Available Network
H Advanced	P 00-4C-22-33-44-55 AP334455 No Yes 6 Connect
F Site Survey	
∦ ∙ About	
	Profile Add Remove Properties Connect
	54Mbps Wireless I AN Adapter Configuration Utility

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

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

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

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

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

- Click on "Remove" button to remove the profile, or •
- Click on "**Properties**" button to view and change its settings. The Properties is very similar to that of adding profile.

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

Add New Prof	ile		X
Profile Name			
SSID			
Wireless Mode	Infrastructure		
Channel	7		
Tx Rate	Auto		
Power Mode	Continuous Access Mode 💌		
🗖 Data Encryp	tion		
Auth. Mode	Open Authentication		
Default Key N	etwork Key	Key Lengti	h
		64 bits	\mathbf{v}
0 2		64 bits	\mathbf{v}
6 3		64 bits	\mathbf{v}
• 4		64 bits	-
Key Format	HEX		
	Apply Cancel		

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

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

About Page

This page displays some information about the 54Mpbs PCI Adapter utility, which includes the version numbers for Driver, Firmware and Utility.

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



APPENDIX A: TROUBLESHOOTING

This chapter provides solutions to frequently encountered problems that can occur during the installation and operation of LevelOne WNC-0300 54Mbps Wireless PCI Adapter. Please read through the following to solve your problems.

- 1. The wireless clients cannot access the network in the infrastructure mode.
 - Check that the wireless network device is being installed and working properly.



System Proper	ties		? 🛽
System Re:	store Au	itomatic Updates	Remote
General	Computer Name	Hardware	Advanced
		System: Microsoft Window Professional Version 2002 Registered to: TinGin 55274-337-54938: Computer:	s XP 94-22998
		Intel Celeron proce 701 MHz 112 MB of RAM	nozze
		OK Cancel	Apply

of stellin roper			
System Re	store Auton	atic Updates	Remote
General	Computer Name	Hardware	Advanced
 ×		Add Hardwa	re Wizard
 D 1 11	aar		
Device Mana	iyei		

	Add Hardware Wizard
Device I	4anager
E ⁄	The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.
	Driver Signing Device Manager
Hardwar	e Profiles Hardware profiles provide a way for you to set up and store different hardware configurations.
	Hardware Profiles
	OK Cancel Apply

Right-click on the wireless network adapter.

Select "Properties"

🚚 Device Manager		- 🗆 🛛
File Action View Help		
🕂 🧟 Computer		~
🗈 🙅 Disk drives		
🛨 😼 Display adapters		
🗉 🖾 Human Interface Devices		
🗈 📹 IDE ATA/ATAPI controllers		
IEEE 1394 Bus host controllers		
🕀 🍋 Infrared devices		
🕀 🧽 Keyboards		
Mice and other pointing devices		
H Modems		
		_
Network adapters		=
1394 Net Adapter #5		
Big Direct 202 11b Wireless Network Adv	Indate Driver	
Buy Dealtek DTI 9120 Earris DCI East Ethern	Dicable	
CMCIA adapters	Uninstall	
Sound video and game controllers	Scap for bordware chaptes	
The System devices	Bernardian	
E 🚭 Universal Serial Bus controllers	Properties	~
Opens property sheet for the current selection.		

Check and make sure that the network adapter is working properly

4Mbps I	High Speed Wire	eless Network Adapter Prope 🕐 🔀
General	Advanced Driver	Resources
	54Mbps High Spe	ed Wireless Network Adapter
	Device type:	Network adapters
	Manufacturer:	Unknown
	Location:	PCI bus 1, device 0, function 0
Devic	e status	
This	device is working pr	operly.
lf you start	are having problem the troubleshooter.	is with this device, click Troubleshoot to
		Troubleshoot
Device	usage:	
Use thi	s device (enable)	*
		OK Cancel

2. What is the difference between 54Mbps and 11Mbps wireless products? What's the benefit of 54Mbps Wireless Access Point?

The 54Mbps is made possible by the new modulation method called OFDM, which is different from the current CCK modulation method for 11Mbps. The 54Mbps wireless products also operate in the 2.4GHz ISM band and they are backward compatible with 11Mbps wireless products.

3. What is Roaming?

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

4. What is a MAC Address?

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

5. What is WEP?

Wired Equivalent Privacy (WEP) is a type of data encryption mechanism described in the IEEE 802.11 standard. The 54Mbps Wireless Access Point supports 64/128/256 bit shared key for WEP.

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

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

7. What is ISM band?

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

8. Could I implement the driver/utility installations on another operating system, e.g. Windows 98SE, 2000 and ME? Are there any differences of driver/utility installations among these different operating systems? Yes, you can. All the installation mentioned in this user's manual could be implemented on Windows 98SE/ME/200/XP and there will be no difference.

