Wireless LAN USB Adapter

User Manual 1.0

© 2010

Contents

| 1. | Win | dows Wir | eless Utility | 3 |
|----|------|-----------|---|----|
| | 1.1 | Winde | ows Zero Configuration for XP | 3 |
| | | 1.1.1 | Ralink Wireless Utility and Windows Zero Configuration | 3 |
| | | 1.1.2 | Windows Zero Configuration (WZC) | 4 |
| | 1.2 | Winde | ows AutoConfig Service for Vista | 9 |
| | | 1.2.1 | Ralink Wireless Utility and Windows AutoConfig Service | 9 |
| | | 1.2.2 | Windows AutoConfig Service | 10 |
| 2. | Rali | nk Wirele | ss Utility (RaUI) | 17 |
| | 2.1 | Start. | | 17 |
| | | 2.1.1 | Start RaUI | 17 |
| | 2.2 | Profil | e | 20 |
| | | 2.2.1 | Profile | 20 |
| | | 2.2.2 | Add/Edit Profile | 21 |
| | | 2.2.3 | Example to Add Profile in Profile | 24 |
| | | 2.2.4 | Pre-logon Connect | 26 |
| | 2.3 | Netwo | ork | 26 |
| | | 2.3.1 | Network | 26 |
| | | 2.3.2 | Example on Adding Profile in Network | 29 |
| | 2.4 | Advai | nced | 30 |
| | | 2.4.1 | Advanced | 30 |
| | | 2.4.2 | Certificate Management | 31 |
| | 2.5 | Link l | Information | 32 |
| | | 2.5.1 | Link Status | 32 |
| | | 2.5.2 | Throughput | 33 |
| | | 2.5.3 | Statistics | 33 |
| | 2.6 | About | t | 34 |
| | | 2.6.1 Ab | out | 34 |
| | 2.7 | WPS. | | 35 |
| | | 2.7.1 | WPS | 35 |
| | | 2.7.2 | Example to Add to Registrar Using PIN Method | 37 |
| | | 2.7.3 | Example to Add to Registrar Using PBC Method | 40 |
| | | 2.7.4 | Example to Configure a Network/AP Using PIN or PBC Method | 44 |
| 3. | Secu | urity | | 46 |
| | 3.1 | Auth. | Encry. Setting – WEP/TKIP/AES | 46 |
| | 3.2 | 802.1 | x Setting | 47 |
| | 3.3 | Exam | ple to Configure Connection with WEP on | 50 |
| | 3.4 | Exam | ple to Configure Connection with WPA-PSK | 52 |
| | 3.5 | Exam | ple to Configure Connection with WPA | 54 |
| 4. | App | endix | | 59 |
| | 4.1 | Count | try Channel List | 59 |
| | 4.2 | Ackno | owledgements | 61 |
| 5. | FAC |) | | 62 |
| | 5.1 | FAQ . | | 62 |

1. Windows Wireless Utility

1.1 Windows Zero Configuration for XP

1.1.1 Ralink Wireless Utility and Windows Zero Configuration

Windows XP includes a wireless configuration utility named "Windows Zero configuration" (WZC) which provides basic configuration functions to the Ralink Wireless NIC. Ralink's utility (RaUI) additionally provides WPA functionality. To make it easier for the user to select the correct utility. RaUI will let users make a selection when it first runs after windows XP boots.

Right-clicking the icon will bring up the selection window and allow the user to make a selection.



Figure 1-1 RaUI.exe

RaUI can co-exist with <u>WZC</u>. When coexisting with <u>WZC</u>, RaUI only provides monitoring functions, such as surveying the link status, network status, statistic counters, advanced feature status, WMM status and WPS status. It won't interfere with WZC's configuration or profile functions. It is shown as Figure 1-2.



Figure 1-2 Select WZC or RaUI

If "Use RaConfig as Configuration utility" is selected, please jump to Section 2 on running RaUI.

If "Use Zero Configuration as Configuration utility" is selected, please continue. We will explain the difference between RaUI and <u>WZC</u>. Figure 1-3 shows the RaUI status when <u>WZC</u> is activated as the main control utility.

| Ralink | | Site Survey | × |
|--|---|--|------|
| SSID SSID Rate Channel | AP1 13.5 Mbps | Cheetah b 6 b 9 0 65% 1STAP b 6 b 9 0 4 60% Froaming2 b 6 b 9 0 4 60% SoftAP-br b 6 b 9 0 7 50% 160 b 6 b 9 0 60% 50% _SM5-192 b 6 b 9 0 39% | |
| ▶ ♦ 🗈 | Link Information | ✓ AP1 Image: bold symbol 7 Image: bold symbol 100% Ralink-Meeting-2591 Image: bold symbol 7 Image: bold symbol 10 Image: bold symbol 44% Accusys_LEO Image: bold symbol 10 Image: bold symbol 20% 20% VMIFI-51 Image: bold symbol 11 Image: bold symbol 65% | MILE |
| Status Extra Info Authentication Encryption | AP1 <> 00-0E-2E-E1-98-2D Link is Up [T× Power:100%] WPA2-P5K AE5 | VWIFI-S1 Image: Workshow of the state of th | |
| Network Type Central Channel | Infrastructure 5 | kkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk | 2 |

Figure 1-3 RaUI status with WZC active

When activating <u>WZC</u>, there are several difference with the RaUI status, compared to the RaUI status without <u>WZC</u> running.

- The profile button will be gray. Profile functionality is removed since the NIC is controlled by <u>WZC</u>.
- The Connect and Add Profile function will be gray. Profile functionality is removed since the NIC is controlled by <u>WZC</u>.

Please read through this document for full details on the other functions provided by RaUI.

1.1.2 Windows Zero Configuration (WZC)

• If there is no connection or it is lost, the status prompt will pop up, as shown in Figure 1-4.



Figure 1-4 status prompt for no connection

• Right-click the network connection icon in taskbar.



Figure 1-5 Select WZC main status

• Select "View Available Wireless Networks" and the "Wireless Network Connection" dialog box will pop up, as shown in Figure 1-6.



Figure 1-6 Wireless Network Connection

• Select the intended access point and click "Connect". Then click "Connect Anyway" as shown as Figure 1-7.

| (⁽⁰⁾⁾ Wireless Network Connect | ion 🛛 🔁 |
|--|--|
| Network Tasks | Choose a wireless network |
| 😴 Refresh network list | Click an item in the list below to connect to a <u>w</u> ireless network in range or to get more information. |
| Set up a wireless network for a home or small office | ((p)) RalinkInitialAP |
| | |
| Change advance Settings | Letwork Connection |
| | Security-enabled wireless network (WPA) |
| | Unsecured wireless network |
| | ((°)) APPA |
| | |

Figure 1-7 Select intended AP: AP1, then click "Connect"



Figure 1-8 Connect AP: AP1 successfully

• If you want to modify information about the AP, click "Change advanced settings" as shown in Figure 1-9. Then select the "Wireless Networks" tab shown as Figure 1-10.



Figure 1-9 Click "Change advanced settings"

| 🕂 Wireless Network Connection Properties 🛛 🛛 🛛 |
|--|
| General Wireless Networks Advanced |
| Use Windows to configure my wireless network settings |
| Available networks: |
| To connect to, disconnect from, or find out more information about wireless networks in range, click the button below. |
| View Wireless Networks |
| Preferred networks: Automatically connect to available networks in the order listed below: P AP1 (Automatic) Move up |
| Move <u>d</u> own |
| Add <u>R</u> emove <u>Properties</u> |
| Learn about <u>setting up wireless network</u> Ad <u>v</u> anced |
| OK Cancel |

Figure 1-10 Choose the "Wireless Networks" tab

• Click "Properties" as shown in Figure 1-11. Then click "OK" button.

| AP1 properties |
|--|
| Association Authentication Connection |
| Network <u>n</u> ame (SSID): AP1 |
| Wireless network key |
| This network requires a key for the following: |
| Network Authentication: Open |
| Data encryption: Disabled |
| Network key: |
| Confirm network key: |
| Key inde <u>x</u> (advanced): 1 |
| This is a <u>computer-to-computer</u> (ad hoc) network; wireless access points are not used |
| OK Cancel |



• After filling in the appropriate value, click "OK." The pop-up will indicate the status as shown in Figure 1-12.



Figure 1-12 Network connection status

• Clicking the Ralink icon will bring up the RaUI main window. Users can find the surrounding APs in the list. The currently connected AP will be shown with a blue icon beside it, as shown in Figure 1-13. Users may use the advanced tab to configure more advanced features provided by Ralink's wireless NIC. For details on configuring the advanced features, please check the Advance setting section.

| Ralink | (| | (i) ? × | 1 | | Site S | urvey | | | × |
|---|--|------------------------|--------------------------------|---|--|---------------------------------|----------------|----------|--|----------|
| (*)* SSID SSID Rate Channel | AP1 13.5 Mbps 7 (2442 MHz) | > IP Address > Mask | 192.168.2.101 255.255.255.0 | Cheeta 1STAP f-roam SoftAP 160 _SM5-1 | ing2 -br | 6 6 6 6 6 6 7 | 0000000 | | 65% 60% 50% 50% 60% 39% | |
| Status | Link Informatio | -98-2D | × | Ralink- Accusy VWIFI- VWIFI- | Meeting-2591 Is_LEO S1 S1 | で 10 10 10 11 11 | | | 44% 20% 65% 70% | |
| Authentication Encryption Network Type Central Channel | WPA2-P5K AES Infrastructure 5 | UU%] | | SortAP FTC-02 AMBITI kkkkkki AP Informa SSID | -98 88-A kkkkkkkkkk1 ation SoftAP-51 | | ib ib ib | ion Open | 81% 10% 0% 76% | ب |

Figure 1-13 Show connection status by using WZC to initiate the connection

1.2 Windows AutoConfig Service for Vista

1.2.1 Ralink Wireless Utility and Windows AutoConfig Service

In Windows Vista, the Auto Config service provides basic wireless configuration functions for the Ralink Wireless Network Interface Controller. In order to perform these functions, the Auto Config service should first be enabled (Refer to Section 1-2-2).

Once the Ralink wireless utility is minimized, click the Ralink icon as shown in Figure 1-1. This will bring up the option menu shown as Figure 1-2 for the user to restore the utility window or terminate the utility.



Figure 1-1





The Ralink wireless utility as shown in Figure 1-3, provides profile management, the available networks listing, a statistical counter display, Wi-Fi multimedia (WMM), protected Wi-Fi setup, Cisco compatible extensions (CCX), call admission control (CAC), radio controls, Ralink driver/utility information, and help functions.



