

802.11N/3.5G Outdoor Router

User Manual

USER MANUAL 1.0.0

Table of Contents

| | |
|--|-----------|
| 1. Terminology | 5 |
| 2. Introduction..... | 7 |
| 2.1 Package contents | 7 |
| 2.2 Product Features..... | 7 |
| 2.3 Front Panel Description | 8 |
| 2.4 Rear Panel Description | 9 |
| 3. Installation..... | 10 |
| 3.1 Hardware Installation..... | 10 |
| 3.1.1 Appearance and Interface Introduction | 10 |
| 3.1.2 Hardware installation steps | 12 |
| 3.2 Software Installation | 14 |
| 4. Software configuration | 14 |
| 4.1 Prepare your PC to configure the WLAN Broadband Router | 15 |
| 4.2 Connect to the WLAN Broadband Router | 16 |
| 4.3 Management and configuration on the Outdoor Router | 16 |
| 4.3.1 Wizard..... | 16 |
| 4.3.2 Operation Mode | 26 |
| 4.3.3 Internet Settings | 28 |
| 4.3.3.1 WAN | 28 |
| 4.3.3.2 LAN | 34 |
| 4.3.3.3 DHCP clients..... | 35 |
| 4.3.3.4 VPN Passthrough | 35 |
| 4.3.4 Wireless Settings..... | 36 |
| 4.3.4.1 Basic..... | 36 |
| 4.3.4.2 Advanced | 38 |
| 4.3.4.3 Security | 40 |
| 4.3.4.4 WPS | 44 |
| 4.3.5 Firewall | 45 |
| 4.3.5.1 MAC/IP/Port Filtering | 45 |
| 4.3.5.2 Port Forwarding | 47 |
| 4.3.5.3 DMZ..... | 48 |

| | | |
|-----------|--|-----------|
| 4.3.5.4 | System Security | 49 |
| 4.3.5.5 | Content Filtering | 50 |
| 4.3.6 | Administration | 52 |
| 4.3.6.1 | Management..... | 52 |
| 4.3.6.2 | QOS..... | 54 |
| 4.3.6.3 | Upload Firmware | 55 |
| 4.3.6.4 | Backup & Restore | 56 |
| 4.3.6.5 | Status..... | 57 |
| 4.3.6.6 | System Log | 58 |
| 4.4 | Configuration Examples | 59 |
| 4.4.1 | Example one – PPPoE on the WAN | 59 |
| 4.4.2 | Example two – fixed IP on the WAN..... | 62 |
| 4.4.3 | Example three –set WLAN to be WAN as WiFi Client..... | 66 |
| 5. | FREQUENTLY ASKED QUESTIONS (FAQ)..... | 70 |
| 5.1 | What and how to find my PC's IP and MAC address? | 70 |
| 5.2 | What is Wireless LAN? | 70 |
| 5.3 | What are ISM bands?..... | 70 |
| 5.4 | How does wireless networking work? | 70 |
| 5.5 | What is BSSID? | 71 |
| 5.6 | What is ESSID? | 71 |
| 5.7 | What are potential factors that may causes interference? | 71 |
| 5.8 | What are the Open System and Shared Key authentications? | 71 |
| 5.9 | What is WEP? | 71 |
| 5.10 | What is Fragment Threshold? | 72 |
| 5.11 | What is RTS (Request to Send) Threshold?..... | 72 |
| 5.12 | What is Beacon Interval? | 72 |
| 5.13 | What is Preamble Type? | 72 |
| 5.14 | What is SSID Broadcast?..... | 72 |
| 5.15 | What is Wi-Fi Protected Access (WPA)?..... | 73 |
| 5.16 | What is WPA2? | 73 |
| 5.17 | What is 802.1x Authentication? | 73 |
| 5.18 | What is Temporal Key Integrity Protocol (TKIP)?..... | 73 |
| 5.19 | What is Advanced Encryption Standard (AES)? | 73 |
| 5.20 | What is Inter-Access Point Protocol (IAPP)? | 73 |
| 5.21 | What is Wireless Distribution System (WDS)? | 73 |
| 5.22 | What is Universal Plug and Play (uPNP)?..... | 73 |
| 5.23 | What is Maximum Transmission Unit (MTU) Size? | 74 |

| | | |
|------|---|----|
| 5.24 | What is Clone MAC Address?..... | 74 |
| 5.25 | What is DDNS?..... | 74 |
| 5.26 | What is NTP Client? | 74 |
| 5.27 | What is VPN? | 74 |
| 5.28 | What is IPSEC?..... | 74 |
| 5.29 | What is WLAN Block Relay between Clients? | 74 |
| 5.30 | What is WMM?..... | 74 |
| 5.31 | What is WLAN ACK TIMEOUT? | 74 |
| 5.32 | What is Modulation Coding Scheme (MCS)? | 74 |
| 5.33 | What is Frame Aggregation? | 75 |
| 5.34 | What is Guard Intervals (GI)?..... | 75 |

1. Terminology

| | |
|---------|---|
| 3DES | Triple Data Encryption Standard |
| AES | Advanced Encryption Standard |
| ANSI | American National Standards Institute |
| AP | Access Point |
| CCK | Complementary Code Keying |
| CSMA/CA | Carrier Sense Multiple Access/Collision Avoidance |
| CSMA/CD | Carrier Sense Multiple Access/Collision Detection |
| DDNS | Dynamic Domain Name Server |
| DH | Diffie-Hellman Algorithm |
| DHCP | Dynamic Host Configuration Protocol |
| DSSS | Direct Sequence Spread Spectrum |
| EAP | Extensible Authentication Protocol |
| ESP | Encapsulating Security Payload |
| FCC | Federal Communications Commission |
| FTP | File Transfer Protocol |
| IEEE | Institute of Electrical and Electronic Engineers |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| ISM | Industrial, Scientific and Medical |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MD5 | Message Digest 5 |
| NAT | Network Address Translation |
| NT | Network Termination |
| NTP | Network Time Protocol |
| PPTP | Point to Point Tunneling Protocol |
| PSD | Power Spectral Density |
| RF | Radio Frequency |
| SHA1 | Secure Hash Algorithm |
| SNR | Signal to Noise Ratio |
| SSID | Service Set Identification |
| TCP | Transmission Control Protocol |
| TFTP | Trivial File Transfer Protocol |

| | |
|------|---------------------------------|
| TKIP | Temporal Key Integrity Protocol |
| UPNP | Universal Plug and Play |
| VPN | Virtual Private Network |
| WDS | Wireless Distribution System |
| WEP | Wired Equivalent Privacy |
| WLAN | Wireless Local Area Network |
| WPA | Wi-Fi Protected Access |

