11B/G Wireless Mini PCI Adapter WL533MAM User's Manual

FCC Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received; including interference that may cause undesired operation.

Federal Communications Commission (FCC) Statement.

This Equipment has been tested and found to comply with the limits 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 in accordance with 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 can be determined 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 and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in devices where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example access points, routers, wireless ADSL modems, and similar equipment). The final end product must be labeled in visible area with the following:

"Contains TX FCC ID: PBLWL533M"

End Product Manual Information

The user manual for end users must include the following information in a prominent location "IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

Other important note:

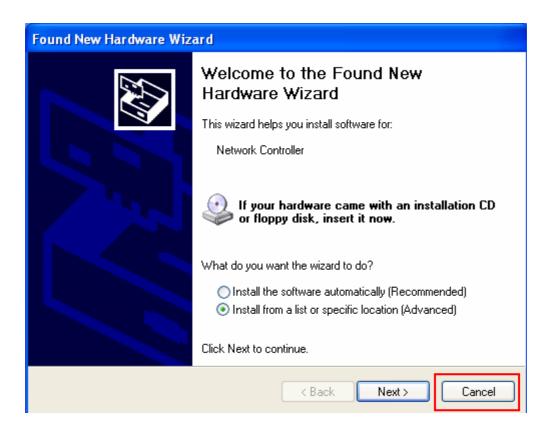
- 1. The end user may not be provided with instructions to remove or install the device.
- 2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- 3. This device is authorised for OEM integration only.

Chapter 1 Install Driver for Windows Series

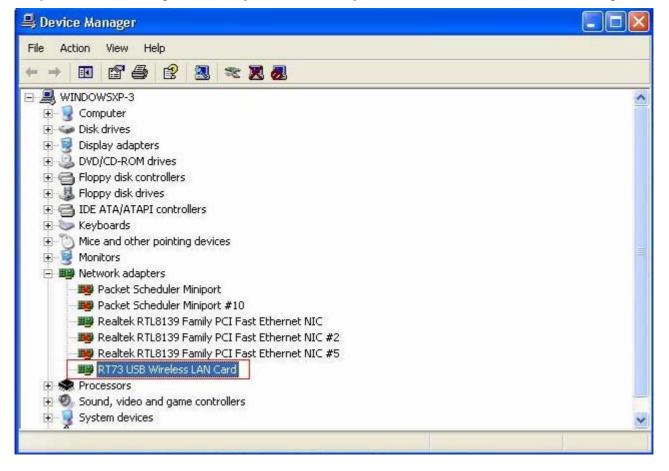
This section describes the installation of the **11b/g Wireless Mini PCI Adapter** driver for the Windows98/ME/2000 and Windows XP operating systems.

1-1 Set up 11b/g Wireless Mini PCI Adapter for Windows Series

Step 1: After inserting the **Wireless Mini PCI Adapter** into the Mini PCI port on notebook or desktop, the Windows will auto-detect the Wireless Mini PCI Adapter and a "**Found New Hardware Wizard**" window will show up. Select "**Cancel**" to install the driver from CD-Rom.



Step 2: Insert the Product CD-ROM into the CD-ROM drive. Select "Setup.exe" to install Driver and Utility.



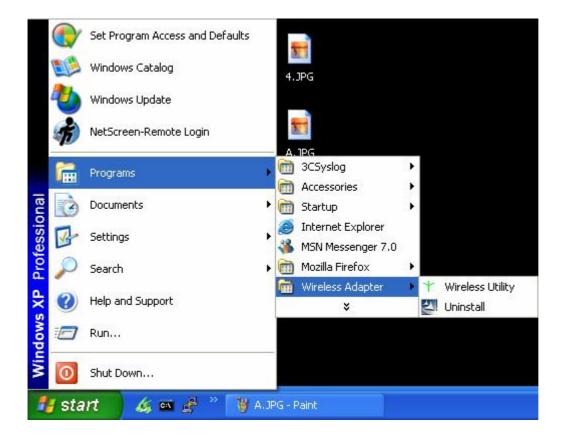
Step 3: After installing the driver, you can check if your device is active in the device management

Chapter 2 Configure Wireless Mini PCI Adapter

This chapter will show you how to configure your **Wireless Mini PCI Adapter** by using utility in the Product CD Package under Windows series Operation System

2-1 Install Utility

1. After finishing the install process, you can execute the utility as follows



 You will see the utility icon after you executing program "Wireless Utility" if your Wireless Mini PCI Adapter is alive



3. If your operation system belong to Windows XP and have update to SP1, click the right button on the icon. You will see the frame below. If you want to configure your **Wireless Mini PCI Adapter** with "Wireless Zero Configure" supported by XP, you should choose "Use Zero Configuration as Configuration utility".



2-2 Configure Wireless Mini PCI Adapter with Zero Configure

After installing **Wireless Mini PCI Adapter**, the Windows XP will display a "Wireless Network Connection" message.



Click on the message and the "*Automatic Wireless Network Configuration*" will then appear automatically and allow users to connect to an available Wireless infrastructure network (Access Point), shown as follows. You may click the "Advanced" button to make advanced configuration for the Wireless LAN Card, shown as below.

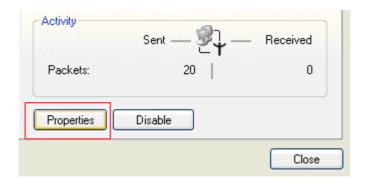
		Connect to Wireless Network				
		The following network(s) are available. To access a network, select it from the list, and then click Connect.				
		Available networks:				
		tidy-amit dale default				
Choose one		1 USB8022				
suitable server		This network requires the use of a network key (WEP). To access this network, type the key, and then click Connect.				
		Network key:				
		If you are having difficulty connecting to a network, click Advanced.				
		Advanced Connect Cancel				

In order to reconfigure you Wireless connection, you can deal as follow procedure

1. Click left button on the network icon as bellow.



2. Click **Properties** to continue



3. Click **Wireless Networks** to reconfigure the Wireless network connection.

Wirel	ess Network Con	nection 4 Pro	perties	?
General	Wireless Networks	Authentication	Advanced	
	Windows to contigue	e ny wireless net	work settings	
	onnect to an available	network, click C	onligure.	
1	default	^	Configu	e
	Hawa		C Ruturi	=
Ŷ	mason3	~	Refrest	1
belov	v maxon3		Move u	
	fidy-amit		Move do	_
Lean	Add Remo about <u>setting up wire</u> auration.		rties Advar	ced
		0	K C	ancel