Figure 1-3 Ralink Utility

The Ralink wireless utility starts in compact mode as shown in Figure 1-3. Clicking the expanding icon at the bottom-right corner can change to the full mode as shown in Figure 1-4.

| Ralink | | 00i ? × | 2 E | | Site Su | rvey | | | × |
|--|---|-----------------------|---|---------|------------------|---------------------------|--------------|---------------------------------|---|
| (1) SSID Rate | AP1 300.0 Mbps FIP | Address 192,168,2,101 | 118 SoftAP-33333 dlink-111 | 00000 | 2 2 2 3 | 69 69 69 | 000 | 65% 10% 70% 81% | |
| | Link Information | × | exx exx Baron_Test baldwin | 00000 | 5 6 6 6 | 09 09 09 | 0000 | 50% 39% 76% 96% 55% | |
| Status Extra Info Authentication Encryption | AP1 <> 00-0E-2E-E1-98-2 Link is Up [Tx Power: 100%] WPA2-PSK AES | 2D] | _wen RT305x_AP Stitch 1STAP _SMS-192 Cheetab | 0000000 | 6 6 6 6 | | 000000 | 39% 94% 94% 55% 0% | |
| Network Type Central Channel | Infrastructure 5 | | AP Information SSID 118 MAC Address 00-21-9 | 1-F7-A9 | -96 En | uthentication cryption | WPA2- AES | PSK | P |

Figure 1-4 Ralink Utility in full mode

1.2.2 Windows AutoConfig Service

The following steps outline the procedure for starting/stopping the Windows AutoConfig service.

Select "Control Panel" from "Settings" in the start menu



Double-click the "Administrative Tools" icon

| 🖁 Control Panel | | | | | | | | |
|------------------------------------|---------------------|---------------------------------------|--------------------------|-------------------------|--------------------------|---------------------|--------------------------|---|
| Control Panel - | | | | | 👻 🌆 Sear | ch | | 2 |
| Control Panel Home Classic View | Name - + | Category - Administrative Tools | AutoPlay | Backup and Restore | Color Management | Date and Time | Default Programs | |
| | Device Manager | Ease of Access Center | Folder Options | Fonts | Game Controllers | Indexing Options | Infrared | |
| | Internet Options | ISCSI Initiator | Keyboard | Mouse | Network and Sharing C | Offline Files | Pen and Input Devices | |
| | People Near Me | Performance Informati | Personaliza | Phone and Modem | Power Options | Printers | Problem Reports a | |
| | Program Updates | Programs and Features | Regional and Language | Scanners and Cameras | Security Center | Sound | Speech Recogniti | |
| | | | | | | 00 | | • |

Double-click "Services"

| the second | | | | | |
|---|--|--|---|--|---|
| 🌀 🕞 🗟 👻 Control P | anel 🝷 Administrative Tools | | - D | Search | 2 |
| Organize 👻 🔠 Views | + | | | - (4) | 0 |
| Favorite Links More >> Folders >> Desktop => Desktop => Public Computer Network Control Panel Administrative Tools Administrative Tools Administrative Tools Ease of Access Cent Fonts Network and Sharing Performance Informs Performance Informs Personalization Programs and Featur Speech Recognition | Name Computer Management Data Sources (ODBC) Event Viewer SiSCSI Initiator Local Security Policy Memory Diagnostics Microsoft .NET Fram Microsoft .NET Fram Print Management Reliability and Perfor Services System Configuration Task Scheduler Windows Firewall wit | Date modified 11/2/2006 8:54 PM 11/2/2006 8:53 PM 11/2/2006 8:54 PM 11/2/2006 8:54 PM 11/2/2006 8:55 PM 11/2/2006 8:53 PM 1/1/2100 9:39 AM 1/1/2100 10:20 AM 11/2/2006 8:55 PM 11/2/2006 8:53 PM | Type - Size Shortaut | 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB | |

Double-click "WLAN AutoConfig"

| File Action View | Help | | | | | | |
|---|---|---------------------|-------------|------------|--------------|---------------|----|
| () () () () () () () () () () | | | | | | | |
| Services (Local) | 🝳 Services (Local) | 141 | | | | | |
| | Select an item to view its description. | Name 🔺 | Description | Status | Startup Type | Log On As | |
| | | Windows Backup | Provides W | 24 million | Manual | Local System | |
| | | Windows CardSpace | Securely e | | Manual | Local System | |
| | | Windows Color Sys | The WcsPl | | Manual | Local Service | |
| | | Windows Connect | Act as a R | Started | Manual | Local Service | |
| | | 🔅 Windows Defender | Scan your | Started | Automatic | Local System | |
| | | Windows Driver Fo | Manages u | Started | Automatic | Local System | |
| | | 🔅 Windows Error Rep | Allows erro | Started | Automatic | Local System | |
| | | Windows Event Coll | This servic | | Manual | Network S | |
| | | Windows Event Log | This servic | Started | Automatic | Local Service | |
| | | Windows Firewall | Windows Fi | Started | Automatic | Local Service | |
| | | 🔅 Windows Image Ac | Provides im | Started | Automatic | Local Service | |
| | | 🔅 Windows Installer | Adds, modi | | Manual | Local System | |
| | | 🔍 Windows Managem | Provides a | Started | Automatic | Local System | |
| | | 🔄 Windows Media Pla | Shares Win | | Manual | Network S | |
| | | 🍓 Windows Modules I | Enables ins | | Manual | Local System | |
| | | 🔍 Windows Presentat | Optimizes | | Manual | Local Service | |
| | | 🔍 Windows Remote M | Windows R | | Manual | Network S | |
| | | Windows Search | Provides c | Started | Automatic | Local System | |
| | | 🔅 Windows Time | Maintains d | Started | Automatic | Local Service | |
| | | 🔅 Windows Update | Enables th | Started | Automatic (D | Local System | |
| | | 🔅 WinHTTP Web Prox | WinHTTP i | | Manual | Local Service | |
| | | Wired AutoConfig | This servic | | Manual | Local System | |
| | | WLAN AutoConfig | Dis servic | Started | Automatic | Local System | |
| | | WMI Performance | Provides p | | Manual | Local System | |
| | | Workstation | Creates an | Started | Automatic | Local Service | 14 |

Manage the AutoConfig properties in the dialog box

| AN AutoConfig | Properties (Local Computer) |
|------------------------------------|---|
| General Log On | Recovery Dependencies |
| Service name: | Wlansvc |
| Display name: | WLAN AutoConfig |
| Description: | This service enumerates WLAN adapters, manages WLAN connections and profiles. |
| Path to executat C:\Windows\sys | ole: stem32\svchost.exe +k LocalSystemNetworkRestricted |
| Startup type: | Automatic |
| Help me configu | re service startup options. |
| Service status: | Stopped |
| Start | Stop Pause Resume |
| You can specify from here. | the start parameters that apply when you start the service |
| Start parameters | |

Windows profile manager can be accessed via control panel or network connection icon in the task bar.

1. Access via network connection icon

Right-click the network connection icon in the taskbar, then select "Network and Sharing Center" from the pop-up menu



Select "Manage wireless networks" from the tasks list

| Control Panel 🕶 | Network and Sharing Center | 👻 🚱 Search | |
|--|--|--|---------------|
| Tasks View computers and devices Connect to a network Manage wireless networks Set up a connection or network Manage network connections Diagnose and repair | Network and Sharing Center SHUFEN-PC (This computer | | View full map |
| | 217 (Public network) | 1 | Customize |
| | Access | Local and Internet | |
| | 22 Sharing and Discovery | | |
| | Network discovery | © Off | • |
| | File sharing | ● Off | - |
| | Public folder sharing | © Off | - |
| | Printer sharing | Off(no printers installed) | - |
| | Password protected sharing | On On | • |
| See also | Media sharing | © Off | - |
| Infrared | Show me all the files and folders | I am sharing | |
| Internet Options | channel de chendre de la chend | E-Ideas as this second to a | |

Right-click the network to bring up the profile managing menu

| d Manage | Wireless Networks | | | _ _ × |
|--------------------------|--|---|--|-------------------------------|
| 00 | di → Control Panel → Manage Wireless Ne | tworks | 👻 🚺 Search | 2 |
| Mana Window remove | ge wireless networks that use (Wireless ws tries to connect to these networks in the ord e network profiles. | Network Connection) ler listed below. To change the orde | er, drag a network up or <mark>d</mark> own in | the list. You can also add or |
| Add 🕫 | 📼 Remove 🛛 🛞 Adapter properties 🛛 🔒 Pro | file types 🛛 🙀 Network and Sharii | ng Center | 0 |
| Networks | you can view and modify (1) | | | 8 |
| | Properties Remove network Rename | -c-nuerprise Type: | any supported | Automatically connect |
| N | 223 Profile name: 223 Security type: WPA2-Enterprise Radio type: Any supported | Mode: Automatically connect | | |

2. Access via control panel

Select "Control Panel" from the start menu



Double-click the "Network and Sharing Center" icon



| Network and Sharing Center | | | |
|--|---|--|---------------|
| Control Panel • N | letwork and Sharing Center | 👻 🚱 Search | P |
| Tasks | Network and Sharing Center | | 6 |
| View computers and devices Connect to a network Manage wireless networks Set up a connection or network Manage network connections | SHUFEN-PC (This computer |) 217 | View full map |
| Diagnose and repair | 217 (Public network) | | Customize |
| | Access | Local and Internet | |
| | Connection | Local Area Connection 2 | View status |
| | Sharing and Discovery Network discovery | © Off | |
| | File sharing | © Off | • |
| | Public folder sharing | © Off | • |
| | Printer sharing | Off(no printers installed) | - |
| | Password protected sharing | o On | • |
| See also | Media sharing | © off | • |
| Infrared Internet Options | Show me all the files and folders Show me all the shared network | I am sharing folders on this computer | |

Select "Manage wireless networks" from the tasks list

Right-click the network to bring up the profile managing menu

| Manage | Wireless Networks | | | _ [] × |
|--------------------------|--|---|--------------------------------------|---------------------------|
| 00 | aff] • Control Panel • Manage Wireless N | etworks | 👻 🐼 Search | 2 |
| Mana Window remove | ge wireless networks that use (Wireles ws tries to connect to these networks in the or e network profiles. | s Network Connection) der listed below. To change the orde | er, drag a network up or down in the | list. You can also add or |
| 🖧 Add 🛛 | 🗆 Remove 🛛 🛞 Adapter properties 🛛 🔒 Pi | ofile types 🛛 🙀 Network and Shari | ng Center | 0 |
| Networks | you can view and modify (1) | | | E |
| | Properties Remove network Rename | | | |
| L | 223 Profile name: 223 Security type: WPA2-Enterprise Radio type: Any supported | Mode: Automatically connect | | |