2. Introduction

The 802.11N/3.5G Outdoor Router is an affordable IEEE 802.11b/g/n specifications and 3.5G WCDMA of Outdoor Router solution; setting SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN. This document describes the steps required for the initial IP address assign and other configuration of the outdoor router. The description includes the implementation of the above steps.

2.1 Package contents

The package of the WLAN Broadband Router includes the following items,

- ✓ 802.11N/3.5G Outdoor Router
- ✓ DC 12V/1.5A Power Adapter
- ✓ Documentation CD
- ✓ POE Injector
- ✓ Tie

2.2 Product Features

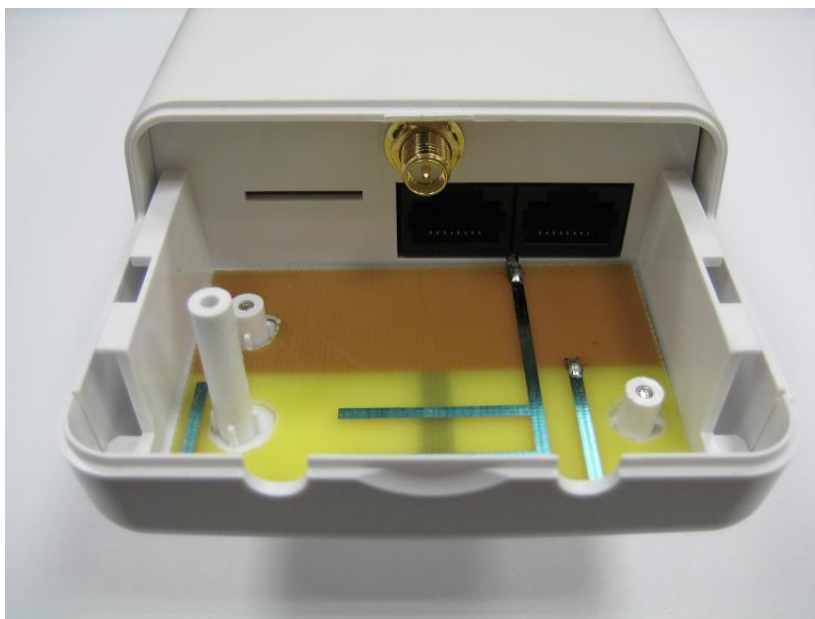
- Compatible with IEEE 802.11n Specifications provides wireless speed up to 150Mbps data rate.
- Compatible with IEEE 802.11g standard to provide wireless speeds of 54Mbps data rate.
- Compatible with IEEE 802.11b standard to provide wireless speeds of 11Mbps data rate.
- Maximizes the performance and ideal for media-centric applications like streaming video, gaming and Voice over IP technology.
- Support various operation (Bridge/Gateway/Ethernet Converter) modes between wireless and wired Ethernet interfaces.
- Supports WPS, 64-bit and 128-bit WEP, WPA, WPA2 encryption to protect the wireless data transmission.
- Support TKIP/AES/TKIPAES of WPA algorithms.
- Support IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- Support DHCP server to provide clients auto IP addresses assignment.
- Support DHCP client, static IP, PPPoE, L2TP and PPTP of WAN Interface.
- Supports firewall security with port filtering, IP filtering, MAC filtering, port forwarding, DMZ hosting and URL filtering functions.
- Support WEB based management and configuration.
- Support System Log.
- Support Dynamic DNS
- Support NTP

2.3 Front Panel Description



| LED Indicator | State | Description |
|----------------|----------|---|
| 1. PWR LED | ON | The WLAN Broadband Router is powered ON. |
| | Off | The WLAN Broadband Router is powered Off. |
| 2. WLAN LED | Flashing | Data is transmitting or receiving on the wireless. |
| | ON | Wireless Radio ON. |
| | Off | Wireless Radio Off. |
| 3. WAN LED ACT | Flashing | Data is transmitting or receiving on the WAN interface. |
| | ON | Port linked. |
| | Off | No link. |
| 4. LAN LED ACT | Flashing | Data is transmitting or receiving on the LAN interface. |
| | ON | Port linked. |
| | Off | No link. |

2.4 Rear Panel Description



| Interfaces | Description |
|---------------|--|
| SMA connector | For external antenna. You can use the SMA connector to connect with 2.4GHz external antenna. |
| LAN(Middle) | The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively. |
| WAN(Right) | The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively. |

3. Installation

3.1 Hardware Installation

3.1.1 Appearance and Interface Introduction

Notes: The product shot is for reference only please refer to physical product.