4. If you need a key (WEP) to connect the Wireless network, you should keyin the key that supported by the Wireless network router or access point

🕹 Wireles	s Network Con	nection 4 Pro	perties	? 🗙					
General	Wireless Networks	Authentication	Advanced						
V es U	Use Windows to configure my wireless network settings								
Available networks:									
To con	To connect to an available network, click Configure.								
i de	fault	^	Configure						
1 We	awa	-		5					
💡 ma	ason3	~	Refresh						
Automa below	d networks: tically connect to a scon3 y-amit	vailable networks	in the order lists Move up Move dow						
	id Remo		Advan	red					
			K C.	ancel					

Wireless Network Prope	erties 🛛 🛛 🔀					
Network name (SSID):	mason3					
This network requires a key for the following:						
Data encryption (WEP enabled) Network Authentication (Shared mode)						
Network key:						
Key format:	Hexadecimal digits 🔽					
Key length:	104 bits (26 digits) 🛛 🔽					
Key index (advanced):	0					
The key is provided for	me automatically					
The key is provided for me automatically This is a computer-to-computer (ad hoc) network; wireless access points are not used OK Cancel						

Chapter 3 Configure Wireless Mini PCI Adapter with

" Wireless Utility" for Windows 98/ME/2000/XP

Click the utility icon, and you will see the application interface as step 2.



3-1 Site Survey Page

SSID	BSSID	Signal	Channel	Encryption	Authentication	Network Type
SAP	00-0C-4	99%	5	NotUse	Unknown	Infrastructure
AP2500	00-0C-4	99%	1	Not Use	Unknown	Infrastructure
WAP11	00-06-25	99%	1	Not Use	Unknown	Infrastructure
NDTES	00-40-96	78%	6	WEP	Unknown	Infrastructure
NDTES	00-0D-5	89%	6	WEP	Unknown	Infrastructure
Dell1184	00-90-4	78%	6	Not Use	Unknown	Infrastructure
default	00-90-96	81%	6	Not Use	Unknown	Infrastructure
- Du ffaloG	00-07-40	100%	11	AES-CC	WPA-PSK	Infrastructure
<mark>⊗</mark> SMC28	00-04-E	100%	11	Not Use	Unknown	Infrastructure
<						

- 1. The means of item
- SSID : Name of AP
- BSSID : Mac Address of AP
- Signal : Signal strength of AP
- Channel : AP used channel
- Encryption : what encrypted mechanism does AP used, the encrypted mechanism contain four ways , WEP, AES, TKIP, NOT USE
- Authentication : What authentication mechanism does AP used.

- Network Type : What Network Type does the AP belong to.
- 2. The connected AP
- the system will choose the suitable AP when you start up RaConfig in the first time
- if you want to connect with another AP, double click mouse's left button in the SSID of AP.
- indicate connect successful.
- 3. if the connect is success, it will show the SSID of the connected AP
- 4. <u>**RESCAN</u>** rescan and upgrade all the AP's information in time</u>
 - <u>CONNECT</u> connect with selected AP
- 6. <u>ADD PROFILE</u> Save the selected AP's information to Profile
- *3-1-1 Add/Edit Profile*

5.

System Configuration: as figure bellow

Add Profile	X
Configuration Authentication and Security	1
Profile Name PROF2	ssid 🔽 🔽 🛃
3 PSM CAM (Constantly Awake Mode)	C PSM (Power Saving Mode)
4 Network Type Ad hoc 💌	TX Power Auto 5
6 Preamble Auto 💌	Ad hoc wireless 802.11 A/B/G mix 🔽 7
⁸ □ RTS Threshold 0 <u>·</u> □ Fragment Threshold 256 ·	2347 2347 Channel 9
OK	Cancel Apply Help

- 1. Profile Name: Different AP can be set up into different Profile Name
- 2. SSID: The drop-down menu can select which AP is detected by system
- 3. Power Save Mode: can select [CAM (Constantly Awake Mode)] or [Power Saving Mode] mode. Selecting the" CAM when AC Power" means the power saving mode can automatically switch into CAM, if the computer uses the AC power, not using the batteries instead. Selecting the "Power Save Mode" can only work under the infrastructure mode.
- 4. Network Type: Can select "Infrastructure" or "802.11 Ad Hoc" mode. When set up to "Infrastructure" mode, the "Power Saving" mode will be enabled, but the "11b Preamble Type" will not; When set up to "802.11 Ad Hoc" mode, the "Power Saving Mode" will not be enabled, but "11b Preamble" will, and the channel selection in the session 7 will show up as well.
- 5. TX Power: Transmit power, the amount of power used by a radio transceiver to send the signal out. User can choose power value by sliding the bar.
- 6. Preamble: There are three types, Auto, Long and Short are supported.
- Ad hoc wireless mode: There are five types. 802.11B only, 802.11 B/G mixed 802.11A only, 802.11 A/B/G mixed and 802.11G only modes are supported.

- 8. RTS Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2312.
- 9. Fragment Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2312.

Note: Channel: Only available for setting under ad-hoc mode. User can choose the channel frequency to start their ad-hoc network.

Profile function is based on the needs to set up the most linkable AP in order to record the system configuration and to set up the authentication security. The function of each session is shown below

3-2 Authentication & Security

As shown in picture. When the Encryption feature is enabled, the other setups are same as the said WEP setting.

•		
•		
•		
•		
	• •	

- 1. Authentication Type: There are three type of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.
- 2. 802.1x Setting: It will display to set when user use radius server to authenticate client certificate for WPA authentication mode. The detail operation will explain in section 5-6 Configure connection with WPA by 802.1x setting
- 3. Encryption Type: For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
- 4. WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 lengths.
- 5. WEP Key: Only valid when using WEP encryption algorithm. The key must matched AP key. There are several formats to enter the keys.
 - i. Hexadecimal, 40bits : 10 Hex characters.

- ii. Hexadecimal, 128bits : 32Hex characters.
- iii. ASCII、 40bits: 5 ASCII characters.
- iv. ASCII, 128bits : 13 ASCII characters.