APPENDIX B: NETWORKING BASIS

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

Using the Windows XP Network Setup Wizard





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

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

Click "**Next**" to continue.

Network Setup Wizard

Select a connection method.
Select the statement that best describes this computer:
O This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer. <u>View an example</u> .
This computer connects to the Internet through another computer on my network or through a residential gateway. <u>View an example</u> .
<u>○</u> <u>□</u> ther
Learn more about home or small office network configurations.
< <u>Back</u> <u>N</u> ext > Cancel

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

Network Setup Wizard			
Give this computer a description and name.			
Computer description:	AREA 51 STATION No. 6 Examples: Family Room Computer or Monica's Computer		
Computer name:	ALIENT Examples: FAMILY or MONICA		
The current computer name is MM.			
Learn more about <u>computer names and descriptions</u> .			
	< Back Next > Cancel		

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

 Name your network.
 Image: Computers on your network

 Name your network by specifying a workgroup name below. All computers on your network should have the same workgroup name.
 AREA51

 Workgroup name:
 AREA51

 Examples: HOME or OFFICE
 Examples: HOME or OFFICE

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

twork Setup Wizard		
Ready to apply network settings	\$	A.S.
The wizard will apply the following setti and cannot be interrupted.	ings. This process may take a few minutes to co	omplete
Settings:		
Internet connection settings.		-
Connecting through another device or	r computer.	=
Network settings:		- 🏼
Computer description:	ABEA 51 STATION No. 6	
Computer name:	ALIENT	
Workgroup name:	AREA51	
		<u> </u>
To apply these settings, click Next.		



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

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

Click "**Next**" to continue.

Network Setup Wizard
You're almost done
You need to run the Network Setup Wizard once on each of the computers on your network. To run the wizard on computers that are not running Windows XP, you can use the Windows XP CD or a Network Setup Disk.
What do you want to do?
Oreate a Network Setup Disk
◯ <u>U</u> se the Network Setup Disk I already have
O Use my Windows XP CD
O Just finish the wizard; I don't need to run the wizard on other computers
< <u>B</u> ack <u>N</u> ext > Cancel

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

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

Network Setup Wizard	
Insert the disk you want to use.	Ø.
Insert a disk the into the following disk drive, and then click Next. 3½ Floppy (A:) If you want to format the disk, click Format Disk. Format Disk	
	Cancel

Copying	×
Please wait while the wizard copies files	D
	Cancel

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.



System will now have to restart in order for the new settings to be effective. Click "**Yes**" to restart the



Checking IP Address of Your Computer in Windows XP

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

Go to Start menu >	Run	? 🛛
Run > type "command"		Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Click " OK "	Open:	
		OK Cancel Browse

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

🔤 Scroll C	:\WINDOWS\System32\cmd.exe	×
Ethernet	adapter Wireless Network Connection 3:	
C D danten	connection-specific DNS Suffix .: Description	A
uapter PD A I SD DD L L	Physical Address. : 00-80-C8-13-AE-1A whop Enabled. : Yes ubcoonfiguration Enabled : Yes P Address. : 192.168.1.2 whoe Mask : : 255.255.255.0 efault Gateway : : 192.168.1.1 MCS Servers : : 192.168.1.1 MS Servers : : : wease Obtained : : : wease Expires : : : WS servers : : : . : : : . : : : . : : : . : : : . : : : . : : : . : : : . : : : . : : : . : : : . : : :	
C:\Docume	nts and Settings\typark>	-

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

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

Go to Start menu >	Run	? 🔀
Run > type "command"	-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Click " OK ″	<u>O</u> pen:	command
		OK Cancel Browse

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

🔤 Scroll	C:\WINDOWS\System32\cmd.exe	×
Ethernet	adapter Wireless Network Connection 3:	-
danton	Connection-specific DNS Suffix .: Description 54Mbps High Speed Wireless Network (A
uapter	Physical Address 00-80-C8-13-AE-1A Dhcp Enabled Yes	
	Autoconfiguration Enabled : Yes IP Address : 192.168.1.3 Subnet Mask : 255.255.255.0	
	Default Gateway : 192.168.1.1 DHCP Server : 192.168.1.1 DNS Servers : 192.168.1.1	
	Lease Obtained Friday, April 04, 2003 11:45:28 PM Lease Expires Saturday, April 05, 2003 11:45:28 PM	1
C:\Docum	nents and Settings\typark>	
		-

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

NOTE:

To renew IP under Windows 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.