2. Ralink Wireless Utility (RaUI)

2.1 Start

2.1.1 Start RaUI

When starting RaUI, the system will connect to the AP with best signal strength without setting a profile or matching a profile setting. When starting RaUI, it will issue a scan command to a wireless NIC. After two seconds, the AP list will be updated with the results of a BSS list scan. The AP list includes most used fields, such as SSID, network type, channel used, wireless mode, security status and the signal percentage. The arrow icon indicates the connected BSS or IBSS network. The dialog box is shown in Figure 2-1.

| Ralink | (| |)() ? X | 1 | | Site Su | rvey | | | | × |
|--|--|------------------------|--------------------------------|---|---------|-----------------------|--------------------------|--------------|--------|--|-------|
| SSID SRate Channel | AP1 13.5 Mbps 7 (2442 MHz) | ⇒ IP Address ⇒ Mask | 192.168.2.101 255.255.255.0 | issue63 catch_me_if_you SoftAP-51 99 Claude0 iverson | 0000000 | 1 1 1 1 1 | | 0000 0 | ; | 70% 76% 76% 60% 55% 24% | - III |
| ⇒ ▲ ≡ | Link Informat | ion | × | pega2 dlink 001601D31484_G | じじじい | 2 3 5 6 | | 0 |) 7 | 39% 100% 44% 50% | |
| Status Extra Info Authentication Encryption | AP1 <> 00-0E-2E-E Link is Up [Tx Power WPA2-PSK AES | [1-98-2D :100%] | | Baron_Test 160 f-roaming2 RT305x_AP_BFu SPitch | >bbbbbb | 6 6 6 6 | | 99 99 | 7 | 99% 55% 50% 96% | 2 |
| Network Type Central Channel | Infrastructure 5 | | | AP Information SSID issue63 MAC Address 00-22-80-8 | 0-3C- | Au BF En | ithenticatio cryption | n WPA AES | 2-P5k | | U) |

Figure 2-1-1 RaUI section introduction

There are three sections to the RaUI dialog box. These sections are briefly described as follow.

Button Section: Include buttons for selecting the Profile page, Network page, Advanced page, Statistics page, WMM page, WPS page, the About button, Radio On/Off button and Help.



Figure 2-1-2 Button section

| A 🗈 | Link Information | ; |
|-----------------|----------------------------|---|
| Status | 4P1 <> 00-0E-2E-E1-98-2D | |
| Extra Info | Link is Up [Tx Power:100%] | |
| Authentication | WPA2-P5K | |
| Encryption | AES | |
| Network Type | Infrastructure | |
| Central Channel | 5 | |

Figure 2-1-3 Link Information page

| + - 🕑 😰 🖹 | Profile List | > |
|---------------------|----------------|-------|
| | | |
| | | |
| Profile Information | | |
| Profile Name | Authentication | ((2)) |

Figure 2-1-4 Profile page

| | | Site | Survey | | | | × |
|-----------------------|--------|------|----------------|-----------|----|------|-------------|
| issue63 | v | 1 | 69 | 0 | Ģ | 70% | ^ |
| _catch_me_if_you | 3 | 1 | 69 | 0 | \$ | 76% | |
| SoftAP-51 | 3 | 1 | 69 | Ô | | 76% | |
| <u>9</u> 9 | 3 | 1 | 69 | Ô | 8 | 60% | |
| Claude0 | 0 | 1 | 69 | | 8 | 55% | |
| iverson | 0 | 1 | 69 | 0 | | 24% | |
| pega2 | 0 | 2 | 69 | 1 | 67 | 39% | |
| dlink | 3 | 3 | 69 | 0 | | 100% | |
| 001601D314B4_G | B | 5 | 69 | | 8 | 44% | |
| _SMS-192 | 3 | 6 | 69 | 0 | | 50% | |
| Baron_Test | 3 | 6 | 69 | Ō | | 99% | |
| 160 | B | 6 | 69 | Ō | | 55% | |
| f-roaming2 | 3 | 6 | 6 | | 8 | 50% | |
| RT305x_AP_BFu | B | 6 | 69 | 0 | | 96% | |
| Stitch | 0 | 6 | 69 | Ó | 8 | 100% | V |
| AP Information | - | _ | | Million . | 20 | | |
| SSID wayne_5g | | | Authentication | Op | en | ((| cy) |
| MAC Address 00-0C-43- | 00-13- | -28 | Encryption | NO | NE | | 1 |

Figure 2-1-5 Network page

| Wireless Mode —Select Your Co | 2,4GHz + 5GHz | - | | | |
|----------------------------------|---------------|--------|------------|-----------|-------|
| 2.4GHz | 0: CH1-11 | - | | | |
| 5GHz | 3: CH 52, 5 | 6, 60, | 64, 149, 1 | .53, 157, | 161 💌 |
| | | | | | |

Figure 2-1-6 Advance page

| | Ab | out | |
|--------------------|------------|---------------------------------------|-------------------------|
| | | | |
| Version Utility | 4.0.0.0 | Date | 2010-03-07 |
| Driver | 1.4.9.0 | Date | 2009-11-26 |
| SDK | 1.0.4.0 | Date | 2010-03-04 |
| Firmware | 0.22 | EEPROM | 1.1 |
| MAC Address | 00-1C-: | 10-01-FE-1B | |
| Ralink | (c) Copyri | ght 2010, Ralink All rights reserv | Technology, Inc /ed. |

Figure 2-1-7 About page

When starting RaUI, a small Ralink icon appears in the notifications area of the taskbar, as shown in Figure 2-1-15. You can double click it to maximize the dialog box if you selected to close it earlier. You may also use the mouse's right button to close RaUI utility.



Figure 2-1-8 Ralink icon in system tray

Additionally, the small icon will change color to reflect current wireless network connection status. The status is shown as follows:



: Indicates the connected and signal strength is normal.

: Indicates that it is not yet connected.

: Indicates that a wireless NIC can not be detected.

R: Indicates that the connection and signal strength is weak.

2.2 Profile

2.2.1 Profile

The Profile List keeps a record of your favorite wireless settings at home, office, and other public hot-spots. You can save multiple profiles, and activate the correct one at your preference. Figure 2-2-1 shows the basic profile section.

| + - 📝 😭 🖹 | | × |
|-------------------------------------|----------------|-------|
| | | |
| | | |
| | | |
| Profile Information | | 1000 |
| Profile Information Profile Name | Authentication | (cp)) |

Figure 2-2-1 Profile function

Definition of each field:

- Profile Name: Name of profile, preset to PROF* (* indicate 1, 2, 3...).
- SSID: The access point or Ad-hoc name.
- Network Type: Indicates the networks type, including infrastructure and Ad-Hoc.
- Authentication: Indicates the authentication mode used.
- Encryption: Indicates the encryption Type used.
- Use 802.1x: Shows if the 802.1x feature is used or not.
- Cannel: Channel in use for Ad-Hoc mode.
- Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode.
- Tx Power: Transmitting power, the amount of power used by a radio transceiver to send the signal out.
- RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or keying in the value directly.

• Fragment Threshold: The user can adjust the Fragment threshold number by sliding the bar or key in the value directly.

Icons and buttons:

- *: Indicates if a connection made from the currently activated profile.
- \approx : Indicates if the connection has failed on a currently activated profile.

✤: Indicates the network type is infrastructure mode.

Indicates the network type is in Ad-hoc mode.

T: Indicates if the network is security-enabled.

+ : Click to add a new profile.

Elick to edit an existing profile.

Deletes an existing profile.

E: Import an existing profile.

Export an existing profile.

Activates the selected profile.

2.2.2 Add/Edit Profile

There are three methods to open the Profile Editor dialog box.

You can open it by clicking the "Add to Profile" button in the Site Survey tab. You can open it by clicking the "Add" button in the Profile tab.

You can open it by clicking the "Edit" button on the Profile tab.

| + + | Profile |
|--------------|--------------------------------------|
| Profile Name | PROF1 |
| SSID | |
| Network Type | Infrastructure - Connect to AP |
| | 🧿 Ad Hoc - Connect to other computer |

Figure 2-2-1 Add a new Profile

Icons and buttons:

- To the next page.
- Eack to the previous page.
- Cancel button.

| Profile Name | PROF1 |
|--------------|--------------------------------|
| | |
| SSID | |
| Network Type | Infrastructure - Connect to AP |
| Network Type | |

Figure 2-2-2 Profile Name, SSID, Network Configuration

- Profile Name: The user can chose any name for this profile, or use the default name defined by system.
- SSID: The user can key in the intended SSID name or select one of the available APs from the drop-down list.
- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Network Type: There are two types, infrastructure and 802.11 Ad-hoc modes. Under Ad-hoc mode, user can also choose the preamble type. The available preamble type includes auto and long. In addition, the channel field will be available for setup in Ad-hoc mode.

| Authentication | Open | • |
|----------------|------|---|
| Encryption | None | |
| | 1 | |

Figure 2-2-3 Authentication and Encryption Configuration

- Authentication Type: There are 7 types of authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK, 802.1X, WAPI-PSK, and WAPI-CA.
- Encryption Type: For open and shared authentication mode, the selection of available encryption type are none and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available.

| Default Tx Key | Key 1 | |
|----------------|--------------------------|---|
| Key Format | Hex(10 or 26 hex digits) | - |
| WEP Key | | |

Figure 2-2-4 WEP Key Configuration

- WEP Key: Only valid when using WEP encryption algorithms. The key must be identical to the AP's key. There are several formats to enter the keys.
- 1. Hexadecimal 40bits: 10 Hex characters.
- 2. Hexadecimal 128bits: 26 Hex characters.
- 3. ASCII 40bits: 5 ASCII characters.
- 4. ASCII 128bits: 13 ASCII characters.

| + + | Profile | |
|-------------------|---------|--|
| WPA Preshared Key | | |
| | | |
| | | |
| | | |

Figure 2-2-5 Pre-shared Key Configuration

• Pre-shared Key: This is the key shared between the AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

| * * | | |
|----------------------|-------------------|--------------------|
| EAP Method | PEAP 💌 | Session Resumption |
| unnel Authentication | EAP-MSCHAP v2 💌 | |
| Tunnel ID | Authentication ID | |
| Tunnel Password | | |
| Domain Name | | |

Figure 2-2-6 802.1x Configuration

• 802.1x Setting: This is introduced in the topic of "Section 3-2 : 802.1x Setting"

| ower Save Mode | CAM | |
|----------------------|-------|--|
| | C PSM | |
| Diagnostic Capabilit | Y | |



- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Channel: Only available for setting under Ad-hoc mode. Users can choose the channel frequency to start their Ad-Hoc network.
- RTS Threshold: User can adjust the RTS threshold number by sliding the bar, or key in the value directly. The default value is 2347.
- Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.