3-2-1 802.1x Setting

ertification CA S	erver		
Authentication	Type PEAP	Session Besumption	Disabled 🔽
3 Identity		Password	
🔲 Use Client d	ertificate		
Issued To :			
Issued By :			
Expired On :			
Friendly Name	4		More
Use Client certif	icate	6	
Protocol	EAP-MSCHAP v2	Identity	
		Password	
	ОК	Cancel	Apply Help

802.1x is a authentication for $\[\] WPA_{a} \]$ and $\[\] WPA_{a} \]$ certificate to server. Show as figure 1. Authentication type:

- i. PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- ii. TLS / Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

- iii. TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- iv. LEAP: Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
- MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.
- Session Resumption: user can choose "Disable ", "Reauthentication ", "Roaming ", "SameSsid " and "Always ".
- 3. Identity and Password: Identity and password for server.
- 4. Use Client Certificate: Client Certificate for server authentication.
- 5. Tunnel Authentication
 - i. Protocol: Tunnel protocol, List information include "EAP-MSCHAP", "EAP-MSCHAP v2", "CAHAP" and "MD5"
 - ii. Tunnel Identity: Identity for tunnel.
 - iii. Tunnel Password: Password for tunnel.
- 6. CA Server: Certificate Authority Server. Each certificate is signed or issued by it. The detail operation will explain in section 4-2-2 CA Server

3-2-2 CA Server

Depending on the EAP in use, only the server or both the server and client may be authenticated and require a certificate. Server certificates identify a server, usually an authentication or RADIUS server to clients. Most EAPs require a certificate issued by a root authority or a trusted commercial CA. Show as the figure.

- 1. Certificate issuer: Choose use server that issuer of certificates.
- 2. Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.
- 3. Server name: Enter an authentication sever root.

802.1x Setting	×
Certification CA Server	
Use certificate chain	
Certificate issuer :	
- Any Trusted CA -	
Allow intermidiate certificates	
Server name :	
 Server name must match exactly 	
O Domain name must end in specified name	
OK Cancel Apply Help	

3-3 Profile Page

Profile can book keeping your favorite wireless setting among your home, office, and other public hotspot. You may save multiple profiles, and activate the correct one at your preference.

Profile	SSID	Channel	Authentication	Encryption	Network Type
PROFI	NDTESTAP2	Auto	Open System	NotUse	Infrastructure
PROF2	WAP11	Auto	Open System	Not Use	Infrastructure
🖌 PROF3 👘	BuffaloG	Auto	Open System	Not Use	Infrastructure
PROF4	Dell1184	Auto	Open System	Not Use	Infrastructure
< 3 ADD		LETE	5 <u>E</u> DIT		ACTIVATE

- 1. Definition of each field:
 - i. Profile: Name of profile, preset to PROF* (* indicate 1, 2, 3,).
 - ii. SSID: AP or Ad-hoc name.
 - iii. Cannel: Channel in use for Ad-Hoc mode.
 - iv. Authentication: Authentication mode.
 - v. Encryption: Security algorithm in use.
 - vi. Network Type: Network's type, icluding infrastructure and Ad-Hoc.
- 2. Connection status



Indicate connection is successful on currently activated profile.

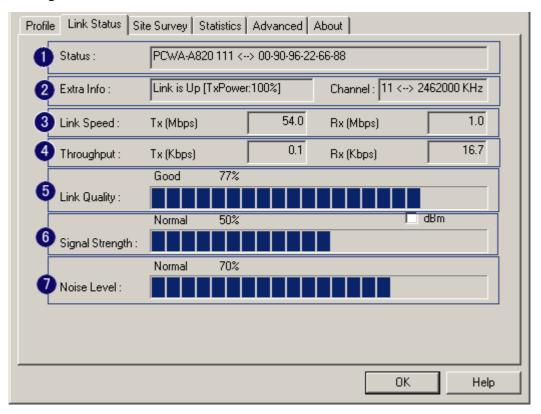


Indicate connection is failed on currently activated profile.

- 3. Add a new profile.
- 4. Delete an existing profile.
- 5. Edit Profile
- 6. Activate selected profile.

3-4 Link Status Page

Show the information of linking status. As show in picture 20, the description of each session is said as following:



- 1. Status: Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.
- 2. Extra Info: Display link status and current channel in use.
- 3. Link Speed: Show current transmit rate and receive rate.
- 4. Throughout: Display transmits and receive throughput in unit of K bits/sec.
- 5. Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.
- 6. Signal Strength: Receive signal strength, user can choose to display as percentage or dBm format
- 7. Noise Level: Display noise signal strength.

3-5 Statistics Page

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for user to understand.

nsmit Statistics		
Frames Transmitted Successfully	=	208
Frames Transmitted Successfully Without Retry	=	196
Frames Transmitted Successfully After Retry(s)	=	12
Frames Fail To Receive ACK After All Retries	=	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0
eive Statistics		
Frames Received Successfully	=	23173
Frames Received With CRC Error	=	224800
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

1. Transmit Statistics:

- i. Frames Transmitted Successfully: Frames successfully sent.
- ii. Frames Transmitted Successfully Without Retry: Frames successfully sent without any retry.
- iii. Frames Transmitted Successfully After Retry: Frames successfully sent with one or more reties.
- iv. Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.
- v. RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.
- vi. RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.
- 2. Receive Statistics:
 - i. Frames Received Successfully: Frames received successfully.
 - ii. Frames Received With CRC Error: Frames received with CRC error.
 - iii. Frames Dropped Due To Out-of-Resource: Frames dropped due to resource issue.
 - iv. Duplicate Frames Received: Duplicate received frames.

3. <u>RESET COUNTERS</u> To zero the statistic numbers of transmitting and receiving data.