Dynamically Assigned IP Address

	Internet Protocol (TCP/IP) Properties
The TCP/IP Properties window appears.	General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for this capability. ID settings assigned automatically if your network administrator for
Select "Obtain an IP address	the appropriate in settings.
automatically " if you are on a — DHCP enabled network.	Obtain an IP address automatically O use the following IP address: IP address:
Click " OK " to close the window with the changes made	Subnet mask: Default gateway:
	Uptain DNS server address automatically
	Preferred DNS server:
	Advanced
	UK Lancel

Static IP Address

Select " Use the following IP	Internet Protocol (TCP/IP) Properties	×
address″	General	
Enter the IP address and	You can get IP settings assigned automatically if your network supports	
subnet mask fields.	the appropriate IP settings.	
	O Obtain an IF address automatically	
Enter the IP address of the	Use the following IP address:	
Router in the Default gateway	IP address: 192.168.1.2	
field.	Subnet mask: [255 . 255 . 0]	
	Default gateway:	
Enter the IP address of the	Obtain DNS server address automatically	
Router in the DNS server field	Use the following DNS server addresses:	
	Preferred DNS server:	
	Alternate DNS server:	
	Advanced	
	OK Cancel	

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"

ocal Area Connection	5 Properties		<u>?</u> ×
General Sharing			
Connect using:			
🗒 54Mbps High	Speed Wire	less Networ	k Adapter
			<u>C</u> onfigure
Components checked	are used by thi	s connection:	
Internet Proto	col (TCP/IP)		
Description Transmission Contra wide area network across diverse inter	ol Protocol/Inter protocol that pro connected netw	met Protocol. " ovides commu vorks. ected	The default nication
	Jai when conne		1 - Carrol
		UK	Lancel

appears.

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

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

Internet Protocol (TCP/IP) Prope General	rties ? ×
You can get IP settings assigned at this capability. Otherwise, you need the appropriate IP settings.	utomatically if your network supports to ask your network administrator for
Obtain an IP address automat	ically
O Use the rollowing iP address:	
[P address:	· · · · · ·
S <u>u</u> bnet mask:	
Default gateway:	
Obtain DNS server address ar	utomatically
 C_ Us <u>e</u> the following DNS server	addresses:
Preferred DNS server:	
<u>A</u> lternate DNS server:	· · ·
	Ad <u>v</u> anced
	OK Cancel

Select "Use the following IP address" Enter the IP address and subnet mask fields.	Internet Protocol (TCP/IP) Properties ? × General . You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Enter the IP address of the Router in the Default gateway field.	Obtain an IP address automatically IP address: IP address: Subnet mask: Default gateway:
Enter the IP address of the Router in the DNS server field	Obtain DNS server address automatically Obtain DNS server addresses. Preferred DNS server: Alternate DNS server: Alternate DNS server: Advanced
	OK Cancel

Wireless Network In Windows 98 and Windows ME

Go to Start menu > Settings >	Network ? ×
Control Panel > Double-click	Configuration Identification Access Control
on Network	The following network components are installed:
Select TCP/IP of the network device	Client for Microsoft Networks S4M WLAN Adapter S4M WLAN PCI Adapter Intel(B) PB0/100 S Desktop Adapter
Click " Properties " to continue	TCP/IP -> 54M WLAN Adapter
	Add Remove Properties Primary Network Logon: Windows Logon Image: Comparison of the line line of the line of the line of the line of the line
The TCP/IP Properties window appears.

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

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

TCP/IP Properties	? ×
Bindings Advanced MetBIU DNS Configuration Gateway WINS Configuration IP A	5 Address
An IP address can be automatically assigned to this compu If your network does not automatically assign IP addresses, your network administrator for an address, and then type it i the space below.	ıter. , ask in
Obtain an IP address automatically	
C Specify an IP address:	
[P Address:	
Sybnet Mask:	
Detect connection to network media	
ОК Са	ancel





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: LevelOne WNC-0300 54Mbps Wireless PCI Adapter

Here is the setup for LevelOne WNC-0300 Wireless PCI Adapter 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 LevelOne WNC-0300 54Mbps wireless PCI Adapter.

- 1. Go to Start > Control Panel
- 2. Double-click on "Network Connections"
- Right-click on the Wireless Network Connection that you use with LevelOne WNC-0300 54Mbps wireless network PCI Adapter.
- 4. Click "**Properties**" to open up the Properties setting window.

