**Step 6:** After switch to AP mode, Ralink Wireless Utility will automatically pup-up. The Wireless Default SSID is assigned as "**SoftAP-2C**".

Ralink Wireless Utilit	Y		1
Config Access Control	Mac Table   Event Lo	Statiotics About	
ssid 🛛	ene x	]	Channel 1 💌
Witeless Mode	02.11 8/G/N nix 💌	<- Use Mac Address	Seculty Setting
Country Region Code 11 B//G 0: CH1-	11 💌	No forwarding anor     Hide SSID     Alow BW 40 MHz	ng wireless clients
Beacon (mc) TX Power Idle time(60 - 3600(s)	100 %	1	
		Default	Apply
			Help

**Step 7**: To make sure your Soft AP is working properly, you need to use another computer which with Wireless LAN feature to access SoftAP-2C AP. In the below example, use another PC with Wireless feature in Vista Operation System. Go to Start  $\rightarrow$  Control Panel  $\rightarrow$  Choose "Network and Sharing Center" option  $\rightarrow$  Click "Connect to a network" to search the available networks.

Net	work and Sharing Center	
View computers and devices Connect to a network		View full m
Manage wireless networks	🔊 🏟	
Set up a connection or network	WINNE-PC Internet	
Manage network connections	(This computer)	
Diagnose and repair	Not connected	
	Wireless networks are available.	

Show All		[
WLAN_SW	Security-enabled network	ller.
SoftAP-2C	Unsecured network	lite.
<b>S</b> 112233	Unsecured network	lte-

Step 8: Select the network "SoftAP-2C" and click "Connect" to establish the connection.

**Step 9:** After the computer is successful connected to SoftAP-2C, Network and Sharing Center screen will be shown as below. Click "**View Status**" to see the detail.

Control Panel +	Network and Sharing Center	• *7 Seach	
Tasks View computers and devices Connect to a network	Network and Sharing G	enter	View full may
Manage winters networks Set up a connection or network Manage network connections Discourse and remain	WINNE-PC (This computer	SoftAP-2C	Internet
	SoftAP-2C (Public networ	42	Customia
	Accent	Local only	
	Connection	Wireless Network Connection (SoftAP-2C)	Disconnec
12	Sharing and Discovery		
1123	Network discovery	9 OH	9
115 3.5	File sharing	9 OH	8
	Public folder sharing	e Oli	9
1	Printer sharing	Off (no printers installed)	9
	Password protected sharing	e On	9
Seeann	Media sharing	e DM	9
litered Options	Show me all the files and folde	ss I am sharing	

**Step 10:** In General tab, click "**Detail...**", and then you can see the current Network connection details. If this computer is successful connect to SoftAP-2C Access Point, the DHCP server will be assigned to same IP address.

annection		Network Connection Deta	ās 🖌
IPv4 Connectivity: IPv6 Connectivity:	Local	Network Connection Details	
dia State:	Enabled	Property	Value
n: Quality: als Sent —	SeftAP-2C 00:05:48 270.0 Mbps still erses Received	Connection-specific DN Description Physical Address DHCP Enabled IPv4 IP Address IPv4 IP Address IPv4 Subnet Mask Lease Obtained Lease Expires IPv4 Default Gateway	802.11n USB Wreless LAN Card 00-06-4F-12-34-56 Yes 192.168.0.49 255.255.255.0 Thursday, October 13, 2005 6:11:36 A Thursday, October 20, 2005 6:11:36 A 192.168.0.1
4,531	j 210 Diagnose	IPv4 DNS Server IPv4 WINS Server NetBIOS over Topip En Link-local IPv5 Address IPv5 Default Gateway IPv6 DNS Server	192.168.0.1 192.168.0.1 Yes le80-2d18.327d 9/32/14ee%13

## 3.2 For Windows Vista

Ralink wireless utility is shown as below. There are 6 setting pages in Ralink wireless utility:

Belkin_N1         00-17-3F-5/           mony_best         00-06-4F-58           Default_WL         00-06-4F-33           Default_11N         00-06-4F-33           WLAN_SW         00-07-40-F1           MISO         00-06-4F-15           mySSID         00-03-7F-F8	A-8E-AD N 3-13-2F N 3-44-66 N 1-99-42 G 5-34-A6 G 5-00-02 G	76% 96% 55% 20% 100% 86%	1 3 6 9	None None None	Unknown Unknown Unknown Unknown	Infrastructur Infrastructur
morry_test         00-06-4F-56           Default_WL         00-06-4F-43           Default_11N         00-06-4F-33           WLAN_SW         00-07-40-F1           MISO         00-06-4F-15           mySSID         00-03-7F-F6	3-13-2F N 3-CF-8F G 3-44-66 N 1-99-42 G 5-34-A6 G 5-00-02 G	96% 55% 20% 100% 86%	3 6 9	None None None	Unknown Unknown Unknown	Infrastructur
Default_WL 00-06-4F-43 Default_11N 00-06-4F-33 WLAN_SW 00-07-40-F1 MISO 00-06-4F-1F mySSID 00-03-7F-F8	0-CF-8F G 0-44-66 N 1-99-42 G 34-A6 G 5-00-02 G	55% 20% 100% 86%	6 9	None	Unknown Unknown	Infrastructur
Default_11N 00-06-4F-33 WLAN_SW 00-07-40-F1 MISO 00-06-4F-1F mySSID 00-03-7F-F8	9-44-66 N 1-99-42 G 5-34-A6 G 5-00-02 G	20% 100% 86%	9	None	Unknown	
WLAN_SW 00-07-40-F1 MISO 00-06-4F-1F mySSID 00-03-7F-FE	-99-42 G -34-A6 G -00-02 G	100%	9	The second		Infrastructur
MISO 00-06-4F-1F mySSID 00-03-7F-FE	-34-A6 G	86%		TKIP	WPA-PSK	Infrastructur
mySSID 00-03-7F-FE	-00-02 G		10	None	Unknown	Infrastructur
		96%	11	None	Unknown	Infrastructur
•			-			

- Profile Page: Manage the profile.
- Link Status Page: Display current connection information.
- Site Survey Page: Display the available networks.
- Statistics Page: Display the packet counters
- **WPS Configuration** Page: Connect to WPS (Wi-Fi Protected Setup) capable APs.
- QoS Page: It involves "WMM Enable", "WMM Power Save Enable" and DLS setup
- About Page: Display Ralink driver and utility information.

## 3.2.1 Profile

In the **"Profile"**, you can view and manage the current using Available Point(s). You can **Add**, **Delete**, **Edit**, or **Activate** the current Available Point(s). Also you can duplicate the AP or set current AP as Default.

Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1	WLAN_SW	Auto	WPA-PSK	TKIP	Infrastructure
			1		

**Profiles Name:** The Profiles List displays all the profiles and the relative settings of the profiles including Profile Name, SSID, and Channel...etc; preset to **PROF**\* (\* indicate 1,2,3,...)

**SSID:** AP to Ad-hoc name.

Channel: Channel in use for Ad-Hoc mode.

Authentication: Authentication mode.

Encryption: Security algorithm in use.

Network Type: Network's type, including Infrastructure and Ad-hoc.

Indicate connection is successful on currently activated profile.

Indicate connection is failed on currently activate profile.

Add/Delete/Edit Button: Click these buttons to add/delete/edit the selected profiles.

Activate Button: Click "Activate" to connect the selected profile. When a profile is activated, the adapter will be initially connected to the profile.

Profile Name	SSID	Channel	Authentication	Encryption	Network Type

By either pushing the "Add" button on Profile Page or the "Add to Profile" button on Site Survey Page, it brings up the profile setting sheet which contains two setting pages -- "Configuration" page and "Authentication and Security" page.