3-6 Advance Page

The advance setting is shown as follows. The description of each session is said as following:

Prof	ile 🛛 Link Status 🗍 Site Sur	vey Statistics Ac	lvanced	About
0	Wireless mode	802.11 B/G mix	•]
0	B/G Protection	Auto	•	
8	Tx Rate	Auto	•	
0	CCX 2.0			3
	LEAP turn on CCKM		Tx BURST	
	🔲 Enable Radio Measur		🔲 Enable TCP Window Size	
	☐ Non-Serving Channel Limit 250 mill	l Measurements iseconds (0-2000)		Fast Roaming at -70 dBm
0	Tum off RF			2 Apply

- Wireless mode: Select wireless mode. 802.11B only, 802.11 B/G mixed 802.11A only, 802.11 A/B/G mixed and 802.11G only modes are supported.
- 2. 11B/G Protection: ERP protection mode of 802.11G definition. User can chosse from Auto, On, and Off
 - i. Auto: STA will dynamically change as AP announcement.
 - ii. On: Always send frame with protection.
 - iii. Off: Always send frame without protection.
- 3. TX Rate: Manually force the Transmit using selected rate. Default is auto.
- 4. CCX2.0: support Cisco Compatible Extensions function:
 - i. LEAP turn on CCKM
 - ii. Enable Radio Measurement: can channel measurement every 0~2000 milliseconds.
- 5. Tx Burst: Ralink's proprietary frame burst mode.
- 6. Wireless radio signal control
 - Y <u>R</u>ADIO OFF

: means to open the wireless radio signal and show simultaneously:

<u>RADIO ON</u>

: means to close the wireless radio signal and show simultaneously:

7. Apply Means the modification of session 1~4 are formally used.

3-7 About Page

About page display the wireless card and driver version information shown as follow figure .

rofile	Link Status Site Su	urvey Statistics A	dvanced About	
	G •	WWW.RA)	LINKTECH.COM	
	(c) Copyright 2004	, Ralink Technology	, Inc. All rights rese	rved.
0	RaConfig Version	1.0.7.0	Date :	08-17-2005
	Driver Version :	1.0.1.4	Date :	07-25-2005
l	EEPROM Version :	1.0		
3	IP Address :	192.168.12.101	Phy_Address :	00-0C-43-26-61-00
	Sub Mask :	255.255.255.0		192.168.12.25

- 1. Connect to RaLink's website: <u>Ralink Technology, Corp.</u>
- 2. Display Configuration Utility, Driver, and EEPROM version information.
- 3. Display Wireless NIC MAC address.

Chapter 4 Example

4-1 Adding profile in site survey page

1. Select the indented network from site survey list.

SSID	BSSID	Sig	C	Encry	Authent	Network T
😸 BuffaloG	00-07-40-76-D	76%	11	Not Use	Unknown	Infrastruct.
3com	00-0B-AC-E7-5	83%	1	Not Use	Unknown	Infrastruct.
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.
AP25-Left	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct.
default	00-90-96-28-39	10	6	Not Use	Unknown	Infrastruct.
\frown	00-07-40-4D-0	10	6	Not Use	Unknown	Infrastruct.
Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.
Wpe	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.
NDTESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct.
<]						·)

2. Click ADD PROFILE.

SSID	BSSID	Sig	C	Encry	Authent	Network T
😸 BuffaloG	00-07-40-76-D	76%	11	Not Use	Unknown	Infrastruct.
3com	00-0B-AC-E7-5	83%	1	Not Use	Unknown	Infrastruct.
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.
AP25-Left	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct.
default	00-90-96-28-39	10	6	Not Use	Unknown	Infrastruct.
	00-07-40-4D-0	10	6	Not Use	Unknown	Infrastruct.
Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.
Ralink_tess	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.
wpa	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.
NDTESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct.

3. System will pop up Add Profile windows

DECEI	D.11104	
Profile Name PROF1	SSID Dell1184	_
ystem Configuration Authentication & Secu	urity	
Power Saving Mode		-
 CAM (Constantly Awake Mode) 	C Power Saving Mode	
CAM when AC Power		
CAM WIEITAC FOWER		
Network Type Infrastructure	•	
11B Preamble Type Auto	Y	
□ RTS Threshold 0 '	2347 2347	
Fragment Threshold ²⁵⁶	2347 2347	

4. Change profile Name from PROF1 to FAVORITE.

Profile Name FAVORITE	SSID Dell1184
System Configuration Authentication & Power Saving Mode C CAM (Constantly Awake Mode) CAM when AC Power	
Network Type Infrastructure 11B Preamble Type Auto RTS Threshold 0 ' Fragment Threshold 256 '	✓ ✓ 2347 2347 2347 2347 2347 2347
<u> </u>	<u>C</u> ANCEL

5. Click OK without changing other value.

Prof	ile Link Status S Profiles List	Site Survey S	tatistics A	lvance About		
	Profile	SSID	Channel	Authentication	Encryption	Network Type
\triangleleft	FAVORITE	Dell1184	Auto	Open System	Not Use	Infrastructure
	<					>
Γ	ADD	DEL	ETE.	EDIT		ACTIVATE

4-2 Add profile in profile page

1. Click ADD in profile page

Image: second	Profile	SSID	Channel	Authentication	Encryption	Network Type
Image:						

2. Add Profile page will pop up

ld Profile			
Profile Name PROF1		SSID	•
System Configuration At	thentication & Securi	ity	
Power Saving Mode —			
CAM (Constantly)	' Awake Mode)	C Power Saving Mode	
CAM when AC P	ower		
· [
Network Type	Infrastructure	•	
11B Preamble Type	Auto	<u>*</u>	
🔲 RTS Threshold	0 ,	2347 2347	
	Ja 256 ,	2347 2347	
Fragment Thresh	Jua		
	<u>OK</u>	CANCEL	

3. Change profile name to TEST.

dd Profile	
Profile Name TEST	SSID 🔽
System Configuration Authentication & Secur	ity
Power Saving Mode	
CAM (Constantly Awake Mode)	C Power Saving Mode
CAM when AC Power	
Network Type Infrastructure	×
11B Preamble Type Auto	Y
□ RTS Threshold 0 '	2347 2347
Fragment Threshold 256	<u>\</u> ²³⁴⁷ 2 ³⁴⁷
Ōĸ	<u>C</u> ANCEL