① LED Panel



② Waterproof Sliding Door

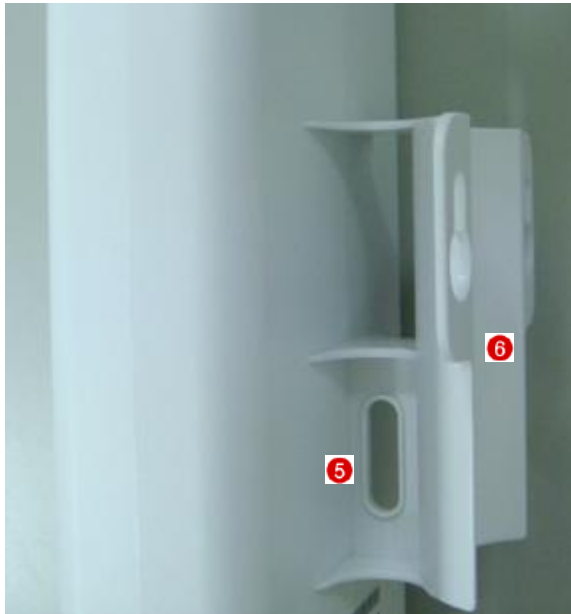
③ Pass through Ethernet cable from this hole

④ Push this button to remove upper housing



5 Pole Mount

6 Wall Mount

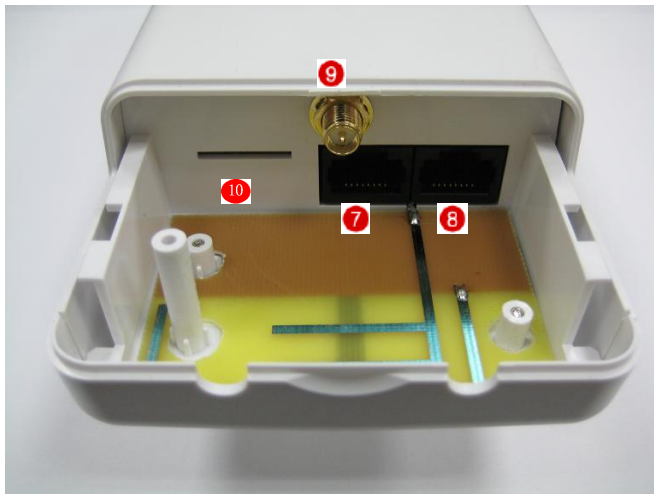


7 LAN port

8 WAN port

9 SMA connector for external antenna

10 SIM slot for 3G SIM card

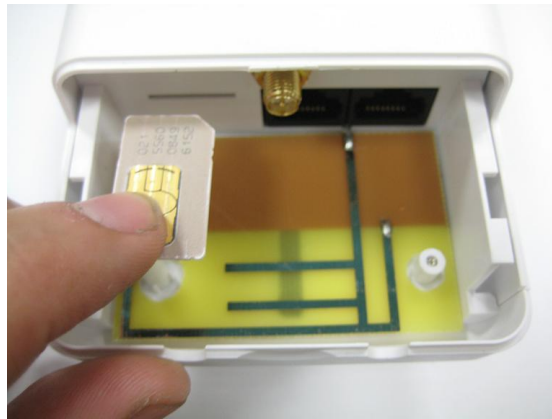


3.1.2 Hardware installation steps

Step1: Push the button in the side to remove upper housing.

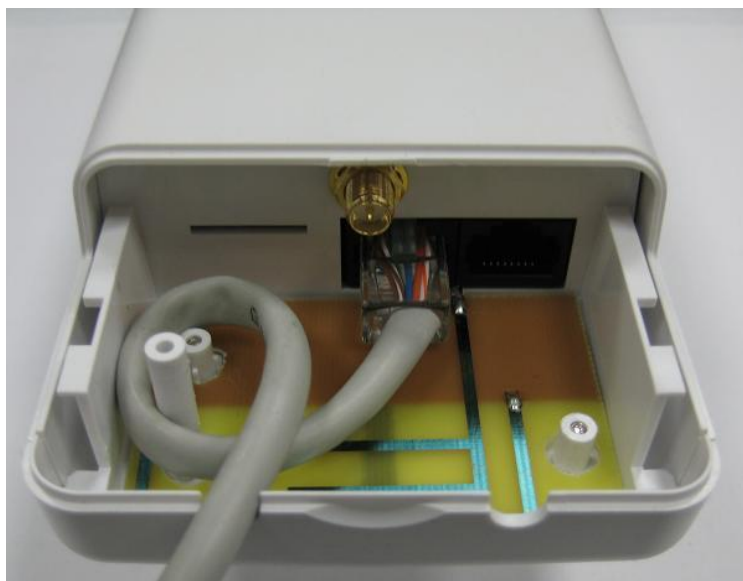


Step2: If you want to use 3G for WAN connection, please insert the 3G SIM card into the SIM slot.



Step3: Pass through Ethernet cable from the hole and insert the cable to LAN port.

Note: RJ-45 8P8C Ethernet cable is required.



Step4: Install the upper housing and make sure the housing is well installed.



Step5:

Install POE Injector

DC: Insert adapter

POE: This hole is linked to LAN port of the Outdoor Router with RJ-45.

LAN: This hole is linked to LAN side PC/Hub or Router/ADSL modem device with RJ-45



Step6: Complete the hardware installation as below diagram .



Notes: Use **Reset button** on POE injector. Push continually the reset button of POE injector about 5 ~ 10 seconds to reset the configuration parameters to factory defaults.



3.2 Software Installation

There is no software driver or utility installation needed, but only the configuration setting. Please refer to chapter 4 for software configuration.

Notice: It will take about 50 seconds to complete the boot up sequence after powered on the Outdoor Router; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.

4. Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The Outdoor Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: 192.168.1.254
Default IP subnet mask: 255.255.255.0
WEB login User Name: admin
WEB login Password: admin

4.1 Prepare your PC to configure the WLAN Broadband Router

For OS of Microsoft Windows 2000/ XP:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Move mouse and double-click the right button on *Network and Dial-up Connections* icon. Move mouse and double-click the *Local Area Connection* icon. The *Local Area Connection* window will appear. Click *Properties* button in the *Local Area Connection* window.
3. Check the installed list of *Network Components*. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
5. Select *TCP/IP* in *Microsoft of Select Network Protocol* dialog box then click *OK* button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
6. Select *TCP/IP* and click the properties button on the *Network* dialog box.
7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: [192.168.1.1](#), any IP address within [192.168.1.1](#) to [192.168.1.253](#) is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: [255.255.255.0](#)
8. Click *OK* to complete the IP parameters setting.