SSID	BSSID	Phy	Signal	A C.	Encryption	Authentic	Network Ty
Belkin_N1	00-17-3F-5A-8E-AD	N	76%	1	None	Unknown	Infrastructu
many_test	00-06-4F-5B-13-2F	N	96%	3	None	Unknown	Infrastructu
Default_WL	00-06-4F-43-CF-8F	G	55%	6	None	Unknown	Infrastructu
Default 11N	00-06-4E-33-44-66	N	20%	6	None	Linknown	Infrastructu
WLAN_SW	00-07-40-F1-99-42	G	100%	9	TKIP	WPA-P5K	Infrastructu
MISO	00-06-4F-1F-34-A6	G	86%	10	None	Unknown	Infrastructu
mySSID	00-03-7F-FE-00-02	G	96%	11	None	Unknown	Infrastructu
-							
				-			

# 3.2.1.1 Add a profile

#### [Configuration page]

dd Profile Configuration   Aut	hentication and Sec	unty		×
Profile Name	PROFI	SSID	[wlan_sw	•
Network Type	Infrastructure	<ul> <li>TX Powe</li> </ul>	r Auto	•
		OK Can	cel Anthy	Help

- Profile Name: Name of the profile
- SSID: Name of the desire network
- Network Type: Netowork of the desired network, either infrastructure or Ad-Hoc.
   Infrastructure This operation mode requires the presence of a wireless Access
   Point. All communication is done via the Access Point or Router.
   Ad-Hoc Select this mode if you want to connect to another wireless station in the

Wireless LAN network without through an Access Point or Router.

Tx-Power: The desired TX power level; the available options are 100%, 75%, 50% and Auto. If you want to lower the transmit power of the adapter for saving the power of the system, you can select the lower percentages from the list. The lower power will cause the lower signal strength and the coverage range.

Configuration Aut	hertication	and Security			
Authentication 1	іре :	WPA-PSK	•		
Encryption		•         •			
WPA Preshared	Key :				
-Wester-	-	10			_
(F Cepff)	Hes	*			
C (1982	Has	<u>v</u>			
(* Kepli)	Hes	+			
C 84900	Has	-			-
TWEP 64 BA	i Endoyofic Is Encipel	rt: Planue Kapie 11 (m. Planue Kapie)	1980K shaastare Xi HEX sharastari	or 5 ASCII chiaiachur ur 11 AGCII chiaiachur	ine i
				C Show Per	eward

#### [Authentication and Security page]

Authentication Type: The authentication of the desired network. For infrastructure network, the available modes are Open, Shared, WPA, WPA-PSK, WPA2, and WPA2-PSK.

**Open:** No authentication is needed among the wireless devices.

**Shared:** Only Wireless device using a shared key (WEP Key identified) is allowed to connecting each other. Setup the same key as the wireless device that the adapter intends to connect.

**WPA:** WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprise, small business and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

**WPA-PSK** – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

**WPA2** – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The different between WPA and WPA2 is that WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP).

**WPA2-PSK** – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP).

**Encryption:** The encryption of the desired network.

- -- For Open and Shared authentications, the available encryption modes are **None** and **WEP**.
- -- For WPA, WPA-PSK, WPA2 and WPA2-PSK authentications, the available modes are **TKIP** and **AES**.

**None** – Disable the Encryption mode.

**WEP** – Enabled the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Key Length & the key Index.

**TKIP** – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10000 packets (a packet is a kind of message transmitted over a network). This insures much greater security than the standard WEP security.

**AES** – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.

**Note**: All devices in the network should use the same encryption method to ensure the communication.

- WPA Pre-Shared Key: The WPA-PSK key can be from 8 to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.
- WEP Key (Key1~Key4): The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit & 128-bit. Select the default encryption key form key1 to key4 by selected the radio button.

Fill the text box by following the rule below:

**64-bit** – Input 10-digit Hex values (in the "**A-F**", "**a-f**, and "**0-9**" range) or 5-digit ASCII characters (including "**a-z**" and "**0-9**") as the encryption keys. For example: "**0123456aef**" or "**test1**"

**128-bit** – Input 26-digit Hex values (in the "**A-F**", "**a-f**, and "**0-9**" range) or 13-digit ASCII characters (including "**a-z**" and "**0-9**") as the encryption keys. For example: "**01234567890123456789abcdef**" or "**administrator**".