4. Pull down SSID and select one intended AP. The AP list is the result of last site survey.

Add Profile			🛛
Profile Name TEST		SSID	-
System Configuration Aut	nentication & Security	MPA AP350 NDTESTAP1	^
Power Saving Mode —		default	12 -
CAM (Constantly I)	wake Mode)	C Power Saving Mode	
CAM when AC Po	ver		
			<u> </u>
Network Type	Infrastructure 💌		
11B Preamble Type	Auto 💌]	
🔲 RIS Threshold	0 ,	2347 2347	
🦵 Fragment Threshold	, 256 ,	2347 2347	
j riaginent ridesion			
	~~]	euror 1	
	<u>O</u> K	CANCEL	

5. Set Power Saving Mode.

ld Profile			
Profile Name TEST		SSID NDTESTAP1	•
ystem Configuration Authen	tication & Security	1	
– Power Saving Mode C CAM (Constantly Awa	ake Mode)	• Power Saving Mode	
CAM when AC Power			
Network Type	rastructure	•	
11B Preamble Type 🛛 🗛	to	r.	
🔲 RTS Threshold	0 .	2347 2347	
🦵 Fragment Threshold	256 ,	2347 2347	
	al.		
<u>O</u> K		CANCEL	

6. Click Authentication & Security page

stem Configuration	uthentication	& Security				
Authentication Type:	Open	1	• Enc	ryption Type:	None	•
WPA Pre-Shared Key:						
- WEP Key						
€ Key# <u>1</u> He	xadecimal	Y				
C Key#2 He	xadecimal	·				
C Key# <u>3</u> He	xadecimal	<u> </u>				
C Key#4 He	xadecimal	-				

7. Click OK. Then we can find the profile name appears in the grid.

rof	ile Link Stati rofiles List —	us Site Survey S	tatistics A	dvance About		
4	Profile TEST	SSID NDTESTAP1	Channel Auto	Authentication Open System	Encryption WEP	Network Type Infrastructure
	<]			 		>
	ADD	DEI	LETE	EDIT		ACTIVATE

8. Click ACTIVATE. Activate the profile setting.

Profile	SSID	Channel	Authentication	Encryption	Network Type
🎸 TEST	NDTESTAP1	Auto	Open System	WEP	Infrastructure

4-3 WEP encryption

1. Select AP with WEP encryption.

SSID	BSSID	Sig	C	Encry	Authent	Network T 🔺
miffy	00-0C-43-25-61	73%	1	TKIP	WPA-P	Infrastruct.
WAP11	00-06-25-55-D8	47%	1	WEP	Unknown	Infrastruct.
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.
NDTESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.
AP25-Left	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct. 🗏
wpa	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.
🥳 Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.
AP350	00-40-96-56-2A	10	6	WEP	Unknown	Infrastruct.
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.
default	00-90-96-28-39	76%	6	Not Use	Unknown	Infrastruct.
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct. 🗸
<						-)) ·

2. Click CONNECT or doucle click intended network.

SSID	BSSID	Sig	C	Encry	Authent	Network T 🔺
miffy	00-0C-43-25-61	73%	1	TKIP	WPA-P	Infrastruct.
WAP11	00-06-25-55-D8	47%	1	WEP	Unknown	Infrastruct.
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.
NDTESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.
AP25-Left い	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct. 🗏
wpa	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.
🥳 Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.
AP350	00-40-96-56-2A	10	6	WEP	Unknown	Infrastruct.
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.
default	00-90-96-28-39	76%	6	Not Use	Unknown	Infrastruct.
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct. 🗸
<						· >

3. Authentication & Security page pop up.

Authentication & Security
Authentication Type: Open Encryption Type: WEP WPA Pre-Shared Key:
WEP Key • Key#1 Hexadecimal • Key#2 Hexadecimal • Key#3 Hexadecimal
© Key# <u>4</u> Hexadecimal ▼ <u>QK</u> <u>CANCEL</u>

4. Enter 0123456789 at Key#1 which is same as our intended AP's setting.

ithentication & Secu	ity		
Authentication Type:	Open	Encryption Type: WEP	•
WPA Pre-Shared Key:			
- WEP Key		\frown	
	adecimal 💌 🚺	123456789	
C V. #2 Hor	adecimal 🔹		
			_
⊂ Key# <u>3</u> He>	radecimal 🗾		
← Key# <u>4</u> Hex	adecimal 💌		
	<u>O</u> K	CANCEL	

SSID	BSSID	Sig	C	Encry	Authent	Network T 🔨
miffy	00-0C-43-25-61	73%	1	TKIP	WPA-P	Infrastruct.
WAP11	00-06-25-55-D8	47%	1	WEP	Unknown	Infrastruct.
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.
MI TESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.
AP25-Left	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct. 🗏
wpa	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.
Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.
AP350	00-40-96-56-2A	10	6	WEP	Unknown	Infrastruct.
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.
default	00-90-96-28-39	76%	6	Not Use	Unknown	Infrastruct.
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct. 🗸
¢]						

4-4 Configure connection with WPA-PSK

1. Select the AP with WPA-PSK authentication mode.

SSID	BSSID	Sig	C	Enery	Authent	Network T
PSKtest N	00-0C-43-25-61	65%	1	TKIP	WPA-P	Infrastruct
NDTESTAP1	00-40-96-56-2A	37%	1	Not Use	Unknown	Infrastruct
miffy	00-0C-43-25-61	65%	1	TKIP	WPA	Infrastruct
SoftAP-D8	00-0A-40-00-00	65%	1	Not Use	Unknown	Infrastruct
AP000C43256	00-0C-43-05-00	55%	1	WEP	Unknown	Infrastruct
WAP11	00-06-25-55-D8	29%	1	WEP	Unknown	Infrastruct
Qoo_1	B2-00-CF-03-3	23%	3	Not Use	Unknown	Ad Hoc
Buffalo	00-07-40-4D-0	10	6	TKIP	WPA	Infrastruct
🛃 NDC_CASE	00-80-C8-03-32	10	6	WEP	Unknown	Infrastruct
NDTESTAP2	00-04-76-A5-E	10	6	WEP	Unknown	Infrastruct
BuffaloG	00-07-40-76-D	34%	11	Not Use	Unknown	Infrastruct