🕆 Wireless Netwo	ork Connection 3 St	atus 🛛 ? 🔀
General Support		
Connection		
Status:		Connected
Duration:		00:37:11
Speed:		54.0 Mbps
Signal Strength:		T
Activity	Sent — 🗐 –	- Received
Packets:	21,840	21,356
Properties	Disable	
		Close

5. Click on the "Wireless Network" tab.

🕹 Wirel	ess Network Con	nection Prop	erties	?×
General	Wireless Networks	Authentication	Advanced	
Connec	t using:			
BP	54Mbps High Spee	d Network Adap	oter	
This co	nnection uses the foll	owing items:	Configure	e
	Client for Microsoft f File and Printer Sha QoS Packet Sched Internet Protocol (T	Networks ring for Microsoft uler CP/IP)	Networks	
- Desci Allow netw	ristail ription vs your computer to av vork.	ccess resources (on a Microsoft	<u>s</u>
🗹 Sho	w icon in notification	area when conne	ected	
		0	к с	ancel

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

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

🕹 Wireless Network Connection Properties 🛛 🔹 💽
General Wireless Networks Authentication Advanced
✓ Use Windows to configure my wireless network settings
Available networks:
To connect to an available network, click Configure.
P APFFFC04 Configure
LUSR2249-Linksys
A FAE Refresh
Preferred networks: Automatically connect to available networks in the order listed below:
APFFFC04 Move up
Move down
Add Remove Properties
Learn about <u>setting up wireless network</u> <u>configuration.</u> Advanced
OK Cancel

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

TLS Authentication

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

Wireless Network Prop	erties 🛛 💽 🔀	
Network name (SSID):	APFFFC04	
Wireless network key (WE	P)	
This network requires a ke	y for the following:	
Data encryption (WEP enabled)		
Network Authenticat	ion (Shared mode)	
Network key:		
Key format:	ASCII characters	
Key length:	104 bits (13 characters) 💟	
Key index (advanced):	0	
The key is provided for me automatically		
This is a computer-to-computer (ad hoc) network; wireless access points are not used		
(OK Cancel	

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.

🕹 Wireless Network Connection Properties 👘 🛛 🔀
General Wireless Networks Authentication Advanced
Select this option to provide authenticated network access for wired and wireless Ethernet networks.
✓ Enable network access control using IEEE 802.1×
EAP type: Smart Card or other Certificate MD5-Challenge Smart Card or other Certificate
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK Cancel

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.

Connect to 192.1	58.1.10
	GA
Connecting to 192.16	8.1.10
User name:	😰 📃 🔽
<u>P</u> assword:	
	Remember my password
	OK Cancel

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

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

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

http://192.168.1.10/certsrv

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

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

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🚱 Back 🔹 🕥 🔹 📓 🏠 🔎 Search 🤺 Favorites 🜒 Media 🚱 🔗 - چ 🚍	
Addres: 🕘 http://192.168.1.10/certsrv/	🔽 🄁 Go 🛛 Links 🂙
Microsoft Certificate Services WirelessCA	<u>Home</u>
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure Once you acquire a certificate, you will be able to securely identify yourself to other people over your e-mail messages, encrypt your e-mail messages, and more depending upon the type of correquest.	e program. r the web, sign ertificate you
Select a task:	
	Next >
	~
😂 Done	Internet

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

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	A.
🚱 Back 🔹 🐑 - 💌 🛃 🏠 🔎 Search 📌 Favorites 🚳 Media 🚱 🔗 🍓 🚍	
Address 🕘 http://192.168.1.10/certsrv/certrqus.asp	🔽 🄁 Go 🛛 Links 🎽
Microsoft Certificate Services WirelessCA	Home
Choose Request Type	
Please select the type of request you would like to make: User certificate request: User Certificate Advanced request	
	Next >
E Done	Internet

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

Microsoft Certificate Services - Microsoft Internet Explorer	- 7 🗙
File Edit View Favorites Tools Help	
🚱 Back 🝷 🕥 🗧 🔀 😭 🔎 Search 📌 Favorites 🜒 Media 🤣 😥 🍓 🚍	
Address 🙆 http://192.168.1.10/certsrv/certrqbi.asp?type=0	💙 芛 Go 🛛 Links 🌺
<i>Microsoft</i> Certificate Services WirelessCA	<u>Home</u>
All the necessary identifying information has already been collected. You may now submit	your request.
More Options >>	
	Submit >
	~
Done	🥝 Internet

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

Microsoft Certificate Services - Microsoft Internet Explorer	_ 7 🗙
File Edit View Favorites Tools Help	
🕞 Back 🔹 🐑 🔹 🛃 🏠 🔎 Search 🤺 Favorites 🔮 Media 🤣 😥 - چ 🚍	
Address 🙆 http://192.168.1.10/certsrv/certrqbi.asp?type=0 🕑 🔁 🖸	50 Links »
<i>Microsoft</i> Certificate Services WirelessCA	Home 🛆
User Certificate - Identifying Information	
All the necessary identifying information has already been collected. You may now submit your request.	
More Options >>	
Waiting for server response	
🙆 Waiting for server response 🖤 Internet	<u>~</u>