### 3.2.1.2 Edit a profile

Selecting an exiting profile then clicking the "**Edit**" button on Profile Page brings up the profile setting sheet filled with the profile information for user modification.

Ralink Wirel	ess Utilit	y					x
Profile Link S	itatus   Si	e Survey   Statis	tics   WPS C	onfiguration   QoS	About		
Profile Lis	t						
Profile N	lame	SSID	Channel	Authentication	Encryption	Network Type	
PR0	F1	WLAN_SW	Auto	WPA-PSK	ткр	Infrastructure	
							- 11
							- 11
							- 11
							- 11
							- 11
				_			
	Add		Delete	Ed	t	Activate	
						ок н	lelp

### 3.2.1.3 Delete a profile

Selecting an exiting profile then clicking the "Delete" button on Profile Page to deletes the profile.

PROFI	WLAN_SW	Auto	WPA-PSK	ТКР	Infrastructure

## 3.2.1.4 Active a profile

Selecting an exiting profile then clicking the "Active" button on Profile Page activates the profile.

ink Wireless Ut	lity Site Survey   Si	atistics   WPS (	Configuration   GoS	About	-
Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1	WLAN_SW	Auto	WPA-PSK	ТКР	Infrastructure
				-	
Add		Delete	E	dt 📘	Activate
					OK Help

## 3.2.2 Link Status

In this section, you can immediately monitor the current connected link status, such as Link Speed, Throughput, Link Quality, Signal Strength, Noise Level ...etc.

Status :	Default_11	N <-> 00-06	4F-5B-13-32	2		
Edra info :	Link is Up (	TxPower:10	074)			
Channel :	6 <-> 2437	KHz: centra	d channel : 4			
Link Speed :	Tx (Mbps)	Г	300.0	Rx (Mbps)	30	0.00
Throughput :	Tx (Kbps)	Г	4.5	Rx (Kbps)	-	0.04
	Good	100%				
Link Quality :						
	Good	100%			∏ d8m	
Signal Strength 1:						
	Good	100%		_	_	_
Signal Strength 2						
	Good	100%				
signal strength 3:		271				
Noise Level :	Law	205				
BW: 40	Gt long	MCS	15	SNR0: 15	SNR1:n/a	

(for Tx Link Speed up to 300 Mbps model)

Status :	Default_11	N <> 00-06-4	F-58-13-32	2		_
Edra info :	Link is Up (	TxPower: 1001	ų			-
Channel :	6 <-> 2437	6 <-> 2437 KHz; central channel : 4				-
Link Speed :	Tx (Mbps)		150.0	Rx (Mbps)	300.0	
Throughput :	Tx (Kbps)		1.0	Rx (Kbps)	51.0	
	Good	100%				_
Link Quality :						
	Good	100%		_	∏ d8m	
Signal Strength 1:						
Card David 2	Good	100%				
agna avergin z	Good	100%				-
Signal Strength 3:						Π.
	Law	26%				
Noise Level :						
HT						-
BW: 40	GI: short	MCS: 7		SNR0: 16	SNR1: 0	

(for Tx Link Speed up to 150 Mbps model)

**Status:** Current connection status. If no connection, it will show Disconnected. Otherwise, the SSID and BSSID will show here.

Extra Info: Display the link status and current channel in use.

**Channel:** Display the number of the radio channel and the frequency used for the networking. **Link Speed (Mbps):** Display the transmission and reception rate of the network. The maximum transmission rate is 300/150Mpbs (depend on model).

Throughput (Kbits/sec): Display transmits and receives throughout in unit of K bits/sec.

Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.

dBm: If you want to know the signal strength in the unit of dBm, select the check box.