2.2.3 Example to Add Profile in Profile

• Click "Add" below the Profile List.

| + - 🛛 🕅 🕅 | | Ŷ |
|---------------------|----------------|-------|
| | | |
| Profile Information | Authentication | ((3)) |
| | | |

• The "Add Profile" will appear.

| Profile Name | PROF1 |
|--------------|--|
| SSID | |
| Network Type | Infrastructure - Connect to AP |
| | C Ad Hoc - Connect to other computer |

• Specify a Profile Name. Select an AP from the SSID drop-down list. The AP list from the last Network.

| Profile Name | PROF1 | |
|--------------|---|---|
| SSID | | - |
| Network Type | _catch_me_if_you_can _wen 001601D314B4_G 1234567 Accusys_LEO Accusys_LeO | < |

• Now the profile which the user set appears in the profile list. Click "Activate".

| + - 🏹 🛛 | 8 🕜 🔊 | Profile List | | × |
|----------------------|-------|------------------------------|---|------|
| PROF1 | AP1 | | 8 | ¢ |
| Profile Informati | on | | | |
| Profile Name SSID | | Authentication Encryption | | (2)) |

• Now the profile which the user active will connect to AP.

| | 0 |
|---------------------|------|
| Profile Information | 1000 |

2.2.4 Pre-logon Connect

The Pre-logon Connect configuration page as shown in Figure 2-2-4.

| Profile | × |
|--|---|
| Use Pre-logon Connection | |
| You need to restart the computer when using/non-using Pre-logon connection. (recommend) | |

Figure 2-2-4 Pre-logon Connect Page

Field definitions:

• Pre-logon Connect: Use ID and Password in Profile.

** Recommend: You need to restart the computer when using/non-using Pre-logon connection.

2.3 Network

2.3.1 Network

The system will display the information of local APs from the last scan result as part of the Network section. The Listed information includes the SSID, BSSID, Signal, Channel, Encryption algorithm, Authentication and Network type as shown in Figure 2-3-1-1.

| cert | 1 | 5 | 149 🧯 | a | 8 | 55% | ~ |
|----------------|-----------|---|-------|-------|-----|------|------|
| wayne_5g | Į | 5 | 161 🧯 | a | 0 | 39% | |
| 🖉 AP1 | 1 | 5 | 7 | 6 9 | 0 6 | 100% | |
| 001601D31 | 4B4_G | 5 | 5 | 6 9 | 1 9 | 50% | |
| 1STAP | 1 | 5 | 6 | 🍈 🔁 🧕 | 0 4 | 65% | |
| 160 | Į | 0 | 6 | i 🔁 🧐 | 0 | 34% | |
| Baron_Test | | 5 | 6 | 6 🛛 | 0 | 76% | |
| WXX | Į | 5 | 6 | 6 9 | 0 7 | 34% | |
| Stitch | 1 | 5 | 6 | 6 9 | 0 7 | 99% | |
| ExRegNW3 | 135DB 🛛 🕴 | 5 | 6 | 6 9 | 0 4 | 76% | |
| RT305×_AP | _BFu 🛛 🕴 | 5 | 6 | 6 9 | 0 | 94% | |
| f-roaming2 | Į | 5 | 6 | 6 | 8 | 55% | |
| cert | 1 | 3 | 6 | 6 9 | | 34% | |
| baldwin | Į | 3 | 6 | g | 0 9 | 50% | |
| Cheetah | Į | 5 | 6 | 6 9 | 0 | 44% | ~ |
| AP Information | | - | | | | | - 27 |

Figure 2-3-1-1 Network function

Definition of each field:

- SSID: Name of BSS or IBSS network.
- Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network
- Channel: Channel in use.
- Wireless Mode: AP support wireless mode. It may support 802.11a, 802.11b, 802.11g or 802.11n wireless mode.
- Security-Enable: Indicates if the AP provides a security-enabled wireless network.
- Signal: Receive signal strength of the specified network.

Icons and buttons:

✓: Indicates that the connection is successful.

♦ : Indicates the network type is in infrastructure mode.

- Indicates the network type is in Ad-hoc mode.
- \square : Indicates that the wireless network is security-enabled.
- a : Indicates 802.11a wireless mode.
- **b**: Indicates 802.11b wireless mode.
- **9**: Indicates 802.11g wireless mode.
- •: Indicates 802.11n wireless mode.

```
    Sorted by SSID
    Sorted by Channel
```

Somed by Channel

Sorted by Signal Strength : Indicate that the AP list is sorted by SSID, Channel or

Signal.

: Button to connect to the selected network.

EXAMPLE: Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

E: Adds the selected AP to the Profile setting. It will bring up a profile page and save the user's setting to a new profile.

Connected network:

- When RaUI first runs, it will select the best AP to connect to automatically.
- If the user wants to use another AP, they can click "Connect" for the intended AP to make a connection.
- If the intended network uses encryption other than "Not Use," RaUI will bring up the security page and let the user input the appropriate information to make the connection. Please refer to the example on how to fill in the security information.

When you double click an AP, you can see detailed information about that AP. The detailed AP information is divided into three parts. They are General, WPS, CCX information and 802.11n (The 802.11n button only exists for APs supporting N mode.) The introduction is as follows:

• General information contains the AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates. It is shown in Figure 2-3-1-2.

| cert | \$ | 149 <mark>a</mark> | | | 55% | |
|----------------|----|--------------------|---------------|------|------|---|
| wayne_5g | 0 | 161 <mark>a</mark> | 0 | | 39% | |
| 🖉 AP1 | 0 | 7 | 6 9 0 | 49 | 100% | |
| 001601D314B4_G | 0 | 5 | 69 | 8 | 50% | |
| 1STAP | 0 | 6 | 6 9 🛈 | 49 | 65% | |
| 160 | 0 | 6 | 6 9 🛈 | | 34% | |
| Baron_Test | 0 | 6 | 6 9 0 | | 76% | |
| WXX | 0 | 6 | 6 9 0 | 8 | 34% | |
| Stitch | 0 | 6 | 6 9 0 | 8 | 99% | |
| ExRegNW3135DB | \$ | 6 | 6 9 0 | 6 | 76% | |
| RT305x_AP_BFu | 0 | 6 | - 🕒 🧐 🛈 | 1.15 | 94% | |
| f-roaming2 | 3 | 6 | 6 | 8 | 55% | |
| cert | 0 | 6 | 69 | | 34% | |
| baldwin | 0 | 6 | 90 | 9 | 50% | |
| Cheetah | 3 | 6 | <u> 6 9 n</u> | 1 | 44% | 1 |

Figure 2-3-1-2 General information about the Access Point

2.3.2 Example on Adding Profile in Network

• Select the AP from the list on the Network tab

| cert | ø | 149 <mark>a</mark> | | | 55% | 1 |
|----------------|----|--------------------|-------------|------|------|----|
| wayne 5g | Ď | 161 <mark>a</mark> | 6 | 3 | 39% | |
| 🖉 AP1 | 3 | 7 | 690 | 141 | 100% | |
| 001601D314B4_G | Ø | 5 | 69 | 8 | 50% | 1 |
| 1STAP | 3 | 6 | 696 | 1 () | 65% | |
| 160 | 0 | 6 | 690 | 0 | 34% | |
| Baron_Test | \$ | 6 | 696 | 0 | 76% | |
| WXX | 3 | 6 | 690 | 1 9 | 34% | |
| Stitch | 3 | 6 | 696 | 9 | 99% | |
| ExRegNW3135DB | 0 | 6 | 690 | 1 () | 76% | |
| RT305x_AP_BFu | 0 | 6 | 690 | 0 | 94% | |
| f-roaming2 | 3 | 6 | 6 | 8 | 55% | |
| cert | 3 | 6 | B 9 | | 34% | |
| baldwin | 0 | 6 | 9 (| 8 | 50% | |
| Cheetah | \$ | 6 | 690 | | 44% | ~ |
| AP Information | | | | | | |
| SSID 1234567 | | Authe | ntication C | pen | ((| 23 |

• Click "Add to Profile"

| | | Site Sur | vey | | | × |
|------------------------------------|-------|---------------|---------------|--------|----------|----|
| Sti Add to Profile | b | 6 | 690 | 2 | 94% | ^ |
| f-roaming2 | Ď | 6 | 6 | 8 | 70% | |
| RT305x_AP_BFu | B | 6 | - 🖲 🖸 f | 1 | 34% | |
| WXX | 0 | 6 | 690 | 8 | 44% | |
| SoftAP-br | 3 | 6 | 690 | 8 | 39% | |
| Baron_Test | 3 | 6 | 690 | | 55% | |
| 160 | 3 | 6 | 690 | 1 | 29% | |
| baldwin | 3 | 6 | 90 | 19 | 44% | |
| 1STAP | 3 | 6 | 690 | 4 | 70% | |
| Cheetah | 3 | 6 | 690 | | 44% | |
| ExRegNW3135DB | 3 | 6 | 690 | 14 | 94% | |
| AP1 | Ø | 7 | 01910 | 6 | 100% | |
| kkkkkkkkkkkkkkkkkk | 3 | 11 | 690 | | 76% | |
| test_ssid | 0 | 11 | 690 | 1 | 50% | |
| RedStone | 3 | 11 | 69 | 8 | 0% | ~ |
| AP Information | | | | | | |
| SSID AP1 MAC Address 00-0E-2E-E | 1-98- | Aut 2D End | hentication W | /PA-PS | ік ES | 2) |

• The System section will appear at the bottom of the Add Profile window. You can specify your own profile name.

| Profile Name | PROF1 |
|--------------|--------------------------------------|
| SSID | AP1 |
| Network Type | Infrastructure - Connect to AP |
| | C Ad Hoc - Connect to other computer |

• Next, you will see the new profile in the profile list. Click "Activate"

| | Site Survey | × |
|--|---|---|
| SSID AP1 Rate 13.5 Mbps IP Address 192.168.2.101 Channel 7 (2442 MHz) Mask 255.255.255.0 | Stitch Ø 6 Ø 94% F-roaming2 Ø Ø 70% RT305x_AP_BFu Ø Ø Ø 34% WXX Ø Ø Ø 7 44% SoftAP-br Ø Ø Ø 9 9 94% Baron Test Ø Ø Ø Ø 9 99% 55% | |
| Profile List × | 160 160 160 160 160 160 160 160 160 160 160 160 160 160 14% 1STAP 160 <td></td> | |
| Profile Information Profile Name PROF1 Authentication WPA2-P5K | AP1 7 9 0 41 100% kkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk | • |

2.4 Advanced

2.4.1 Advanced

Figure 2-4 shows the Advance functions of RaUI.

| Wireless Mode -Select Your Cor | 2.4GHz + 5GHz |
|-----------------------------------|--|
| 2.4GHz | 0: CH1-11 |
| 5GHz | 3: CH 52, 56, 60, 64, 149, 153, 157, 161 💌 |
| | |
| | |
| | |
| | |
| | |

Figure 2-4 Advance function

- Wireless mode: Select wireless mode. 2.4G, 5G and 2.4+5G are supported.(2.4G/5GHz options are depend on different products)
- Wireless Protection: Users can choose from Auto, on, and off. (This is not supported by 802.11n adapters.)