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

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	A.
🚱 Back 🔹 🕥 - 💌 🛃 🏠 🔎 Search 👷 Favorites 🔇 Media 🚱 🔗 - 头 🥽	
Address 🗃 http://192.168.1.10/certsrv/certfnsh.asp	🔽 🄁 Go 🛛 Links 🎽
Microsoft Certificate Services WirelessCA	<u>Home</u>
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
Done	🔮 Internet

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

Root Cer	rtificate Store 🔀
1	Do you want to ADD the following certificate to the Root Store? Subject : WirelessCA, TW Issuer : Self Issued Time Validity : Monday, January 06, 2003 through Thursday, January 06, 2005 Serial Number : 132713D1 4F4837B3 41E04CF7 2497D9FA Thumbprint (sha1) : 244FCB3C 2D9F2F21 4DC262F9 2008DEFA B490D10E Thumbprint (md5) : 1EBA1EC0 2036AD70 6E5121A6 A136E4AC Yes No

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.

Connect Wireless Network Connection 🛛 🔹 🔀		
User name on certific chance@FAE.local	ate:	~
Friendly name:		
Issuer:	WirelessCA	
Expiration date:	1/6/2004 4:02:09 PM	
	OK Can	icel

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

Validate	Server Certificate	
⚠	The Root Certification Authority for the server's certificate is Do you want to accept this connection?	WirelessCA
	OK Cancel	

MD5 Authentication

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

Wireless Network Properties 🛛 🛛 🛛			
Network name (SSID):	APFFFC04		
Wireless network key (WEP) This network requires a key for the following:			
Data encryption (WEP enabled)			
Network Authenticat	ion (Shared mode)		
Network key:	******		
Key format:	ASCII characters 🔽		
Key length:	40 bits (5 characters) 🛛 🗸		
Key index (advanced):	0		
The key is provided for me automatically			
This is a computer-to-computer (ad hoc) network; wireless access points are not used			
OK Cancel			

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

- 30. Click "**OK**" to close the Wireless Network Properties window, thus make the changes effective.
- 31. Select "Authentication" tab.
- 32. Select **"Enable network access control using IEEE 802.1X**" to enable 802.1x authentication.
- 33. Select "**MD-5 Challenge**" from the drop-down list box for EAP type.

🕹 Wireless Network Connection Properties 💫 🛛 🔀			
General Wireless Networks Authentication Advanced			
Select this option to provide authenticated network access for wired and wireless Ethernet networks.			
☑ Enable network access control using IEEE 802.1×			
EAP type: MD5-Challenge MD5-Challenge Smart Card or other Certificate Properties			
Authenticate as computer when computer information is available Authenticate as quest when user or computer information is			
unavailable			
OK Cancel			

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.

Wireless Netwo	ork Connection	1	? 🗙
		P	2
User name:			
Password:			
Logon domain:			
(ОК	Cancel	

Authenticator: Wireless Network Access Point

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

	22 Mbps wizard Status	5 >> Basic Setting IP	Setting Advanced Setting Security units in Tools
	802.1×	• Enabled	
802.1x g		C Disabled	
	Encryption Key	Length 💿 64 bits	C 128 bits C 256bits
		Lifetime 30 Minute	25 💌
	RADIUS Server 1	IP	
		Port	1812
		Shared Secret	
	RADIUS Server 2 (optional)	IP	0.0.0
		Port	0
		Shared Secret	
		Apply Cance	I 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.
- 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 "Apply" button for the 802.1x settings to take effect after Access Point reboots itself.

NOTE:

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

Radius Server: Window2000 Server

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

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

Windows Components Wizard	×
Windows Components You can add or remove components of Windows 2000.	
To add or remove a component, click the checkbox. A shaded part of the component will be installed. To see what's included i Details.	box means that only n a component, click
Lomponents:	
🗹 📻 Accessories and Utilities	12.1 MB
🗹 😫 Certificate Services	1.4 MB
🗹 🗩 Indexing Service	0.0 MB
Internet Information Services (IIS)	21.7 MB
Management and Monitoring Tools	52MB 🗾
Description: Installs a certification authority (CA) to issue certific public key security applications.	ates for use with
Total disk space required: 2.1 MB	Details
Space available on disk: 3524.4 MB	
< Back	Next > Cancel

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

Windows Components Wizard	×
Certification Authority Type There are four types of certification authoritie	s.
Certification Authority types: Centerprise root CA Centerprise subordinate CA Centerprise subordinate CA Centerprise subordinate CA	Description: The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.
Advanced options	(Beels David Devel
	< Back Next > Cancel

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

Windows Components Wizard			
CA Identifying Information Enter information to identify	this CA		
CA name:	WirelessCA		
Organization:			
Organizational unit:			
City:			
State or province:	Country/region: US		
E-mail:			
CA description:			
Valid for:	2 Years Expires: 1/8/2005 12:15 PM		
	< Back Next > 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.