For OS of Microsoft Windows Vista / 7:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Move mouse and double-click the right button on *Network Connections* item. The *Network Connections* window will appear. Double click *Local Area Connection* icon, then User Account Control window shown. Right click *Continue* button to set properties.
3. In *Local Area Connection Properties* window, Choose *Networking* tab, move mouse and click *Internet Protocol Version 4 (TCP/IPv4)*, then click *Properties* button.
4. Move mouse and click *General* tab, Select *Specify an IP address* and type in values as following example.
 - ✓ IP Address: [192.168.1.1](#), any IP address within [192.168.1.1](#) to [192.168.1.253](#) is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: [255.255.255.0](#)
5. Click *OK* to complete the IP parameters setting.

For OS of Microsoft Windows NT:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Move mouse and double-click the right button on *Network* icon. The *Network* window will appear. Click *Protocol* tab from the *Network* window.
3. Check the installed list of *Network Protocol* window. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
5. Select *TCP/IP* in *Microsoft of Select Network Protocol* dialog box then click *OK* button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
6. Select *TCP/IP* and click the properties button on the *Network* dialog box.
7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: [192.168.1.1](#), any IP address within [192.168.1.1](#) to [192.168.1.253](#) is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: [255.255.255.0](#)
8. Click *OK* to complete the IP parameters setting.

4.2 Connect to the WLAN Broadband Router

Open a WEB browser, i.e. Microsoft Internet Explore 6.1 SP1 or above, then enter 192.168.1.254 on the URL to connect the WLAN Broadband Router.

4.3 Management and configuration on the Outdoor Router

4.3.1 Wizard

This Wizard page guides you to configure Internet connection and Wireless Settings quickly.

Setup Wizard

This mode is for home networking. The 'Setup Wizard' will guide you to configure the router to connect to your ISP(Internet Service Provider).

The wizard will guide you through these three quick steps. Begin by clicking on Next.

Step 1. Configure LAN IP address settings.

Step 2. Configure Internet connection.

Step 3. Configure Wireless settings.

Click *Next* button to next step for LAN IP address settings.

Step 1: configure LAN IP address settings

Setup Wizard

This mode is for home networking. The 'Setup Wizard' will guide you to configure the router to connect to your ISP(Internet Service Provider).

Step 1. Configure LAN IP address settings

| LAN Setup | |
|-------------|--|
| IP Address | <input type="text" value="192.168.1.254"/> |
| Subnet Mask | <input type="text" value="255.255.255.0"/> |

Step 2: configure Internet connection



Click *Next* button to next step for Internet connection settings. There are six options (DHCP, Static Mode, PPPOE, L2TP, PPTP, 3G) for Internet connection on WAN port.

a. DHCP (Auto Config)

Step 2. Configure Internet Connection

| | |
|----------------------|----------------------|
| WAN Connection Type: | DHCP (Auto Config) ▼ |
| DHCP Mode | |
| Hostname(optional) | <input type="text"/> |

| | | | |
|------|------|--------|-------|
| Back | Next | Cancel | Apply |
|------|------|--------|-------|

If you select **DHCP** option, please click *Next* button to jump at Step3.

b. Static Mode (fixed IP)

Step 2. Configure Internet Connection

WAN Connection Type:

Static Mode (fixed IP) ▼

| Static Mode | |
|----------------------|----------------------|
| IP Address | <input type="text"/> |
| Subnet Mask | <input type="text"/> |
| Default Gateway | <input type="text"/> |
| Primary DNS Server | <input type="text"/> |
| Secondary DNS Server | <input type="text"/> |

| Item | Description |
|----------------------|---|
| IP Address | Fill in the IP address for WAN interface. |
| Subnet Mask | Fill in the subnet mask for WAN interface. |
| Default Gateway | Fill in the default gateway for WAN interface out going data packets. |
| Primary DNS Server | Fill in the IP address of Domain Name Server 1. |
| Secondary DNS Server | Fill in the IP address of Domain Name Server 2. |

When you finish these settings, then click *Next* button to jump at Step3.

c. PPPOE Connection

Step 2. Configure Internet Connection

WAN Connection Type: PPPOE (ADSL) ▼

| PPPoE Mode | |
|-----------------|--|
| User Name | <input type="text"/> |
| Password | <input type="password"/> |
| Verify Password | <input type="password"/> |
| Operation Mode | Keep Alive ▼ |
| | Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds On demand Mode: Idle Time <input type="text" value="5"/> minutes |

| Item | Description |
|-----------------|--|
| User Name | If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server. |
| Password | If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server. |
| Verify Password | Fill in the password again for verification. |
| Operation Mode | Keep Alive: Keep the PPPoE connection all the time. Please also configure the Redial Period field. On Demand: Please configure the Idle Time field. When time is up, the PPPoE connection will disconnect. The connection will re-connect when any outgoing packet arise. Manual: Let user connect the PPPoE connection manually. |

When you finish these settings, then click *Next* button to jump at Step3.

d. L2TP

Step 2. Configure Internet Connection

WAN Connection Type: L2TP ▼

| L2TP Mode | |
|--|---------------------------|
| Server IP Address | <input type="text"/> |
| User Name | <input type="text"/> |
| Password | <input type="text"/> |
| Address Mode | Static ▼ |
| IP Address | <input type="text"/> |
| Subnet Mask | <input type="text"/> |
| Default Gateway | <input type="text"/> |
| Operation Mode | Keep Alive ▼ |
| Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds | |

Back
Next
Cancel
Apply

If you select **L2TP**, please fill in these fields on next page.