Auto: STA will dynamically change as AP announcement.

On: The frames are always sent with protection.

Off: The frames are always sent without protection.

- TX Rate: Manually select the transfer rate. The default setting is auto. (802.11n wireless cards do not allow the user to select the TX Rate.)
- Enable TX Burst: Ralink's proprietary frame burst mode.
- Enable TCP Window Size: Optimize the TCP window size to allow for greater throughput.
- Fast Roaming at-: enables fast roaming, which is set by the transmit power.
- Select Your Country Region Code: There are eight countries to choose from in the country channel list. (11A ListBox only shows for 5G adapters.)
- Show Authentication Status Dialog: When you connect to an AP with authentication, choose whether show the "Authentication Status Dialog" or not. The Authentication Status Dialog displays the processes during 802.1x authentication.
- Apply the above changes.

2.4.2 Certificate Management

The Certificate Management configuration page as shown in Figure 2-4-2.

| Install Certificate | | |
|---------------------|---------|------------|
| User certificate | | Browse |
| Issuer certificate | | Browse |
| | Install | |
| | | UpMove |
| | | DownMove |
| | | Install AS |
| | | Delete |
| | | |

Figure 2-4-2 Certificate Management function

2.5 Link Information

2.5.1 Link Status

The link status page displays detailed information about the current connection as shown in Figure 2-5-1.

| Status | AP1 <> 00-0E-2E-E1-98-2D | |
|-----------------|----------------------------|--|
| Extra Info | Link is Up [Tx Power:100%] | |
| Authentication | WPA2-PSK | |
| Encryption | AES | |
| Network Type | Infrastructure | |
| Central Channel | 5 | |

Figure 2-5-1 Link Status function

- Status: Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.
- Extra Info: Display link status in use.
- Channel: Display current channel in use.
- Authentication: Authentication mode in use.
- Encryption: Encryption type in use.
- Network Type: Network type in use.
- IP Address: IP address about current connection.

2.5.2 Throughput

The throughput page displays detailed information about the current connection as shown in Figure 2-5-2.

| tint. A shirt | 1.11 | | 100.9/ |
|------------------------|------------|-----------------------|-----------|
| Link Quality | | | 100 % |
| Signal Strength | 1 | | 41 dBm |
| Signal Strength : | 2 | | -/6 dBm |
| | | | |
| Transmit | | Deseive | |
| Transmit | 10 5 Mbc - | Receive | DO O Mhas |
| Transmit Link Speed | 13.5 Mbps | Receive Link Speed | 39.0 Mbps |

Figure 2-5-2 Throughput function

- Link Speed: Show current transmit rate and receive rate.
- Throughout: Display transmits and receive throughput in unit of Mbps.
- Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.
- Signal Strength 1: Receive signal strength 1, user can choose to display as percentage or dBm format.
- Signal Strength 2: Receive signal strength 2, user can choose to display as percentage or dBm format.
- Signal Strength 3: Receive signal strength 3, user can choose to display as percentage or dBm format.

2.5.3 Statistics

The Statistics page displays detailed counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for the user to understand. Figure 2-5-1 shows the detailed page layout.

| Transmit C Receive | | Reset Counter |
|---------------------------------------|---|---------------|
| Transmitted Successfully | = | 2613 |
| Retransmitted Successfully | = | 260 |
| Fail To Receive ACK After All Retries | = | 735 |

Figure 2-5-1 Statistics function

Transmit Statistics:



- Frames Transmitted Successfully: Frames successfully sent.
- Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.
- RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.
- RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.
- Frames Retransmitted Successfully: Successfully retransmitted frames numbers.
- Reset counters to zero.

Receive Statistics:

| Link Inform | nation | |
|--------------------------------|--------|---------------|
| 🔿 Transmit 🛛 💽 Receive | | Reset Counter |
| Received Successfully | = | 1152 |
| leceived With CRC Error | = | 375989 |
| Dropped Due To Out-of-Resource | = | 0 |
| Duplicate Frames Received | - | 0 |

- Frames Received Successfully: The number of frames successfully received.
- Frames Received With CRC Error: The number of frames received with a CRC error.
- Frames Dropped Due to Out-of-Resource: The number of frames dropped due to a resource issue.
- Duplicate Frames Received: The number of duplicate frames received.
- Reset all the counters to zero.

2.6 About

2.6.1 About

Click "About" displays the wireless card and driver version information as shown in Figure 2-10.

| ~ | (c) Copyri | ght 2010, Ralink | Technology, Ir |
|--------------------|------------|------------------|----------------|
| MAC Address | 00-1C-1 | 10-01-FE-1B | |
| Firmware | 0.22 | EEPROM | 1.1 |
| SDK | 1.0.4.0 | Date | 2010-03-04 |
| Driver | 1.4.9.0 | Date | 2009-11-26 |
| Version Utility | 4.0.0.0 | Date | 2010-03-07 |

Figure 2-10 About function

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

2.7 WPS

2.7.1 WPS

Figure 2-7-1 illustrates the RaUI WPS functions.

| + - 📝 😰 📝 | Profile List | 3 |
|-------------------------------------|-----------------|-------|
| | Add WPS Profile | |
| | | |
| | | |
| | | |
| Profile Information | | |
| Profile Information Profile Name | Authentication | ((2)) |



- WPS Configuration: The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. Ralink STA supports the configuration and setup using a PIN configuration method or a PBC configuration method through an internal or external Registrar.
- WPS AP List: Displays the SSID of the surrounding APs with WPS IE from the last scan result.
- PBC: Start to add to AP using PBC configuration method.
- PIN: Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
- Auto: Starts to add to AP by using to select the AP automatically in PIN method.

| WPS AP List | | Auto |
|-------------|--------------------------------|------|
| WPS Method | Push-Button Configuration(PBC) | |
| | 🧭 PIN / numeric code | |

Figure 2-7-1-1 WPS Profile

- PIN Code: The user is required to enter an 8-digit PIN Code into Registrar. When an STA is the Enrollee, you can click "Renew" to re-generate a new PIN Code.
- Config Mode: The station serving as an Enrollee or an external Registrar.

| onfig Mode Registrar 🗨 WPS Profile | Pin Code 381331 | 7 | Ren | iew |
|------------------------------------|--------------------|----|-----|-------------|
| | onfig Mode Registr | ar | J 📃 | WPS Profile |
| | - J | | | |

Figure 2-7-1-2 WPS PIN function

After the user clicks PIN or PBC, please do not rescan within two-minutes of the connection. If you want to abort this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.

- Progress Bar: Displays the rate of progress from Start to Connected.
- Status Bar: Displays the current WPS Status.

There are examples in <u>section 2-7-3</u>(PIN Enrollee Setup), <u>section 2-7-4</u>(PBC Enrollee Setup) and <u>section 2-7-5</u>(Registrar Configures and AP)

2.7.2 Example to Add to Registrar Using PIN Method

The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. The following image outlines the process.



• Select an AP (SSID/BSSID) that STA will join to and Select the "PIN/numeric code" method.



- Select "Enrollee" from the Config Mode drop-down list.
- Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.

| Pin Code 3813317 |
|-----------------------------------|
| onfig Mode Enrollee 💽 WPS Profile |

If you use <u>Microsoft Window Connection Now</u> as an External Registrar, you must start PIN connection at STA first. After that, search out your WPS Device name and MAC address at Microsoft Registrar. Add a new device and enter PIN Code of STA at Microsoft Registrar when prompted.

• Click "PIN" to enter the PIN

| | | 11.07 | |
|----------------|----------------|----------------|----------------|
| | | 0 % | |
| is is not used | | | |
| | | | |
| L | us is not used | us is not used | us is not used |

• The result should appear as the image below.

| | | 15 % | |
|----------------|----------------------|------|--|
| PIN - Begin as | ssociating to WPS AP | | |
| | | | |

• Configure one or more credentials

| _ | | 40 % | |
|------------|---------|------|--|
| PIN - Send | ding M1 | | |
| | | | |

• Then connect successfully. The result appears as the following image.

| • | Profile | | × |
|-----------------|-----------------------|-------|---|
| | | 100 % | |
| PIN - Get WPS (| profile successfully. | | |
| | | | |

• Click "Finish"



Describe "WPS Status Bar" - "PIN - xxx" as follow:

• Acceptable PIN Configurations:

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Req (Start) ~> Sending M1 ~> Received M2 ~> (Received M2D ~> Sending EAP-Rsp (ACK)) ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp(Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

- WPS configuration doesn't complete after a two-minute connection: WPS EAP process failed.
- When errors occur within two minutes of connecting, the WPS status bar might report "WPS EAP process failed".

Error messages might be:

- 1. Receive EAP with wrong NONCE.
- 2. Receive EAP without integrity.
- 3. Error PIN Code.
- 4. An inappropriate EAP-FAIL received.

2.7.3 Example to Add to Registrar Using PBC Method

The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If there is only one Registrar in PBC mode, the PBC mode selected is obtained from ID 0x0004, and is found after a complete scan. The Enrollee can then immediately begin running the Registration Protocol.

If the Enrollee discovers more than one Registrar in PBC mode, it MUST abort its connection attempt at this scan and continue searching until the two-minute timeout.

*Before you press PBC on STA and candidate AP. Make sure all APs aren't PBC mode or APs using PBC mode have left their Walk Time.