**Signal Strength:** Receive signal strength, user can choose to display as percentage or dBm format.

**Signal Strength2:** Receive signal strength 2, user can choose to display as percentage or dBm format.

Noise Level: Display the noise signal strength.

**HT:** Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value. (show the information only for 802.11n wireless card.)

#### 3.2.3 Site Survey

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your adapter and automatically connect to the wireless device with the highest signal strength. From the **"Site Survey"**, all the network nearby will be listed. You can change the connection to another network or add one of the networks to your own profile list.

SSID	BSSID	Phy	Signal	▲ C	Encryption	Authentic	Network Ty
morry_test	00-06-4F-5B-13-2F	N	91%	3	None	Unknown	Infrastructur
Default_11N	00-06-4F-33-44-66	N	15%	6	None	Unknown	Infrastructur
Default_WL	00-06-4F-49-C2-8B	G	55%	6	None	Unknown	Infrastructur
WLAN_SW	00-07-40-F1-99-42	G	100%	9	TKIP	WPA-PSK	Infrastructur
MISO	00-06-4F-1F-34-A6	G	91%	10	WEP	Unknown	Infrastructur
Belkin_N1	00-17-3F-5A-8E-AD	N	70%	11	None	Unknown	Infrastructur
3ComNokia	00-14-7C-BB-E0-1A	G	15%	11	None	Unknown	Infrastructur
mySSID	00-03-7F-FE-00-02	G	94%	11	None	Unknown	Infrastructur
< [			111				•
< [	M ALL CAN	_	III	_	1		

SSID: Name of BBS of IBSS network.

**BSSID:** MAC address of AP or randomly generated of IBSS.

Signal: Receive signal strength of specified network.

Channel: Channel in use.

**Encryption:** Encryption algorithm used within than BBS or IBSS. Valid value includes WEP, TKIP, AES, and Not Use.

**Authentication:** Authentication mode used within then network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.

Network Type: Network type in use, Infrastructure or Ad-Hoc.

**Rescan:** Issue an rescan command to wireless NIC to update information on surrounding wireless network.

**Re-Scanning:** Clicking the re-scan button to perform the re-scanning action.

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

#### [Connect A Network]

(1) When Raconfig first ran, it will select the best AP to connect automatically.

(2) If user wants to connect to other AP, he can double-click mouse on the intended AP to make connection.

(3) If the intended network has encryption other than "Not Use", Raconfig will bring up the security page and let use input the appropriate information to make the connection.

Main and the second sec

### **⊙Example 1: Open and Non-Encrypted**

Step 1 – Choose "Open" authentication type

#### Step 2 - Choose "None" encryption type

Authentication Type :	Ciper.	• 1 Use 802.1x	
Encryption	None		
WPA Preshared Key :			
Wep Fag			
R Legti M		1	
C Gett 1		[	
C (1)(1)	-	[	
C Lott 1		[	
WEERINGEN	otori, Filman Kasiri S	DHER of a latence to ABC	distation
*WEP 1288 A Em	prine Please Lege	25 PEC (harschreist 13 AS	CR schweigtere

**Step 3** – After the profile is saved, click "**Activate**" button on Profile Page to activate the profile.

Profile Name FIRCE1	SSID WLAN, SW	Ourral	Athentication WFA-P3K	Encryption TIGE	Network Type Intrastouchure
19042	Defaul_110	Auto	Open	Han	Manuchan
_					
	16				

## ⊙ Example 2: WEP-Encrypted

- Step 1 Choose "Open" or "Shared" authentication type
- Step 2 Choose "WEP" encryption type
- Step 3 –Enter the WEP KEY

Add Profile		×
Configuration Authentication	and Security	
Authentication Type : Encryption :	Open Use 802. tx	-
WPA Preshared Key :		
-Wep Key (≆ Key#1 Hex	·	
⊂ Keytt2 Hex	•	
C Keytt3 Hex	•	
С Кеу#4 Нех	•	
* WEP 64 Bits Encryption * WEP 128 Bits Encryption	n: Please Keyin 10 HEX characters or 5 ASCII characters on: Please Keyin 26 HEX characters or 13 ASCII character	
	C Show Pase	ward
	OK Cancel Apply	Help