| Item | Description |
|------------------------|---|
| L2TP Server IP Address | Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded L2TP client supported by this router to make a VPN connection. If you select the L2TP support on WAN interface, fill in the IP address for it. |
| User Name | Fill in the user name and password to login the L2TP server. |
| Password | Fill in the user name and password to login the L2TP server. |
| Address Mode | Static: To configure the IP address information by manually, please fill in the related setting at below. Dynamic: The option allows the machine to get IP address information automatically from DHCP server on WAN side. |
| IP Address | Fill in the IP address for WAN interface. |
| Subnet Mask | Fill in the subnet mask for WAN interface. |
| Default Gateway | Fill in the default gateway for WAN interface out going data packets. |
| Operation Mode | Keep Alive: Keep the L2TP connection all the time. Please also configure the Redial Period field. Manual: Let user connect the L2TP connection manually. |

When you finish these settings, then click *Next* button to jump at Step3.

e. PPTP

Step 2. Configure Internet Connection

WAN Connection Type: PPTP ▼

| PPTP Mode | |
|--------------------------------|--|
| Server IP Address(Domain name) | <input type="text"/> |
| User Name | <input type="text"/> |
| Password | <input type="text"/> |
| Address Mode | Static ▼ |
| IP Address | <input type="text"/> |
| Subnet Mask | <input type="text"/> |
| Default Gateway | <input type="text"/> |
| Operation Mode | Keep Alive ▼ |
| | Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds |

Back
Next
Cancel
Apply

| Item | Description |
|------------------------|---|
| PPTP Server IP Address | Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection. If you select the PPTP support on WAN interface, fill in the IP address for it. |
| User Name | Fill in the user name and password to login the PPTP server. |
| Password | Fill in the user name and password to login the PPTP server. |
| Address Mode | Static: To configure the IP address information by manually, please fill in the related setting at below. Dynamic: The option allows the machine to get IP address information automatically from DHCP server on WAN side. |
| IP Address | Fill in the IP address for WAN interface. |
| Subnet Mask | Fill in the subnet mask for WAN interface. |
| Default Gateway | Fill in the default gateway for WAN interface out going data packets. |
| Operation Mode | Keep Alive: Keep the PPTP connection all the time. Please also configure the Redial Period field. Manual: Let user connect the PPTP connection manually. |

When you finish these settings, then click *Next* button to jump at Step3.

f. 3G

Step 2. Configure Internet Connection

WAN Connection Type:

3G

| 3G Mode | |
|--------------|--------------------|
| USB 3G modem | Qualcomm_3G_Module |
| APN | internet |
| PIN | |
| Dial Number | *99# |
| Username | |
| Password | |

Back

Next

Cancel

Apply

| Item | Description |
|--------------|--|
| USB 3G Modem | This field is automatically showing the model name of the embedded 3G modem module. |
| APN | Please input the access point name. |
| PIN | Please input Pin Code for your UMTS or HSDPA connection, this is optional, and only required if your service provider asks you to do so. |
| Dial Number | Please input Dialed Number for your UMTS or HSDPA connection, the default is *99#. This field should not be altered except when required by your service provider. |
| User Name | Please input user name assigned by your Internet service provider here. |
| Password | Please input password assigned by your Internet service provider here. |

When you finish these settings, then click *Next* button to jump at Step3.



Step 3: configure Wireless Settings

There are five options (Disable, WEP, WPA-PSK/WPA2-PSK) for Wireless security connection.

Step 3. Configure Wireless Settings

| Wireless Settings | |
|---------------------|---|
| Wireless Band | 802.11B/G/N ▼ |
| Frequency (Channel) | AutoSelect ▼ Current Channel: 1 |
| Network Name (SSID) | 802.11n_Router |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Security Mode | Disable ▼ |

[Back](#) [Next](#) [Cancel](#) [Apply](#)

1. OPENWEP

Step 3. Configure Wireless Settings

| Wireless Settings | |
|---------------------|---|
| Wireless Band | 802.11B/G/N ▼ |
| Frequency (Channel) | AutoSelect ▼ Current Channel: 1 |
| Network Name (SSID) | 802.11n_Router |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Security Mode | OPENWEP ▼ |
| Pre-Shared Key | |

[Back](#) [Next](#) [Cancel](#) [Apply](#)

2. SHAREDWEP

Step 3. Configure Wireless Settings

| Wireless Settings | |
|---------------------|---|
| Wireless Band | 802.11B/G/N ▼ |
| Frequency (Channel) | AutoSelect ▼ Current Channel: 1 |
| Network Name (SSID) | 802.11n_Router |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Security Mode | SHAREDWEP ▼ |
| Pre-Shared Key | <input type="text"/> |

[Back](#)[Next](#)[Cancel](#)[Apply](#)

3. WPA-PSK

Step 3. Configure Wireless Settings

| Wireless Settings | |
|---------------------|---|
| Wireless Band | 802.11B/G/N ▼ |
| Frequency (Channel) | AutoSelect ▼ Current Channel: 1 |
| Network Name (SSID) | 802.11n_Router |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Security Mode | WPA-PSK ▼ |
| Pre-Shared Key | <input type="text"/> |

[Back](#)[Next](#)[Cancel](#)[Apply](#)

4. WPA2-PSK

Step 3. Configure Wireless Settings

| Wireless Settings | |
|---------------------|---|
| Wireless Band | 802.11B/G/N ▼ |
| Frequency (Channel) | AutoSelect ▼ Current Channel: 1 |
| Network Name (SSID) | 802.11n_Router |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Security Mode | WPA2-PSK ▼ |
| Pre-Shared Key | <input type="text"/> |

| Item | Description |
|---------------------|---|
| Network Mode | Click to select wireless mode from pull down menu. |
| Frequency (Channel) | Select the wireless communication frequency/channel from pull-down menu. |
| Network Name (SSID) | It is the wireless network name. The SSID can be 32 bytes long. |
| Channel Bandwidth | Select the operating channel width 20 MHz or 20/40 MHz. |
| Security | Please select the security mode related wireless data encryption. |
| KEY | WEP: When you select WEP, please input 5, 13 (ASCII), 10 or 26 (HEX) characters for WEP Key. WPA-PSK/WPA2-PSK: When WPA/WPA2 Pre-shared key encryption is selected, please fill in the Pre-shared key. The format can be passphrase or Hex (64 characters). |

When you finish these settings, then click **Apply** button to save.