Push PBC button on both Registrar and Enrollee



• Select an AP (SSID/BSSID) that STA will join to and Select the "Push-button Configuration" method.

| WPS AP List | 💽 🔽 At | ito |
|-------------|--------------------------------|-----|
| WPS Method | Push-Button Configuration(PBC) | |
| | 🦳 PIN / numeric code | |

- Click PBC to start the PBC connection.
- Push the PBC on AP.

| | | 0% | |
|---------------|----------|------|--|
| | | 0 /0 | |
| WPS status is | not used | | |
| | | | |

• The progress bar as shown in the figure below indicates that scanning progress.

| - | | 10.9/ | |
|------------|---------|-------|--|
| - | | 10 % | |
| PBC - Scan | ning AP | | |
| | | | |

• When one AP is found, join it.

| _ | _ | 70.0/ | |
|---------------|------|-------|--|
| | | /0 /8 | |
| PBC - Sending |) M5 | | |

• Configure and receive one or more credential(s).

| Profile | × |
|--------------------------|--------------------------------------|
| | 100 % |
| PS profile successfully. | |
| | |
| Finish | |
| | ² S profile successfully. |

• Then connect successfully. The result will be displayed as it is in the figure below.

| R | Ralink | (| |)() ? × |
|----------------------------|---|----------------------------------|------------------------|--------------------------------|
| ۳» ک سال | SSID Rate Channel | AP1 54.0 Mbps 7 (2442 MHz) | ⇒ IP Address ≫ Mask | 192.168.2.101 255.255.255.0 |
| + - | DF1 | Profile L D | ist | ه ۵ × |
| Profile Profile SSID | Information Name PROF 4P1 | 1 Aut | hentication WPA | 12-P5K |

Describe "WPS Status Bar" - "PBC - xxx" as follow:

• A successful PBC Configuration:

Start PBC connection ~> Scanning AP ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Rsp (Start) ~> Sending M1 ~> Received M2 ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp (Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

• No PBC AP available:

Scanning AP ~> No PBC AP available ~> Scanning AP ~> No PBC AP available ~>...

• Too Many PBC AP available:

Scanning AP ~> Too Many PBC AP available ~> Scanning AP ~> Too Many PBC AP available ~>...

• WPS configuration doesn't complete after **two-minute connection**: WPS EAP process failed.

• When Errors occur within two-minutes of establishing a connection, the WPS status bar might report "WPS EAP process failed".

Error messages might be:

- 1. Receive EAP with wrong NONCE.
- 2. Receive EAP without integrity.
- 3. An inappropriate EAP-FAIL received.

Describe "Multiple PBC session overlaps" as follow:

• Dual bands:

AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

AP2 is a A-Band AP using PBC mode. (ID = 0x0004)

They have the same UUID-E.

STA would regard these two APs as a dual-radio AP and select one band to connect.

• Different UUID-E :

AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

AP2 is a G-Band AP using PBC mode. (ID = 0x0004)

They have the different UUID-E.

STA would regard these two APs as two different APs and wait until only one PBC AP is available.



Push PBC button on both Registrar and Enrollee

Select an AP (SSID/BSSID) that STA will config and Select the "PIN/numeric code" method.



- Select "Registrar" from the Config Mode drop-down list.
- Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.

| | Pin Code | 31289207 | Renew |
|-----------------------------------|-------------|-----------|-------------|
| nfig Mode Registrar 💌 WPS Profile | Config Mode | Registrar | WPS Profile |

• Enter the details of the credential and change configurations (SSID, Authentication, Encryption and Key) manually if needed.

| | | | _ |
|----------------|-------------------|---|---|
| SSID | ExRegNW01FE1B | | |
| BSSID | 00-0E-2E-E1-98-2D | | |
| Authentication | WPA2-PSK | • | |
| Encryption | AES | - | |

- Start PIN or PBC. The following procedures are as similar as <u>section 2-7-3</u> (PIN Enrollee Setup) or <u>section 2-7-4</u>(PBC Enrollee Setup),
- If your AP Enrollee has been configured before the WPS process, the credential you set in advance will be updated to the AP itself. Otherwise, after a successful registration, the AP Enrollee will be re-configured with the new parameters, and the STA Registrar will connect to the AP Enrollee with these new parameters.

Describe "WPS Status Bar" - "PIN - xxx" as follow:

A successful PIN Configuration:

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~> Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~> Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

Describe "WPS Status Bar" - "PBC - xxx" as follow:

A successful PBC Configuration:

```
Start PBC connection ~> Scanning AP ~> Begin associating to WPS AP ~>
Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~>
Receive M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~>
Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~>
Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS
status is connected successfully-SSID
```

3. Security

| Authentication | Open | |
|----------------|------|---|
| Encryption | None | - |
| | | |

3.1 Auth.\ Encry. Setting – WEP/TKIP/AES

Figure 3-1 Auth.\Encry. Settings in the Profile Page

- Authentication Type: There are 7 authentication modes supported by RaUI. They are Open, Shared, WPA and WPA-PSK, WPA2 and WPA2-PSK, 802.1x, WAPI-PSK and WAPI-CA.
- Encryption Type: For open and shared authentication mode, the available encryption types are none and WEP. For Shared and 802.1x authentication mode, the selection of available encryption is WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available. For WAPI-PSK and WAPI-CA authentication mode, only SMS4 encryption is available.

| Authentication | 802.1X | • |
|----------------|--------|---|
| Encryption | WEP | • |
| | | |

Figure 3-1-2 Authentication \ Encryption Settings in the Profile Page • 8021X: This is introduced in the topic of <u>Section 3-2</u>.

| ++ | Profile | \$ |
|-------------------|---------|----|
| WPA Preshared Key | | |
| | | |
| | | |
| | | |

Figure 3-1-3 Pre-shared Key Configuration

• Pre-shared Key: This is the shared key between the AP and STA. If operating in WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

| Default Tx Key | Key 1 | - |
|----------------|--------------------------|---|
| Key Format | Hex(10 or 26 hex digits) | - |
| WEP Key | | |

Figure 3-1-4 WEP Key Configuration

- WEP Key: Only valid when using WEP encryption algorithm. The key must match the AP's key. There are several formats to enter the keys.
 - 1. Hexadecimal 40bits: 10 Hex characters.
 - 2. Hexadecimal 128bits: 32Hex characters.
 - 3. ASCII 40bits: 5 ASCII characters.
 - 4. ASCII 128bits: 13 ASCII characters.

3.2 802.1x Setting

802.1x is used for authentication of the "WPA" and "WPA2" certificate by the server.

| EAP Method | PEAP | - | Session Resumption |
|----------------------|-------------------|---|--------------------|
| unnel Authentication | EAP-MSCHAP v2 | • | |
| Tunnel ID | Authentication II | | |
| Tunnel Password | | | |
| Domain Name | | | |

Authentication type:

- PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authenticates 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.
- 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.
- 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.
- EAP-FAST: Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication.
- LEAP: Light Extensible Authentication Protocol is an EAP authentication type used primarily by 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.(Only support XP)

Session Resumption: The user can choose "Disable" and "Enable".

Tunnel Authentication:

- Protocol: Tunnel protocol, List information include "EAP-MSCHAP v2", "EAP-TLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS-CHAP-V2", "PAP" and "EAP-MD5".
- Tunnel Identity: Identity for tunnel.

• Tunnel Password: Password for tunnel.

ID \ PASSWORD

- Authentication ID/Password: The identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain names can be keyed in the blank space.
- Tunnel ID/Password: Identity and Password for the server..

Client Certification



Use Client certificate: Client certificate for server authentication. **EAP Fast**

| Allow unauthenticated | provision mode |
|------------------------|-------------------|
| Provisioning Tunnel | AP-MSCHAP v2 |
| 🔽 Use protected authen | cation credential |
| | Import |
| | Remove |

- Allow unauthenticated provision mode: During the PAC can be provisioned (distributed one time) to the client automatically. It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server.
- Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method.

Server Certification

| | artification | |
|----------------|--|---|
| T Use berver c | ercincation | - |
| Allow inte | rmidiate certificates | |
| Server Name | | - |
| | Serve name must match exactly | |
| | C Domain name must end in specified name | |

- Certificate issuer: Select the server that issues the certificate.
- Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the "certificate issuer must be" field.
- Server name: Enter an authentication sever root.

3.3 Example to Configure Connection with WEP on

• Select an AP with WEP encryption and click "Connect".

| baldwin | 0 | 6 | 9 | 0 7 | 39% | |
|---------------------|---|--------------------|--------|----------|------|--|
| AP1 | 0 | 7 | 09 | 0 6 | 100% | |
| Ralink-Meeting-2591 | 0 | 7 | 69 | 0 () | 39% | |
| ClaudeAP | 0 | 11 | 69 | 8 | 55% | |
| WAPI_Cert | 0 | 11 | 9 | 0 | 29% | |
| kkkkkkkkkkkkkkkk | 0 | 11 | 69 | 0 | 60% | |
| VWIFI-S1 | 0 | 11 | 69 | 8 | 70% | |
| test_ssid | 0 | 11 | 69 | 0 | 44% | |
| | 0 | 11 | 69 | 0 () | 60% | |
| Sam_AP | 3 | 64 <mark>a</mark> | | 0 | 42% | |
| cert | 0 | 149 <mark>a</mark> | | <u> </u> | 29% | |
| wayne_5g | 0 | 161 <mark>a</mark> | | 0 | 44% | |
| lalala | 0 | 161 <mark>a</mark> | | 0 | 24% | |
| ppp | 4 | 1 | 69 | | 15% | |
| SoftAP-FE | 0 | 1 | 69 | 0 | 70% | |
| AP Information | 3 | | 15 125 | | | |

• The Auth.\Encry. function will appear as below;

| Ralink | ■ D ⊘ © i ? × | Site Survey | × |
|-------------------------|--|---|---|
| SSID Rate Channel | 1234567 36.0 Mbps IP Address 192.168.1.108 1 (2412 MHz) Mask 255.255.255.0 | dlink ½ 3 10 9 0 81% _SM5-192 ½ 6 10 9 0 39% Cheetah ½ 6 10 9 0 44% ExRegNW3135DB ½ 6 10 9 0 61% Baron_Test ½ 6 10 9 0 86% | |
| = + + | Profile X | Stitch Image: boot stitch | - |
| Encryption | WEP | AP1 V 7 9 0 47 100% Ralink-Meeting-2591 V 7 9 0 47 39% ClaudeAP V 11 9 55% 55% WAPI_Cert V 11 9 29% | |
| | | SSID AP1 Authentication Open MAC Address 00-0E-2E-E1-98-2D Encryption WEP | ŋ |