👯 Select Certificate Temp	ate <mark>?</mark> X
Select a certificate template t	issue certificates
🔯 User Signature Only	Secure Email, Clier
Smarteard User	Secure Email, Clier
🙀 Authenticated Session	Client Authenticatic
🗱 Smartcard Logon	Client Authenticatic
Code Signing	Code Signing
🗱 Trust List Signing	Microsoft Trust List
Enrollment Agent	Certificate Benuest
	OK Cancel

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"
 - gf Group Policy - 🗆 🗵 Action View 🛛 🗢 🔿 🗈 🔃 😢 Tree Automatic Certificate Request Default Domain Policy [fae01.FAE.LOCAL] Policy Computer Computer Settings
 Software Settings
 Original Settings Scripts (Start down) 🦉 Security Settings Account Policies
 Coal Policies
 Event Log
 Restricted Groups 🗄 📴 System Services 🗄 📴 Registry 词 File Syste ÷ 🚊 🧰 Public Key Policies Automatic Certificate Request Setting Encrypted Date Automatic Certificate Reque 🚞 Enterprise Trust View 🗄 🥷 IP Security Policies on Active Directory Administrative Templates Refresh User Configuration Export List... 🗄 📄 Software Settings Help 🗄 🛅 Windows Settings Create a new Automatic Certificate Request object and add it to the Security Configuration Editor.
- 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.

Automatic Certificate Request Setup Wizar	d 🔀		
Certificate Template The next time a computer logs on, a certific provided.	cate based on the template you select is		
A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list. Certificate templates:			
Name	Intended Purposes		
Computer Domain Controller Enrollment Agent (Computer) IPSEC	Client Authentication, Server Authenticatior Client Authentication, Server Authenticatior Certificate Request Agent 1.3.6.1.5.5.8.2.2		
•			
	< Back Next > Cancel		

- 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.

Networking Services	×		
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.			
Subcomponents of Networking Services:			
UM Internet Services Proxy	U.U MB		
🗹 🛃 Domain Name System (DNS)	1.1 MB		
Image: Provide the state of	0.0 MB		
🗹 💂 Internet Authentication Service	0.0 MB		
🔲 🗔 📇 QoS Admission Control Service	0.0 MB 🛄		
Simple TCP/IP Services	0.0 MB		
🗆 📃 Site Server ILS Services	1.5 MB 💌		
Description: Enables authentication, authorization and accounting of di users. IAS supports the RADIUS protocol.	al-up and VPN		
Total disk space required: 0.4 MB	Details		
Space available on disk: 8462.6 MB			
ОК	Cancel		

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.

Client address (IP or DNS):				
192.168.1.1				Verify
Client-Vendor:				
RADIUS Standard				▼
🔲 Client must always send	the signature a	attribute in the r	equest	
Shared secret:	****			
Confirm shared secret:	****			

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



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

t	Select Attribute	<u>? ×</u>
	Select the type of attribute Attribute types:	e to add, and then click the Add button.
	Name	Description
	Called-Station-Id Calling-Station-Id Client-Friendly-Name Client-IP-Address Client-Vendor Day-And-Time-Restric Framed-Protocol NAS-Identifier NAS-IP-Address NAS-Port-Type Service-Type Tunnel-Type Windows-Groups	Phone number dialed by user Phone number from which call originated Friendly name for the RADIUS client. (IAS only) IP address of RADIUS client. (IAS only) Manufacturer of RADIUS proxy or NAS. (IAS onl Time periods and days of week during which use The protocol to be used String identifying the NAS originating the request IP address of the NAS originating the request Type of physical port used by the NAS originatin Type of service user has requested Tunneling protocols to be used Windows groups that user belongs to
	•	•
		Add Cancel

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.

Add Remote Access Policy	×
Permissions Determine whether to grant or deny remote access permission.	
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.	
If a user matches the specified conditions:	
 Grant remote access permission 	
C Deny remote access permission	
< Back Next > Cancel	

33. Click "Edit Profile" to open up

i Re	emote Access Policy
USE	er Pronie Specify the user profile.
	You can now specify the profile for users who matched the conditions you have specified.
	Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.
	Edit Profile
L	
	< Back Finish Cancel

For TLS Authentication Setup (Steps 34 ~ 38)