4.3.2 Operation Mode

a. Bridge:

- ☒ **Bridge:**
All ethernet and wireless interfaces are bridged into a single bridge interface.
- ☐ **Gateway:**
The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
- ☐ **Wireless ISP:**
The wireless apcli interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LAN ports.

:

Apply

Cancel

The **Bridge** mode allows that all Ethernet and wireless interfaces are bridged into a single bridge interface.

b. Gateway:

- ☐ **Bridge:**
All ethernet and wireless interfaces are bridged into a single bridge interface.
- ☒ **Gateway:**
The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
- ☐ **Wireless ISP:**
The wireless apcli interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LAN ports.

:

Apply

Cancel

The **Gateway** mode allows that the first Ethernet port is treated as WAN port and the Ethernet port and the wireless interface are bridged together and are treated as LAN ports.

c. Wireless ISP

☐ **Bridge:**

All ethernet and wireless interfaces are bridged into a single bridge interface.

☐ **Gateway:**

The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

☒ **Wireless ISP:**

The wireless apcli interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LAN ports.

:

Apply

Cancel

The **Wireless ISP** mode allows that the wireless interface is treated as WAN port, and the Ethernet ports are LAN port.

4.3.3 Internet Settings

4.3.3.1 WAN

a. STATIC

WAN Connection Type: STATIC (fixed IP) ▼

| Static Mode | |
|----------------------|------------------------|
| IP Address | <input type="text"/> |
| Subnet Mask | <input type="text"/> |
| Default Gateway | <input type="text"/> |
| Primary DNS Server | <input type="text"/> |
| Secondary DNS Server | <input type="text"/> |
| MAC Clone | |
| Enabled | Disable ▼ |

Apply Cancel

| Item | Description |
|----------------------|---|
| IP Address | Fill in the IP address for WAN interface. |
| Subnet Mask | Fill in the subnet mask for WAN interface. |
| Default Gateway | Fill in the default gateway for WAN interface out going data packets. |
| Primary DNS Server | Fill in the IP address of Domain Name Server 1. |
| Secondary DNS Server | Fill in the IP address of Domain Name Server 2. |
| MAC Clone | Take NIC MAC address of PC on LAN side as the MAC address of WAN interface. |

b. DHCP

WAN Connection Type:

DHCP (Auto config) ▼

| DHCP Mode | |
|------------------------|----------------------|
| Hostname (optional) | <input type="text"/> |
| MAC Clone | |
| Enabled | Disable ▼ |

Apply

Cancel

| Item | Description |
|-----------|--|
| Hostname | Fill in the host name of Host Name of DHCP server. The default value is empty. |
| MAC Clone | Take NIC MAC address of PC on LAN side as the MAC address of WAN interface. |

c. PPPoE

WAN Connection Type: PPPoE (ADSL) ▼

| PPPoE Mode | |
|-----------------|--|
| User Name | <input type="text"/> |
| Password | <input type="password"/> |
| Verify Password | <input type="password"/> |
| Operation Mode | Keep Alive ▼ |
| | Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds On demand Mode: Idle Time <input type="text" value="5"/> minutes |
| MAC Clone | |
| Enabled | Disable ▼ |

Apply Cancel

| Item | Description |
|-----------------|---|
| User Name | If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server. |
| Password | If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server. |
| Verify Password | Fill in the password again for verification. |
| Operation Mode | Keep Alive: Keep the PPTP connection all the time. Please also configure the Redial Period field. Manual: Let user connect the PPTP connection manually. |
| MAC Clone | Take NIC MAC address of PC on LAN side as the MAC address of WAN interface. |

d. L2TP

WAN Connection Type: L2TP

| L2TP Mode | |
|--|--------------------------|
| Server IP | <input type="text"/> |
| User Name | <input type="text"/> |
| Password | <input type="password"/> |
| Address Mode | Static |
| IP Address | <input type="text"/> |
| Subnet Mask | <input type="text"/> |
| Default Gateway | <input type="text"/> |
| Operation Mode | Keep Alive |
| Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds | |

| MAC Clone | |
|-----------|----------------------|
| Enabled | Disable |

Apply Cancel

| Item | Description |
|-----------------|---|
| Server IP | Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded L2TP client supported by this router to make a VPN connection. If you select the L2TP support on WAN interface, fill in the IP address for it. |
| User Name | Fill in the user name and password to login the L2TP server. |
| Password | Fill in the user name and password to login the L2TP server. |
| Address Mode | Static: To configure the IP address information by manually, please fill in the related setting at below. Dynamic: The option allows the machine to get IP address information automatically from DHCP server on WAN side. |
| IP Address | Fill in the IP address for WAN interface. |
| Subnet Mask | Fill in the subnet mask for WAN interface. |
| Default Gateway | Fill in the default gateway for WAN interface out going data packets. |
| Operation Mode | Keep Alive: Keep the L2TP connection all the time. Please also configure the Redial Period field. On Demand: Please configure the Idle Time field. When time is up, the L2TP connection will disconnect. The connection will re-connect when any outgoing packet arise. Manual: Let user connect the L2TP connection manually. |
| MAC Clone | Take NIC MAC address of PC on LAN side as the MAC address of WAN interface. |

e. PPTP

WAN Connection Type: PPTP

| PPTP Mode | |
|--|-------------------------|
| Server IP | <input type="text"/> |
| User Name | <input type="text"/> |
| Password | <input type="text"/> |
| Address Mode | Static |
| IP Address | <input type="text"/> |
| Subnet Mask | <input type="text"/> |
| Default Gateway | <input type="text"/> |
| Operation Mode | Keep Alive |
| Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds | |

| MAC Clone | |
|-----------|----------------------|
| Enabled | Disable |

Apply Cancel

| Item | Description |
|-----------------|---|
| Server IP | Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection. If you select the PPTP support on WAN interface, fill in the IP address for it. |
| User Name | Fill in the user name and password to login the PPTP server. |
| Password | Fill in the user name and password to login the PPTP server. |
| Address Mode | Static: To configure the IP address information by manually, please fill in the related setting at below. Dynamic: The option allows the machine to get IP address information automatically from DHCP server on WAN side. |
| IP Address | Fill in the IP address for WAN interface. |
| Subnet Mask | Fill in the subnet mask for WAN interface. |
| Default Gateway | Fill in the default gateway for WAN interface out going data packets. |
| Operation Mode | Keep Alive: Keep the PPTP connection all the time. Please also configure the Redial Period field. On Demand: Please configure the Idle Time field. When time is up, the PPTP connection will disconnect. The connection will re-connect when any outgoing packet arise. Manual: Let user connect the PPTP connection manually. |
| MAC Clone | Take NIC MAC address of PC on LAN side as the MAC address of WAN interface. |

f. 3G

WAN Connection Type: 3G ▼

| 3G Mode | |
|-------------|------------------------|
| 3G Modem | Unconnected |
| APN | internet |
| PIN | |
| Dial Number | *99# |
| Username | |
| Password | |
| MAC Clone | |
| Enabled | Disable ▼ |

| Item | Description |
|--------------|--|
| USB 3G Modem | This field is automatically showing the model name of the embedded 3G modem module. |
| APN | Please input the access point name. |
| PIN | Please input Pin Code for your UMTS or HSDPA connection, this is optional, and only required if your service provider asks you to do so. |
| Dial Number | Please input Dialed Number for your UMTS or HSDPA connection, the default is *99#. This field should not be altered except when required by your service provider. |
| User Name | Please input user name assigned by your Internet service provider here. |
| Password | Please input password assigned by your Internet service provider here. |
| MAC Clone | Take NIC MAC address of PC on LAN side as the MAC address of WAN interface. |

4.3.3.2 LAN

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

| LAN Setup | |
|----------------------|--|
| MAC Address | 00:1A:EF:19:67:5B |
| IP Address | <input type="text" value="192.168.1.254"/> |
| Subnet Mask | <input type="text" value="255.255.255.0"/> |
| DHCP Type | Server <input type="button" value="v"/> |
| Start IP Address | <input type="text" value="192.168.1.100"/> |
| End IP Address | <input type="text" value="192.168.1.200"/> |
| Lease Time | <input type="text" value="86400"/> |
| 802.1d Spanning Tree | Disable <input type="button" value="v"/> |
| LLTD | Disable <input type="button" value="v"/> |
| IGMP Proxy | Disable <input type="button" value="v"/> |
| UPNP | Disable <input type="button" value="v"/> |
| DNS Proxy | Disable <input type="button" value="v"/> |

| Item | Description |
|----------------------|--|
| MAC Address | Show the MAC address of LAN interface. |
| IP Address | Fill in the IP address of LAN interfaces. |
| Subnet Mask | Fill in the subnet mask of LAN interfaces. |
| Default Gateway | Fill in the default gateway for LAN interfaces out going data packets. |
| DHCP Type | Disable: Disable DHCP server on LAN side. Server: Enable DHCP server on LAN side. |
| Start IP Address | Fill in the start IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range. |
| End IP Address | Fill in the end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range. |
| Lease Time | Fill in the lease time of DHCP server function. |
| 802.1d Spanning Tree | Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. |

| | |
|------------|---|
| LLTD | Select enable or disable the Link Layer Topology Discover function from pull-down menu. |
| IGMP Proxy | Select enable or disable the IGMP proxy function from pull-down menu. |
| UPNP | Select enable or disable the UPnP protocol from pull-down menu. |
| DNS Proxy | Select enable or disable the DNS Proxy function from pull-down menu. |

4.3.3.3 DHCP clients

The “DHCP clients” page shows all the active DHCP clients. The table window shows the active clients with their Hostname, MAC address, assigned IP address, and time expired information.

DHCP Client List

You could monitor DHCP clients here.

| DHCP Clients | | | |
|--------------|-------------------|---------------|------------|
| Hostname | MAC Address | IP Address | Expires in |
| networktest | 00:24:1D:C6:6C:8A | 192.168.1.100 | 23:55:27 |

Refresh

4.3.3.4 VPN Passthrough

| VPN Pass Through | |
|-------------------|----------|
| L2TP Passthrough | Enable ▾ |
| IPSec Passthrough | Enable ▾ |
| PPTP Passthrough | Enable ▾ |

Apply Cancel

| Item | Description |
|-------------------|---|
| L2TP Passthrough | Select enable or disable the L2TP pass-through function from pull-down menu. |
| IPSec Passthrough | Select enable or disable the IPSec pass-through function from pull-down menu. |
| PPTP Passthrough | Select enable or disable the PPTP pass-through function from pull-down menu. |

4.3.4 Wireless Settings

4.3.4.1 Basic

| Wireless Network | |
|-------------------------------|--|
| Wireless On/Off | <input type="button" value="Wireless OFF"/> Current Status:Radio ON |
| Antenna Switch | <input type="radio"/> External <input checked="" type="radio"/> Internal |
| Wireless Mode | <input type="text" value="AP"/> |
| Wireless Band | <input type="text" value="802.11B/G/N"/> |
| SSID | <input type="text" value="802.11n_Router"/> |
| Broadcast Network Name (SSID) | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| AP Isolation | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| BSSID | <input type="text" value="00:1A:EF:3E:DB:08"/> |
| Frequency (Channel) | <input type="text" value="AutoSelect"/> Current Channel: 1 |
| HT Physical Mode | |
| Operating Mode | <input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Guard Interval | <input type="radio"/> Long <input checked="" type="radio"/> Auto |
| MCS | <input type="text" value="Auto"/> |