• Enter 1234567890 in the Key#1 Hexadecimal field. This value is same as our intended AP's setting.

| | Site Survey | × |
|--|--|---|
| S5ID 1234567 Rate 36.0 Mbps IP Address 192.168.1.108 Channel 1 (2412 MHz) Mask 255.255.0.0 | dlink Ø 3 Ø 0 81% _SM5-192 Ø 6 Ø 0 39% Cheetah Ø 6 Ø 0 44% ExRegNW3135DB Ø 6 Ø 0 41% Baron_Test Ø 6 Ø 0 6% RT305x_AP_BFu Ø 6 Ø 0 76% | |
| Profile X Default Tx Key Key 1 | Stitch Ø 6 Ø 0 91% wxx Ø 6 Ø 0 7 39% 1STAP Ø 6 Ø 0 1 44% 000 Ø 6 Ø 0 1 44% baldwin Ø 6 Ø 0 7 39% | |
| Key Format Hex(10 or 26 hex digits) | API 100% Ralink-Meeting-2591 7 b 9 0 4 39% ClaudeAP 11 b 9 55% WAPI_Cert 11 9 29% API Information SSID API Authentication Open MAC Address 00-0E-2E-E1-98-2D Encryption WEP | • |

• Click "OK". The dialog box will appear as below;

| | Silte Survey | × |
|--|---|---|
| SSID AP1 Rate 11.0 Mbps IP Address 192.168.2.101 Channel 7 (2442 MHz) Mask 255.255.255.0 | dlink b 3 9 1 81% _SMS-192 b 6 9 1 39% Cheetah b 6 9 1 44% EXRegNW3135D8 b 6 9 1 44% Baron_Test b 6 9 1 86% RT305x_AP_BFu b 6 9 1 76% | |
| Link Information X | Stitch 10 6 10 9 10 9 1% wxx 1/2 6 10 9 10 7 39% 1STAP 1/2 6 10 9 10 1 44% 000 1/2 6 10 9 81% | |
| Status AP1 <> 00-0E-2E-E1-98-2D Extra Info Link is Up [Tx Power:100%] Authentication Open Encryption WEP | baldwin Image: boldwin Image: boldwi | |
| Network Type Infrastructure | AP Information SSID AP1 Authentication Open MAC Address 00-0E-2E-E1-98-2D Encryption WEP | Ď |

3.4 Example to Configure Connection with WPA-PSK

- Site Survey × 2 000 ^ Cheetah 0 55% 6 č g 0 RT305x_AP_BFu 6 86% 9 0 ExRegNW3135DB 6 99% 49 **9** 0 Ō 6 WXX 8 44% 6 g RT61AP_Z 29% baldwin 6 29% O V AP1 b \square 100% もし 9 🛈 💔 1STAP 6 39% 000 90 NAP2-WEP-197 8 Ø 20% g 0 11 55% test_ssid g **VWIFI-S1** 11 76% b **VWIFI-S1** 11 g 0 39% Ō g 11 ClaudeAP 65% Ь FTC-02 11 g 34% 11 g RT2860AP1 Ь 0 24% * **AP Information** SSID AP1 Authentication WPA-PSK... TKIP+AES MAC Address 00-0E-2E-E1-98-2D Encryption
- Select the AP with a WPA-PSK authentication mode and click "Connect".

• Auth.\Encry. function appears.

| Ralink | | Site Survey | × |
|----------------|-----------------------|---|---|
| SSID Rate | RT2860AP1 1.0 Mbps | 001601D31484_G ½ 5 ½ 9 7 50% Stitch ½ 6 ½ 9 1 7 86% Baron_Test ½ 6 ½ 9 0 86% Cheetah ½ 6 ½ 9 0 55% RT305x 4P PE 4 6 ½ 9 0 56% | |
| ■ + + | Profile X | ExRegNW3135DB 0 6 5 9 0 47 99% wxx 0 6 5 9 0 7 44% RT61AP_Z 0 6 5 9 7 29% baldwin 0 6 9 0 7 29% | |
| Authentication | WPA2-P5K | AP1 P 7 P 9 10% 1STAP P 6 P 9 10% NAP2-WEP-197 P 8 P 1 39% test_ssid P 11 P 0 55% WWIFI-S1 P 11 P 76% WWIF1-S1 P 11 P 0 39% | • |
| | | AP Information SSID AP1 Authentication WPA-PSK MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES | 9 |

• Select WPA-PSK as the Authentication Type. Select TKIP or AES encryption. Enter the WPA Pre-Shared Key as "12345678".

| | Site Survey | × |
|--|---|---|
| Image: SSID RT2860AP1 Image: SSID RT2860AP1 Image: SSID RT2860AP1 Image: SSID Image: SSID Image: SSID <t< th=""><th>001601D314B4_G 0 5 0 9 7 50% Stitch 0 6 0 9 1 86% Baron_Test 0 6 0 9 0 86% Cheetah 0 6 0 9 0 55% RT305x_AP_BFu 0 6 0 9 0 86% ExcegtW3135DB 0 6 0 9 0 47 99%</th><th></th></t<> | 001601D314B4_G 0 5 0 9 7 50% Stitch 0 6 0 9 1 86% Baron_Test 0 6 0 9 0 86% Cheetah 0 6 0 9 0 55% RT305x_AP_BFu 0 6 0 9 0 86% ExcegtW3135DB 0 6 0 9 0 47 99% | |
| Profile X | wxx 6 5 9 7 44% RT61AP_Z 6 5 9 7 29% baldwin 6 9 7 29% | |
| WPA Preshared Key ****** | AP1 7 9 9 100% 1STAP 6 9 4 39% NAP2-WEP-197 8 9 7 20% test_ssid 11 9 7 5% WWIFI-S1 11 9 7% 7% | |
| | AP Information SSID AP1 Authentication WPA-PSK MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES | 2 |

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

| Ralink | D Ø Ø (1) ? × | Site Survey | × |
|--|--|--|---|
| SSID Rate Channel | AP1 270.0 Mbps IP Address 192.168.2.101 7 (2442 MHz) Mask 255.255.255.0 | 001601D314B4_G Ø 5 Ø 7 50% Stitch Ø 6 Ø Ø 7 86% Baron_Test Ø 6 Ø Ø 86% Cheetah Ø 6 Ø Ø 86% RT305x_AP_BFu Ø 6 Ø Ø 86% ExRegNW3135DB Ø 6 Ø Ø 1 99% | |
| ⊳ ∧ ∎ | Link Information X | wxx Image: bold win | |
| Status Extra Info Authentication Encryption Network Type | AP1 <>00-0E-2E-E1-98-2D Link is Up [Tx Power:100%] WPA2-P5K AES Difractructure | 1STAP Image: Constraint of the sector of t | * |
| Central Channel | 5 | AP Information SSID AP1 Authentication WPA-PSK MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES | ッ |

3.5 Example to Configure Connection with WPA

Site Survey × 2 RT61AP_Z 69 8 29% ~ 6 Ď 90 2 baldwin 6 29% Ċ AP1 7 q 0 100% 9 0 1STAP 6 49 39% 0 NAP2-WEP-197 8 2 20% g 0 🤣 test_ssid 11 55% りりりりりり g **VWIFI-S1** 11 76% ğ 0 **VWIFI-S1** 11 39% g ClaudeAP 11 65% g FTC-02 34% 11 ğ 0 RT2860AP1 11 24% g นนนนน 11 29% Ô 64 a 42% Sam_AP 149 <mark>a</mark> cert 10% lalala 161 **a** ۵ 15% AP Information Authentication WPA SSID AP1 MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES

• Select an AP with WPA authentication mode and click "Connect".

• The Auth.\Encry. function pop up. (If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.)

| Ralink | | Site Survey | × |
|------------------------------|-----------------------|--|---------|
| SSID Rate Channel | test_ssid 6.5 Mbps | RT61AP_Z baldwin compare compare <thcompare< th=""> <thcompare< th=""></thcompare<></thcompare<> | |
| = + + | Profile X | WWIFI-51 Image: Market for the state s | |
| Authentication Encryption | WPA | RT2860AP1 V 11 V V 24% uuuuu V 11 V 0 4 29% Sam_AP V 64 0 7 42% cert V 149 0 10% | |
| | | Ialala 161 161 15% AP Information SSID AP1 Authentication WPA MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES | • 10 |

• Click "8021X" and the setting page will appear.

| | Site Survey | × |
|---|--|----------|
| SSID test_ssid Rate 6.5 Mbps IP Address 192.168.1.18 Channel 11 (2462 MHz) Mask 255.255.255.0 | RT61AP_Z baldwin c baldwin c <thc< th=""> <thc< th=""> <thc< th=""> <thc< th=""></thc<></thc<></thc<></thc<> | <u>ר</u> |
| Profile X EAP Method PEAP Session Resumption | WWIFI-51 I1 I | Ш |
| Tunnel Authentication EAP-MSCHAP v2 Tunnel ID Authentication ID Tunnel Password | uuuuu ½ 11 5 9 0 () 29% Sam_AP ½ 64 a 0 7 42% cert ½ 149 a ■ 10% lalala ½ 161 a 0 15% | • |
| Domain Name | AP Information SSID AP1 Authentication WPA MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES | 9 |

• Authentication type and setting method:

PEAP:

1. Select "PEAP" as the Authentication type from the drop-down list. Key-in "wpatest2" for the identity. "Select "EAP-MSCHAP v2" from the drop-down list for tunnel authentication and key-in the tunnel identity as "wpatest2" and the tunnel password as "test2". These settings are the same as our intended AP's setting.

| ++ | Profile | |
|----------------------|---------------------|--------------------|
| EAP Method | PEAP | Session Resumption |
| unnel Authentication | EAP-MSCHAP v2 💌 | |
| Tunnel ID | Authentication IC 💌 | wpatest2 |
| Tunnel Password | **** | |
| Domain Name | | |

2. Click to next page.

*If you want to disconnect, please click cancel button in Authentication Status function. *In Profile function, show "Profile Name" option only in adding AP to Profile function. 3. If the connection is successful, the dialog will appear as below.