**Step 4** –After the profile is saved, click the "**Activate**" button on Profile Page to active the profile.

PTOFILE FLIGTINE	SSID	Channel	Authentication	Encryption	Network Type
PROF1	WLAN SW	Auto	WPA-PSK	TKIP	Infrastructure
PROF2	WEP_Encyption	Auto	Open	WEP	Infrastructure

### ⊙ Example 3: WPA-PSK/WPA2-PSK

- Step 1 Choose "WPA-PSK" or "WPA2-PSK" authentication type
- Step 2 Choose "TKIP" or "AES" encryption type
- Step 3 –Enter the pre-shared KEY

Authentication Type :	WPA-PSK -				
Encryption :	тюр 💌				
WPA Preshared Key :					
- Wep Kep					
(₹ Key#1 Hex	그				
C Keylt2 Hex	<u>v</u>				
C Key#3 Hex	v				
C Keyllä Hex	Ψ				
* WEP 64 Bits Encryptic * WEP 128 Bits Encrypt	n: Please Keyin 10 HEX characters or 5 ASCII charact on: Please Keyin 26 HEX characters or 13 ASCII chara	ins icters			
	C Same P	herene			

**Step 4** –After the profile is saved, click the "**Activate**" button on Profile Page to active the profile.

Endia Na	SSID	Dencel	Authentication	Ecopption	Network Type
PROF	WLAN_SW	Auto	WPA-PSK	TKIP	Infrastructure
-					
-					
-					
-					
-					
1					

### $\odot$ Example 4:WPA/WPA2

Step 1 – Choose "WPA" or "WPA2" authentication type

Step 2 - Choose "TKIP" or "AES" encryption type

Authentication Type :	WPA 💌				
Encryption :	THOP				
WPA Preshared Key :					
Wep Kep					
€ Kestt1 Hex	Ŧ				
C Keptt2 Hex	Ŧ				
C Keylt3 Hex	¥				
C Keyllä Hax	Ŧ				
* WEP 64 Bits Encryptic * WEP 120 Bits Encrypt	<ul> <li>Please Keyin 10 HEX charact on Please Keyin 26 HEX charact</li> </ul>	erz or 5 ASCII characters cters or 13 ASCII characters			
		C Show Burnard			

**Step 3** –After the profile is saved, click the "**Activate**" button on Profile Page to active the profile.

TKIP Infrastructure

WPA Wireless Network	k properties	
Connection Security		
Security type: Egoryption type:	WPA-Enterprise TKIP	•
Chgose a network a	uthentication method:	Settings
Cache user infor to this network	mation for subsequent co	nnections
		Curred
		un cance

Step 4 – The Windows profile setting dialog is popped-up for user to modify.

## 3.2.4 Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates the MIB counters into a format easier for user to understand. You may reset the counters to Zero by clicking "**Reset Counter**".

Transmit Statistics			1
Frames Transmitted Successfully	-	1806	
Frames Transmitted Successfully After Retry(s)	-	1388	
Frames Fail To Receive ACK After All Retries	-	7	
RTS Frames Successfully Receive CTS		0	
RTS Frames Fail To Receive CTS		0	
Receive Statistics			1
Frames Received Successfully	-	13162	
Frames Received With CRC Error	-	273993	
Frames Dropped Due To Out-of-Resource		0	
Duplicate Frames Received	-	٥	
		Reset Counter	1

### [Transmit Statistics]

Frames Transmitted Successfully: Frames successfully sent

Frames Transmitted Successfully After Retry: Frames sent successfully with retry.

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 frames.

RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS frames.

#### [Receive Statistics]

Frames Received Successfully: Frames received successfully.

Frames Received with CRC Error: Frames received with CRC error.

Frames Dropped Due to Out-of-Resource: Frames dropped due to resource issue.

Duplicate Frames Received: Duplicate received frames.