2. Click CONNECT or double click the intended network.

SSID	BSSID	Sig	C	Encry	Authent	Network T
PSKtest 📐	00-0C-43-25-61	65%	1	TKIP	WPA-P	Infrastruct
NDTESTAP1	00-40-96-56-2A	37%	1	Not Use	Unknown	Infrastruct
miffy	00-0C-43-25-61	65%	1	TKIP	WPA	Infrastruct
SoftAP-D8	00-0A-40-00-00	65%	1	Not Use	Unknown	Infrastruct
AP000C43256	00-0C-43-05-00	55%	1	WEP	Unknown	Infrastruct
WAP11	00-06-25-55-D8	29%	1	WEP	Unknown	Infrastruct
Qoo_1	B2-00-CF-03-3	23%	3	Not Use	Unknown	Ad Hoc
Buffalo	00-07-40-4D-0	10	6	TKIP	WPA	Infrastruct
🚽 NDC_CASE	00-80-C8-03-32	10	6	WEP	Unknown	Infrastruct
NDTESTAP2	00-04-76-A5-E	10	6	WEP	Unknown	Infrastruct
BuffaloG	00-07-40-76-D	34%	11	Not Use	Unknown	Infrastruct

3. Authentication & Security page will pop up.

athentication & Securi	WPA-PSK	- Francisco Tarras (TVID	
Authentication Type:	WPA-PSK	▼ Encryption Type: TKIP	-
WPA Pre-Shared Key:	ļ		
- WEP Key			
€ Key# <u>1</u> Hexa	decimal 📃 💌		
C Key#2 Hexa	decimal 🔻		
		, 	
C Key# <u>3</u> Hexa	decimal 💌	J	
C Key# <u>4</u> Hexa	decimal 📃 💌		
	<u>O</u> K	CANCEL	

*If AP setup security to "Both " (TKIP + AES), system define is AES that security is severely.

4. Authentication Type is WPA-PSK. Select correct encryption (TKIP or AES).Enter WPA Pre-Shared Keysecret as 01234567.

Authentication Type: WPA Pre-Shared Key:	WPA-PSK 01234567	Encryption Ty	ље: ТКIР	•
- WEP Key-	adecimal 👻	·		
	adecimal 💌	, ,		
	adecimal 💌			
C Key# <u>4</u> Hexa	adecimal 💌]	2076	<u> </u>

5. Click OK. Be careful, if the WPA Pre-Shared Key entered is not correct, even though the AP can be connected, but you won't be able to exchange any data frames.

SSID	BSSID	Sig	C	Encry	Authent	Network T
😸 PSK test 🔵	00-0C-43-25-61	65%	1	TKIP	WPA-P	Infrastruct
ND TESTAP1	00-40-96-56-2A	37%	1	Not Use	Unknown	Infrastruct
miffy	00-0C-43-25-61	65%	1	TKIP	WPA	Infrastruct
SoftAP-D8	00-0A-40-00-00	65%	1	Not Use	Unknown	Infrastruct
AP000C43256	00-0C-43-05-00	55%	1	WEP	Unknown	Infrastruct
WAP11	00-06-25-55-D8	29%	1	WEP	Unknown	Infrastruct
Qoo_1	B2-00-CF-03-3	23%	3	Not Use	Unknown	Ad Hoc
Buffalo	00-07-40-4D-0	10	6	TKIP	WPA	Infrastruct
NDC_CASE	00-80-C8-03-32	10	6	WEP	Unknown	Infrastruct
NDTESTAP2	00-04-76-A5-E	10	6	WEP	Unknown	Infrastruct
BuffaloG	00-07-40-76-D	34%	11	Not Use	Unknown	Infrastruct

4-5 Configure connection with WPA2-PSK

1.	Select the AP with WPA2-PSK authentication mode.	

SSID	BSSID	Sig	C	Encrypt	Authent	Network T
🤡 default	00-50-18-29-88	10	6	None	Unknown	Infrastruct.
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct.
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2-PSK	Infrastruct.
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct.
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct.
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct.
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct.
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct.
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct.
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct.
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct.
•)

2. Click CONNECT or double click the intended network.

.

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.,
😸 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2-PSK	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct
•						

3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

tuthentication Type :	WPA2-PSK -	802.1x Setting
incryption :	TKIP	
VPA Preshared Key :		
Wep Key		
	x 💌	
C Key#2 He	x v	
C Key#3 He	x 💌	
C Key#4 He	K 💌	
	yption: Please Keyin 10 HEX charact syption: Please Keyin 26 HEX charac	
		Show Passward

*If AP setup security to "Both " (TKIP + AES), system define is AES that security is severely.

4. Authentication Type is WPA-PSK. Select correct encryption (TKIP or AES). Enter WPA Pre-Shared Keysecret as 12345678.

Authentication and Sec	urity			×
Authentication Type :	WPA2-PSK	•	802.1x Setting	
Encryption :	TKIP		•	
WPA Preshared Key :	12345678	>		
r Wep Key				
€ Key#1 Hex	· ·			
C Key#2 Hex				
C Key#3 Hex				
C Key#4 Hex	-			
	vption: Please Keyin ryption: Please Keyir			
		2	Show Passward	
	ОК	Cancel		

5. Click OK. Be careful, if the WPA Pre-Shared Key entered is not correct, even though the AP can be connected, but you won't be able to exchange any data frames.

default WL-HDD	00-50-18-29-8B					Network T.
VIL HOD	00 00 10 20 00	10	6	None	Unknown	Infrastruct
WENDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
😸 miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2-PSK	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct.
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct.
•						•

4-6 Configure connection with WPA by 802.1x setting

1. Select A.P with WPA authentication mode.

SSID	BSSID	Sig	C	Encrypt	Authent	Network T
😸 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct.
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct.
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA	Infrastruct.
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct.
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct.
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct.
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct.
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct.
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct.
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct.
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct.
•						•

2. Click CONNECT or double click the intended network

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
🥁 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct.
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct
•						

3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

Authentication Type :	WPA -	802.1x Setting
Encryption :	TKIP	-
WPA Preshared Key :		
Wep Key		
€ Key#1	ies 💌	
C Key#2	iex 💌	
C Key#3	fex 💌	
C Key#4	ies 📼	
	cryption: Please Keyin 10 HEX incryption: Please Keyin 26 HEX	
		Show Passward

*If AP setup security to "Both " (TKIP + AES), system define is AES that security is severely.
4. Click 802.1x setting.