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

Edit Dial-in Profile	<u>? ×</u>
Dial-in Constraints IP Authentication Encryption	Multilink Advanced
Check the authentication methods which are allowe Extensible Authentication Protocol Select the EAP type which is acceptable for this protocol Smart Card or other Certificate	d for this connection. olicy.
 Microsoft Encrypted Authentication version 2 (I Microsoft Encrypted Authentication (MS-CHAP Encrypted Authentication (CHAP) Unencrypted Authentication (PAP, SPAP) 	MS-CHAP v2))
Unauthenticated Access Allow remote PPP clients to connect without ne any authentication method.	egotiating
OK Ca	ncel Apply

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

🐇 Active Directory Users and Computers				
] 🥪 <u>C</u> onsole <u>W</u> indow <u>H</u> elp	Console Window Help			_ _ _ _ _
	🗙 😭 😫 😫	╳ ฮ 🖸 😫 🦉 🖉 🕍 ▽ 🍕 🍘		
Tree	Users 21 objects			
Active Directory Users and Computers	Name	Туре	Description	
🗄 🗊 FAE.LOCAL	🕵 Administrator	User	Built-in account for admini	
🗄 💼 Builtin	🕵 Cert Publishers	Security Group	Enterprise certification an	
🗄 🖷 Computers	🕵 DHCP Adminis	Security Group	Members who have admini	
🗄 🥝 Domain Controllers	🕵 DHCP Users	Security Group	Members who have view	
🚊 🚍 ForeignSecurityPrincipals	🕵 DnsAdmins	Security Group	DNS Administrators Group	
Inters	🕵 DnsUpdatePr	Security Group	DNS clients who are permi	
	🕵 Domain Admins	Security Group	Designated administrators	
	🕵 Domain Comp	Security Group	All workstations and serve	
	🕵 Domain Contr	Security Group	All domain controllers in th	
	🕵 Domain Guests	Security Group	All domain guests	
	🕵 Domain Users	Security Group	All domain users	
	🕵 Enterprise Ad	Security Group	Designated administrators	
	🕵 Group Policy	Security Group	Members in this group can	
	5 Guest	User	Built-in account for guest	
	🕵 IUSR_FAE01	User	Built-in account for anony	
	🕵 IWAM_FAE01	User	Built-in account for Intern	
	si 🔊 🔊	User	Key Distribution Center Se	
	🕵 RAS and IAS	Security Group	Servers in this group can	
	🕵 Schema Admins	Security Group	Designated administrators	
l r	🛃 IsinternetUser	User	This user account is used	
	🕵 test	User		
L 7				_
	ļ			

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

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

test Properties
Remote control Terminal Services Profile General Address Account Profile Telephones Organization Member Of Dial-in Environment Sessions Remote Access Permission (Dial-in or VPN) Allow access Deny access Control access through Remote Access Policy Terminal Services Profile Organization Organization Organization Environment Sessions Sessions Control access through Remote Access Policy
 Verify Caller-ID: Callback Options No Callback Set by Caller (Routing and Remote Access Service only) C Always Callback to:
Assign a Static IP Address Apply Static Routes Define routes to enable for this Dial-in connection. Static Routes
OK Cancel Apply

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**"

of Group Policy		
📙 Action View 🗍 🗢 🔿 🗈	• × 🛱 😫	
Tree	Policy A	Computer Setting
Default Domain Policy [fae01.FA	Enforce password history	1 passwords remembered
🗐 💂 Computer Configuration	🔀 Maximum password age	42 days
🗄 📄 Software Settings	🐯 Minimum password age	0 days
🖃 📄 Windows Settings	🕮 Minimum password length	0 characters
🔚 Scripts (Startup/Shu	Decemente must meet complexity requiremente	Disabled
🖃 🔂 Security Settings	Store password using reversible encryption f	Distred
📄 🛃 Account Policies 👇		
- 🛃 Password Pc		
🗈 🛃 Account Loci		
庄 🛃 Kerberos Pol		
🗄 🕂 🛃 Local Policies		
🗄 🛃 Event Log		
🗄 📴 Restricted Group		
🗄 🧾 System Services		
🗄 📴 Registry		
🗄 📴 File System		
🗄 🚞 Public Key Policie		
🗄 🛃 IP Security Polici 🚟		
🗄 📄 Administrative Template:		
🖻 🐗 User Configuration		
📄 💼 Software Settings 📃		
	<u> </u>	

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

Security	Policy Setting	1
F	Store password using reversible encryption for all users in the domain	
I Defir I O E O E	ne this policy setting: Enabled Disabled	
	OK Cancel	

- 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**"