| Ralink | | × | | | 5ite Surve | Υ | | × |
|---|--|---|--|------------|--|---|---|---|
| (1) > SSID (2) > Rate (1) > Channel | AP1 1.0 Mbps IP Address 192.168.1.18 7 (2442 MHz) Mask 255.255.255. Link Information | × | RT61AP_Z baldwin AP1 ISTAP NAP2-WEP-197 test_ssid VWIFI-S1 VWIFI-S1 | 0000000000 | 6 6 7 6 8 11 11 11 | | 29% 29% 100% 39% 20% 55% 76% 39% | |
| Status Extra Info Authentication Encryption Network Type Central Channel | AP1 <> 00-0E-2E-E1-98-2D Link is Up [Tx Power:100%] WPA TKIP+AE5 Infrastructure 5 | A | ClaudeAP FTC-02 RT2860AP1 uuuuu Sam_AP cert Ialala P Information SID AP1 | 000000000 | 11 11 11 64 a 149 a 161 a | | 65% 34% 24% 29% 42% 10% 15% | × |

TLS / Smart Card:

1. "Select TLS / Smart Card" from the Authentication type drop-down list. TLS only requires the identification to be set as "wpatest2" for server authentication.

| * * | | |
|----------------------|---------------------|--------------------|
| EAP Method | TLS / Smart Card 💌 | Session Resumption |
| unnel Authentication | | |
| Tunnel ID | Authentication IC 💌 | wpatest2 |
| Tunnel Password | | |
| Domain Name | | |

2. TLS must use client certification. Click "Client Certification" and select a certification for server authentication.



3. Click to the next page.

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.*In Profile function, show "Profile Name" option only in adding AP to Profile function.4. If it connected successfully, the result will appear as in the image below.

| Ralink | | |)(i) ? × | E. | E | | Site Sur | vey | | | | × |
|---|---|------------------------|------------------------------------|-----------------|--|---|---|----------------------------|--------------------------|-----------------------------|---|---|
| SSID Rate Channel | AP1 1.0 Mbps 7 (2442 MHz) Link Inform | > IP Address > Mask | 192,168.1.18 255.255.255.0 × | <i>*</i> | RT61AP_Z baldwin AP1 1STAP NAP2-WEP-197 test_ssid VWIFI-51 VWIFI-51 Claude 0 | ტიტიტიტი | 6 6 7 8 11 11 11 | 000000 | 0000000 | 144 42444 | 29% 29% 100% 39% 20% 55% 76% 39% | |
| Status Extra Info Authentication Encryption Network Type Central Channel | AP1 <> 00-0E-2E Link is Up [Tx Pow WPA TKIP+AES Infrastructure 5 | -E1-98-2D er:100%] | | -AF SS M. | FTC-02 RT2860AP1 uuuuu Sam_AP cert lalala Pinformation ID AP1 AC Address 00-0E-2 | 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 | 11 11 11 64 149 161 Aut 2D Enc | a a a hentication | D D D D N WF | ∲ €9 ≧ ₽A IP+AI | 34% 24% 29% 42% 10% 15% | • |

TTLS:

1. Select TTLS from the Authentication type drop-down list. Key-in the identity as "wpatest2". Select CHAP for tunnel authentication, and key-in the identity as "wpatest2" and tunnel password as "test2". These settings are the same as our intended AP's setting.

| ++ | Profile | |
|-----------------------|---------------------|--------------------|
| EAP Method | TTLS 💌 | Session Resumption |
| Tunnel Authentication | СНАР | |
| Tunnel ID | Authentication ID 💌 | wpatest2 |
| Tunnel Password | **** | |
| Domain Name | | |

2. Click "OK". The dialog box should appear as the image below.

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.*In Profile function, show "Profile Name" option only in adding AP to Profile function.3. If the connection is successful, the dialog box will appear as the image below.

| Ralink | | 1 | Sit | e Surve | 9y | | | × |
|--|--|--|---------|--|----------------------|-----------------------|---|---|
| SSID Rate Channel | AP1 1.0 Mbps IP Address 192.168.1.18 7 (2442 MHz) Mask 255.255.255.0 | RT61AP_Z baldwin & AP1 1STAP NAP2-WEP-197 test_ssid | 0000000 | 6 6 7 6 8 11 | 89 99 89 89 | | 29% 29% 100% 39% 20% 55% | |
| | Link Information X | VWIFI-S1 VWIFI-S1 ClaudeAP | 000 | 11 11 11 | 69 69 | 0 | 76% 39% 65% | |
| Status Extra Info Authentication | AP1 <> 00-0E-2E-E1-98-2D Link is Up [Tx Power:100%] wpΔ | FTC-02 RT2860AP1 uuuuuu | じじじょ | 11 11 11 | 69 69 | 0 0 0 0 0 | 34% 24% 29% | |
| Encryption Network Type | TKIP+AES Infrastructure | cert lalala AP Information | 666 | 149 <mark>a</mark> 161 <mark>a</mark> | | 0 | 42% 10% 15% | ~ |
| | 5 | SSID AP1 MAC Address 00-0E-2E-E | 1-98-20 | Auth Encry | entication /ption | WPA TKIP+ | -AES | |

EAP-FAST:

1. Select EAP-FAST from the Authentication type drop-down list. Key-in the identity as "wpatest2" and a domain name into the blank field. The tunnel identity is "wpatest2" and password is "test2". These setting are the same as our intended AP's setting.

| ++ | Profile | | |
|-----------------------|-------------------|--------------------|--|
| EAP Method | EAP-FAST | Session Resumption | |
| Tunnel Authentication | EAP-MSCHAP v2 💌 | | |
| Tunnel ID | Authentication ID | wpatest2 | |
| Tunnel Password | **** | | |
| Domain Name | | | |

- 2. Click to the next page.
- 3. If the connection is successful, the dialog box will appear as the image below.

| Ralink | | Site Su | rvey > |
|---|--|--|---|
| SSID Rate Channel | AP1 1.0 Mbps IP Address 192.168.1.18 7 (2442 MHz) Mask 255.255.255.0 | RT61AP_Z ₺ 6 baldwin 6 6 ✓ AP1 7 1STAP ₺ 6 NAP2-WEP-197 ₺ 8 test_ssid ₺ 11 | ▶ ♀ 29% 29% ♥ ● ♀ 100% ▶ ● ● ↑ 100% ▶ ● ● ↑ 39% ▶ ● ● ↑ 20% ▶ ● ● ▼ 20% ▶ ● ● ● 55% |
| <u>א א</u> | Link Information X | VWIFI-51 11 VWIFI-51 11 VWIFI-51 11 ClaudeAP 11 | 9 7 76% 9 10 7 39% 9 9 7 65% |
| Status Extra Info | AP1 <> 00-0E-2E-E1-98-2D Link is Up [Tx Power:100%] | FTC-02 11 RT2860AP1 11 UUUUU 11 11 | |
| Encryption Network Type Central Channel | TKIP+AES Infrastructure S | Sam_AP 64 cert 1/9 lalala 1/0 161 AP Information | a U 42% a 10% a D 15% |
| | | SSID AP1 A MAC Address 00-0E-2E-E1-98-2D Er | uthentication WPA |

*If you want to disconnect, please click "Cancel" on the Authentication Status function page. *In Profile function, show "Profile Name" option only in adding AP to Profile function.

4. Appendix

4.1 Country Channel List

Country channel list, channel classification and range.

| Country Name | Classification | Range |
|----------------|----------------|---------|
| Argentina | 0 | CH1~11 |
| Australia | 1 | CH1~13 |
| Austria | 1 | CH1~13 |
| Bahrain | 0 | CH1~11 |
| Belarus | 1 | CH1~13 |
| Belgium | 1 | CH1~13 |
| Bolivia | 1 | CH1~13 |
| Brazil | 0 | CH1~11 |
| Bulgaria | 1 | CH1~13 |
| Canada | 0 | CH1~11 |
| Chile | 0 | CH1~11 |
| China | 1 | CH1~13 |
| Colombia | 1 | CH1~13 |
| Costa Rica | 1 | CH1~13 |
| Croatia | 0 | CH1~11 |
| Cyprus | 1 | CH1~13 |
| Czech Republic | 1 | CH1~13 |
| Denmark | 1 | CH1~13 |
| Ecuador | 0 | CH1~11 |
| Egypt | 1 | CH1~13 |
| Estonia | 1 | CH1~13 |
| Finland | 1 | CH1~13 |
| France | 1 | CH1~13 |
| France2 | 3 | CH10~13 |
| Germany | 1 | CH1~13 |
| Greece | 1 | CH1~13 |
| Hong Kong | 0 | CH1~11 |

| 1 | CH1~13 |
|---|---|
| 1 | CH1~13 |
| 5 | CH1~14 |
| 4 | CH14~14 |
| 1 | CH1~13 |
| 0 | CH1~11 |
| 0 | CH1~11 |
| 1 | CH1~13 |
| 0 | CH1~11 |
| 1 | CH1~13 |
| 0 | CH1~11 |
| 0 | CH1~11 |
| 1 | $CH1_{\sim}13$ |
| | 1 1 1 1 1 1 1 5 4 1 <td< td=""></td<> |

| Portugal | 1 | CH1~13 |
|--------------------------|---|--------|
| Puerto Rico | 0 | CH1~11 |
| Romania | 0 | CH1~11 |
| Russia | 1 | CH1~13 |
| Saudi Arabia | 0 | CH1~11 |
| Singapore | 1 | CH1~13 |
| Slovakia | 1 | CH1~13 |
| Slovenia | 1 | CH1~13 |
| South Africa | 1 | CH1~13 |
| South Korea | 1 | CH1~13 |
| Spain | 1 | CH1~13 |
| Sweden | 1 | CH1~13 |
| Switzerland | 1 | CH1~13 |
| Taiwan | 0 | CH1~11 |
| Thailand | 1 | CH1~13 |
| Turkey | 1 | CH1~13 |
| United Arab Emirates | 1 | CH1~13 |
| United Kingdom | 1 | CH1~13 |
| United States of America | 0 | CH1~11 |
| Uruguay | 0 | CH1~11 |
| Venezuela | 0 | CH1~11 |
| Yugoslavia | 0 | CH1~11 |

4.2 Acknowledgements

The above settings are used in the test platform by RaLink technology corp. Users can set the function in accordance with their AP.

Acknowledgements:

"This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)". This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

5. FAQ

5.1 FAQ

If you create an adhoc profile for 2.4G channel, and then switch wireless mode to 5G(as Figure 5-1), device will re-send beacon at the first channel of 5G. Note the original adhoc profile will keep previous settings.



Figure 5-1 Switch wireless mode when activate an adhoc profile

Federal Communications Commission (FCC) Interference 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 generate, 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 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.

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

RF exposure warning

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

The equipment must not be co-located or operating in conjunction with any other antenna or transmitter.