Authentication Type :	TKI		•			l x Setting
Encryption :	<u> </u> IN	Г				_
WPA Preshared Key :						
-Wep Key						
€ Key#1	ex	_				
C Key#2	ex	-				
C Key#3	lex	_				
C Key#4	ex	-				
* WEP 64 Bits En * WEP 128 Bits E	cryption: ncryption:	Please Key Please Ke	in 10 HEX ch yin 26 HEX c	aracters haracters		
				ſ	Show Pa	issward

5. 802.1x setting page will pop up.

802.1x Setting					>
Certification CA 9	Gerver				
 Authentication 	Type PEAP	-	Session Resumption	Disabled	•
3 Identity		Pas	sword		
🜖 🔲 Use Client (certificate				
Issued To :					
Issued By :					
Expired On :					
Friendly Name	e :			More	
Tunneled Autho	entication				
6 Protocol	EAP-MSCHAP v2	2 💌	dentity		
			Password		٦,
	ОК		Cancel App	y He	

- 6. Authentication type and setting method:
 - 1. PEAP:
 - Authentication type chooses PEAP, key identity into wpatest2. Protocol chooses
 EAP-MSCHAP v2 for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

Authentication	Type PEAP	-	Session Resu	Imption	Disabled
Identity		Pass	sword		
🔲 Use Client co	ertificate				
Issued To :					
Issued By :					
Expired On :					
Expired On : Friendly Name					More
					More
Friendly Name			Identity		More

302.1x Setting
Certification CA Server
Authentication Type PEAP Session Resumption Disabled •
Identity wpatest2 Password
Use Client certificate
Issued To :
Issued By :
Expired On :
Friendly Name : More
Tunneled Authentication
Protocol EAP-MSCHAP v2 Identity wpatest2
Password test2
OK Cancel Apply Help

TLS / Smart Card: 2.

İ. Authentication type chooses TLS / Smart Card, TLS only need identity that is wpatest2 for server authentication.

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
🤡 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct
•						

TLS must use client certificate. Click more to choose certificate. ii.

802.1x Setting	>
Certification CA Server	
Authentication Type TLS/Smart Carc 💌 Session Resumption Disa	abled 🔻
Identity wpatest2 Password	
☑ Use Client certificate	
Issued To :	
Issued By :	
Expired On :	
Friendly Name :	fore
Tunneled Authentication	
Protocol 🗾 Identity	
Password	
OK Cancel Apply	Help

iii. Certificate page will pop up; choose a certificate for server authentication.

Certificate Selection	1		×
Issued To	Issued By	Expired On	Friendly Name
Users	2003ærv	2005/3/19	
	Ж		ancel

iv. Display certificate information in use client certificate page.

2.1x Setting		
ertification CA S	erver	
Authentication	Type TLS/Smart Carc Session Resumption Disable	ed 🔻
Identity	vpatest2 Password	
🔽 Use Client c	ertificate	
Issued To : U	2795	
Issued By : 12)03serv	
Expired On : 2		_
Friendly Name	: (null) Mor	e
_ Tunneled Authe	ntication	
Protocol	✓ Identity	
	,	
	Password	
	OK Cancel Apply	Help

ertification CA 9	Server				
Authentication	n Type TTLS	•	Session Re	sumption	Disabled
Identity	wpatest2	Pas	sword		
🔽 Use Client	certificate				
Issued To :					
Issued By :					
Expired On :					
Friendly Name	e:				More
Tunneled Auth	entication				
Protocol	CHAP	-	Identity	wpatest2	
			Password	test2	

3. TTLS:

i. Authentication type chooses TTLS, identity is wpatest2. Protocol chooses CHAP for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

802.1x Setting		×
Certification CA Server		
Authentication Type TTLS	Session Resumption Disabled	-
Identity wpatest2	Password	
Use Client certificate		
Issued To :		
Issued By :		
Expired On :		
Friendly Name :	More	
Tunneled Authentication		
Protocol CHAP	✓ Identity wpatest2	
	Password test2	
ОК	Cancel Apply Help	

802.1x Setting ×
Certification CA Server
Authentication Type PEAP Session Resumption Disabled
Identity wpatest2 Password
✓ Use Client certificate
Issued To :
Issued By :
Expired On :
Friendly Name :More
Tunneled Authentication
Protocol EAP-MSCHAP v2 Identity wpatest2
Password test2
OK Cancel Apply Help

- 4. MD5:
 - i. Authentication type chooses MD5, MD5 only need identity and password that are wpatest2 and test2 for server authentication.

02.1:	x Setting						,
Certifi	ication CA	Server					
ļ	Authenticatio	on Type Md.	5-Challenge 💌	Session Re	sumption	Disabled	•
I	Identity	wpatest2	Pa	ssword			
	🛛 Use Client	certificate					
1	lssued To :						
	Issued By :						
E	Expired On :						
F	Friendly Nam	ie :				More	
E Tu	unneled Auth	nentication					
F	Protocol		T	Identity			
							_
				Password			
			ок	Cancel	Apply	Н	elp

tification CA	Server
Authenticatio	n Type FEAP Session Resumption Disabled
Identity	wpatest2 Password
🔽 Use Client	certificate
Issued To :	
Issued By :	
Expired On :	
Expired On : Friendly Narr	e: More
	e:
Friendly Narr	e:
Friendly Nan Tunneled Aut	e :

4-7 Configure connection with WPA2 by 802.1x setting

1. Select A.P with WPA2 authentication mode.

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
🥳 default	00-50-18-29-88	10	6	None	Unknown	Infrastruct
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct
•						▶

Profile Link Status Site Survey Statistics Advanced About

2. Click CONNECT or double click the intended network.

Profile Link Status Site Survey Statistics Advanced About

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.,			
🥩 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct			
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct			
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2	Infrastruct			
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct			
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct			
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct			
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct			
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct			
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct			
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct			
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct			
Connected <> default Rescan Connect Add to Profile									

3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

ithentication and	Jecurry					>
Authentication Type :		IPA2			802.1x Setting	
Encryption :	TH	<ip< th=""><th></th><th></th><th>•</th><th>]</th></ip<>			•]
WPA Preshared Key	:]
⊂ Wep Key						
€ Key#1	Hex	_				
🔿 Key#2	Hex	~				
C Key#3	Hex	~				
C Key#4	Hex	v				
			10 HEX characte 26 HEX charac			
				□ s	how Passward	
[OK			Cancel		

*If AP setup security to "Both " (TKIP + AES), system define is AES that security is severely.