🐗 Active Directory Users and Compu	ters			- D ×
] 🧔 <u>C</u> onsole <u>W</u> indow <u>H</u> elp				
] Action ⊻iew] 🗢 → 🔁 💽	🗙 😭 🗗 🗟	< 🖆 🖻 🗟 🛛 🦉 🖉 🏙 🗸 🍕 🍺		
Tree	Users 21 objects			
Active Directory Users and Computers	Name	Туре	Description	
E FAE.LOCAL	Administrator	User	Built-in account for admini	
	Cert Publishers	Security Group	Enterprise certification an	
Computers	DHCP Adminis	. Security Group	Members who have admini	
Domain Controllers	CONTRACT USERS	Security Group	Members who have view	
	Copy		PNS Administrators Group	
	Add men	nbers to a group	PNS clients who are permi	
	Disable A	Account	M workstations and sorve	
	Reset Pa	issword	All domain controllers in th	
	Dor Open he		All domain quests	
	Dor Send ma	ilie page il	All domain users	
	C Ent		Designated administrators	
	Grc All Tasks	: 1	Vembers in this group can	
	💑 Gut Delete		Built-in account for guest	
	🖸 IUS Rename		Built-in account for anony	
	🖸 IW. Refresh		Built-in account for Intern	
	Szakrt 📃 📃		y Distribution Center Se	
	RA Propert	ties	ervers in this group can	
	Sci Help		pesignated administrators	
	🖉 test	User		
	😴 TsInternetUser	User	This user account is used	
Opens property sheet for the current select	ion.			

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

test Properties 🥂 🔀
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 Image: Constraint of the second
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 list.

Edit Dial-in Profile			
Dial-in Constraints IP Multilink Authentication Encryption Advanced			
Check the authentication methods which are allowed for this connection. Extensible Authentication Protocol Select the EAP type which is acceptable for this policy.			
MD5-Challenge Configure			
 Microsoft Encrypted Authentication version 2 (MS-CHAP v2) Microsoft Encrypted Authentication (MS-CHAP) Encrypted Authentication (CHAP) Unencrypted Authentication (PAP, SPAP) 			
Unauthenticated Access Allow remote PPP clients to connect without negotiating any authentication method.			
OK Cancel Apply			

APPENDIX D: GLOSSARY

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

 $\mbox{Ad-Hoc}$ — 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.

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

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

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

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

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

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

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

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

 $\mathbf{Browser}$ — An application program that enables one to read the content and interact in the World Wide Web or Intranet.

 \mathbf{BSS} — BSS stands for "Basic Service Set". It is an Access Point and all the LAN PCs that associated with it.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Multiple Bridge – One of the additional AP operating modes offered by 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 - Request To Send. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

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

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

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

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

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

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

Wireless Bridge – One of the additional AP operating modes offered by 54mpbs Access Point, which allows a pair of APs to act as the bridge that connects two Ethernet networks or Ethernet enabled clients together.

APPENDIX E: TECHNICAL SPECIFICATION

Item	Specification
Standards	Wireless: IEEE 802.11b, 802.11g (draft), PCI Standard
	v2.2
Data Rate	• 802.11g (draft): Up to 54Mbps (6/9/12/18/24/36/48/54)
	 802.11b: Up to 11Mbps (1/2/5.5/11)
Emission Type	Direct Sequence Spread Spectrum (DSSS)
Data	 BPSK, QPSK, CCK and OFDM (BPSK/QPSK/16-QAM
Modulation	/64-QAM)
RF Frequency	 2412 MHz – 2462 MHz (North America)
	 2412 MHz – 2472 MHz (General Europe)
	 2412 MHz – 2484 MHz (Japan)
Operating	 1 ~ 11 Channels (North America)
Channel	 1 ~ 13 Channels (Europe)
	 1 ~ 14 Channels (Japan)
RF Output	 16 ~ 18 dbm (typical)
Power	
Sensitivity for	 1, 2 Mbps (BPSK, QPSK): -90 dbm
802.11b	 5.5 Mbps (CCK): -86 dbm
	 11 Mbps (CCK): -82 dbm
	• (Typically @PER < 8% packet size 1024 and $@25^{\circ}C \pm 5^{\circ}C$)
Sensitivity for	 ◆ 54 Mbps: -68 dbm
802.11g (draft)	 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
	(Typically @PER < 8% packet size 1024 and @25 $^{\circ}$ C +5 $^{\circ}$ C)
Security	 Wired Equivalent Privacy (WEP) 64 / 128 bit
	 802.1x security (MD5 and TLS) in Windows XP only.
	Wi-Fi Protected Access (TBD)
Antenna Type	 Single Dipole Antenna, 1.5dBi gain

Interface	PCI Standard v2.2
Power Voltage	 ◆ 5 Volt <u>+</u> 5%
Power	 802.11g (draft): TX 650mA, RX 450mA, Standby 20mA
Consumption	 802.11b: TX 600mA, RX 350mA, Standby 20mA

* Design and specifications are subject to change without notice.