4. Click 802.1x setting.

Authentication an	d Security			×
Authentication Type	e: WPA2		802.1x Setting)
Encryption :	TKIP		•	
WPA Preshared Ke	ey :		í.	
r Wep Key				
Key#1	Hex 💌			
C Key#2	Hex			
C Key#3	Hex 💌			
C Key#4	Hex 💌			
* WEP 64 Bit * WEP 128 B	s Encryption: Please K its Encryption: Please	eyin 10 HEX characters Keyin 26 HEX characters		
			Show Passward	
	ОК		Cancel	

5. 802.1x setting page will pop up.

802.1x Setting					>
Certification CA 9	Gerver				
 Authentication 	Type PEAP	-	Session Resumption	Disabled	•
3 Identity		Pas	sword		
🜖 🔲 Use Client (certificate				
Issued To :					
Issued By :					
Expired On :					
Friendly Name	e :			More	
Tunneled Autho	entication				
6 Protocol	EAP-MSCHAP v2	2 💌	dentity		
			Password		٦,
	ОК		Cancel App	y He	

- 6. Authentication type and setting method:
 - 1. PEAP:
 - Authentication type chooses PEAP, key identity into wpatest2. Protocol chooses
 EAP-MSCHAP v2 for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

02.1x Setting)
Certification CA Ser	ver					
Authentication T	ype PEAP	▼	Session Re	sumption	Disabled	•
Identity		Pas	sword			
🔲 Use Client cer	tificate					
Issued To :						
Issued By :						
Expired On :						
Friendly Name :					More	
- Tunneled Authent	ication					
Protocol	EAP-MSCHAP v2	-	Identity			
			Password			
	OK]	Cancel	Apply	н	elp

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
🤡 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct.
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct.
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2	Infrastruct.
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct.
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct.
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct.
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct.
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct.
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct.
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct.
•						

2. TLS / Smart Card:

i. Authentication type chooses TLS / Smart Card, TLS only need identity that is wpatest2 for server authentication.

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
🥳 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct.
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct.
 ↓ Connected <> defau 	alt	Rescar		Conne	ct Ac	Id to Profile

Profile Link Status Site Survey Statistics Advanced About

ii. TLS must use client certificate. Click more to choose certificate.

802.1x Setting	×
Certification CA Server	
Authentication Type TLS/Smart Carc Session Resumption Disc	abled 🔻
Identity wpatest2 Password	
Use Client certificate	
Issued To :	
Issued By :	
Expired On :	
Friendly Name :	More
Tunneled Authentication	
Protocol dentity	
Password	
OK Cancel Apply	Help

Issued By 2003serv	Expired On	(
2003serv		Friendly Name
20053017	2005/3/19	
ок		Cancel
	ΟΚ	ΟΚ

iii. Certificate page will pop up; choose a certificate for server authentication.

iv. Display certificate information in use client certificate page.

802.	1x Setting					3
Cei	rtification CA Server					
	Authentication Type	LS/Smart Carc 💌	Session Res	umption	Disabled	•
	Identity wpatest2	Pas	sword			
	🔽 Use Client certificate					
	Issued To: Users					
	Issued By: 2003serv					
	Expired On : 2005/6/23 Friendly Name : (null)				More	
Г	Tunneled Authentication—					
	Protocol	~	Identity			
			Password			
		ОК	Cancel	Apply	Н	elp

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
🥌 default	00-50-18-29-88	10	6	None	Unknown	Infrastruct
WLHDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct
•						•

Profile Link Status Site Survey Statistics Advanced About

3. TTLS:

i. Authentication type chooses TTLS, identity is wpatest2. Protocol chooses CHAP for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

302.1x Setting						×
Certification CA S	erver					
Authentication	Type TTLS	•	Session Re	sumption	Disabled	•
Identity	wpatest2	Pas	sword			
🔽 Use Client d	certificate					
Issued To :						
Issued By :						
Expired On :						_
Friendly Name	:				More	
Tunneled Authe	entication					
Protocol	CHAP	•	Identity	wpatest	2	
			_			_
			Password	test2		
	ОК		Cancel	Apply	н	elp

Profile Link Status Site	Survey Statistics	Advanced	About	
--------------------------	-------------------	----------	-------	--

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.,
🥳 default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct
miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2	Infrastruct
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct
•						Þ
Connected <> defau	ılt	Rescar		Conne	et Ac	ld to Profile

- 4. MD5:
 - i. Authentication type chooses MD5, MD5 only need identity and password that are wpatest2 and test2 for server authentication.

tification CA	Server				
Authenticatio	on Type Md5-Challen;	ge 💌 Session R	esumption	Disabled	•
Identity	wpatest2	Password			
🔽 Use Client	t certificate				
Issued To :					
Issued By :					
Expired On :					
Expired On : Friendly Nam				More	
	ne:			More	
Friendly Nam	ne:	 Identity 		More	
Friendly Narr	ne:	Identity Password		More	

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
default	00-50-18-29-8B	10	6	None	Unknown	Infrastruct.
WL-HDD	00-11-2F-DE-34	68%	1	None	Unknown	Infrastruct.
🖇 miraclews	20-05-08-23-02-11	94%	3	TKIP	WPA2	Infrastruct.
MGB100-aren	00-50-18-04-19-15	10	6	None	Unknown	Infrastruct.
MGB100-noJ	00-50-18-08-19-01	10	8	AES	WPA-P	Infrastruct.
wallance	00-50-18-00-0F-63	10	9	None	Unknown	Infrastruct.
RT61_Duncan	00-50-18-00-0F	10	10	AES	WPA-P	Infrastruct.
WDSTKIP	00-50-18-08-1A	10	11	AES	WPA-P	Infrastruct.
default	00-50-18-00-0F-02	89%	11	None	Unknown	Infrastruct.
default	20-05-08-23-05-06	47%	6	None	Unknown	Infrastruct.
default	00-13-46-50-C4	57%	6	None	Unknown	Infrastruct.
1						