| Item | Description |
|-------------------------------|--|
| Wireless On/Off | Click Wireless OFF button to turn off wireless RF radio. Click Wireless ON button to turn on wireless RF radio. |
| Antenna Switch | Select Internal antenna or External antenna for using. The default is using Internal antenna. |
| Wireless Mode | Click to select wireless mode from pull down menu. |
| SSID | It is the wireless network name. The SSID can be 32 bytes long. User can use the default SSID or change it. |
| Broadcast Network Name (SSID) | Enable or disable the SSID broadcast function. |
| AP Isolation | Wireless network is similar to the virtual local area network. All of the Wireless client devices can access each other completely. When you enable this function, it will turn off connection between wireless clients. Only allows connection between wireless client and this AP router. |

| | |
|---------------------|--|
| BSSID | Show the MAC address of Wireless interface. |
| Frequency (Channel) | Select the wireless communication frequency/channel from pull-down menu. |
| Operating Mode | Select “Mixed Mode” for 11b/g/n mode or “Green Field” for 11n mode. |
| Channel BandWidth | Select the operating channel width 20 MHz or 20/40 MHz. |
| Guard Interval | Select “Long” or “Auto”. Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Only effect under Mixed Mode. |
| MCS | Select 0~7 or “Auto” from pull down menu. The default is “Auto”. Only effect under Mixed Mode. |

4.3.4.2 Advanced

| Advanced Wireless | |
|-------------------------|---|
| B/G Protection Mode | Auto ▼ |
| Beacon Interval | 100 ms (range 20 - 999, default 100) |
| Data Beacon Rate (DTIM) | 1 ms (range 1 - 255, default 1) |
| Fragment Threshold | 2346 (range 256 - 2346, default 2346) |
| RTS Threshold | 2347 (range 1 - 2347, default 2347) |
| TX Power | 100 (range 1 - 100, default 100) |
| Short Preamble | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Short Slot | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Tx Burst | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Country Code | US (United States) ▼ |

| Item | Description |
|-----------------------|---|
| B/G Protection Mode | Default: Auto . You can select the other options including On and Off . The B/G protection technology is CTS-To-Self. It will try to reserve the throughput for 11g clients from 11b clients connecting to the device as AP mode. |
| Beacon Interval | Beacons are the packets sending by Access point to synchronize the wireless network. The beacon interval is the time interval between beacons sending by this unit in AP or AP+WDS operation. The default and recommended beacon interval is 100 milliseconds. |
| Data Beacon Rate(DTM) | This is the Delivery Traffic Indication Map. It is used to alert the clients that multicast and broadcast packets buffered at the AP will be transmitted immediately after the transmission of this beacon frame. You can change the value from 1 to 255. The AP will check the buffered data according to this value. For example, selecting "1" means to check the buffered data at every beacon. |
| Fragment Threshold | The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help you to improve the network performance. |
| RTS Threshold | The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347 bytes. |
| TX Power | The default TX power is 100%. In case of shortening the distance and the coverage |

| | |
|----------------|---|
| | of the wireless network, input a smaller value to reduce the radio transmission power. For example, input 80 to apply 80% Tx power. |
| Short Preamble | Default: Disable. It is a performance parameter for 802.11 b/g mode and not supported by some of very early stage of 802.11b station cards. If there is no such kind of stations associated to this AP, you can enable this function. |
| Short Slot | It is used to shorten the communication time between this AP and station. |
| TX Burst | The device will try to send a serial of packages with single ACK reply from the clients. Enable this function to apply it. |
| Country Code | Select the country code for wireless from pull down menu. |

4.3.4.3 Security

a. Disable

| Security Wireless | |
|-------------------|-----------|
| Security Mode | Disable ▼ |

If you set Security Mode to “**Disable**”, the wireless data transmission will not include encryption to prevent from unauthorized access and monitoring.

b. OPEN-WEP // SHARED-WEP

| Security Wireless | |
|-------------------|------------|
| Security Mode | OPEN-WEP ▼ |

| Wire Equivalence Protection (WEP) | | | |
|-----------------------------------|-------------|----------------------|-------|
| Default Key | | Key 1 ▼ | |
| WEP Keys | WEP Key 1 : | <input type="text"/> | Hex ▼ |
| | WEP Key 2 : | <input type="text"/> | Hex ▼ |
| | WEP Key 3 : | <input type="text"/> | Hex ▼ |
| | WEP Key 4 : | <input type="text"/> | Hex ▼ |

If you set Security Mode to “**OPEN-WEP or SHARED-WEP**”, please fill in the related configurations as below.

| Item | Description |
|----------------|--|
| Default Key | Specify a Key number for effective. |
| WEP Keys (1~4) | When you select WEP AUTO, please input 5, 13 (ASCII), 10 or 26 (HEX) characters for WEP Key. |

c. WPAPSK/WPA2PSK

| Security Wireless | |
|-------------------|------------------------|
| Security Mode | WPA-PSK ▼ |

| WPA | |
|----------------------|---|
| WPA Cipher Suite | <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES |
| Pre-Shared Key | <input type="text"/> |
| Key Renewal Interval | <input type="text" value="3600"/> seconds (60 ~ 9999) |

| Security Wireless | |
|-------------------|-------------------------|
| Security Mode | WPA2-PSK ▼ |

| WPA | |
|----------------------|---|
| WPA Cipher Suite | <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES |
| Pre-Shared Key | <input type="text"/> |
| Key Renewal Interval | <input type="text" value="3600"/> seconds (60 ~ 9999) |

If you set Security Mode to “**WPAPSKWPA2PSK**”, please fill in the related configurations as below.

| Item | Description |
|----------------------|---|
| WPA Algorithms | Select TKIP , AES , or TKIPAES for WPA algorithms. |
| Pre-Shared key | Please fill in a passphrase like ‘test wpa 123’, or a hexadecimal string like ‘65E4 E123 456 E1’. |
| Key Renewal Interval | Please fill in a number for Group Key Renewal interval time. |

d. WPA-RADIUS

| Security Wireless | |
|----------------------|---|
| Security Mode | WPA-RADIUS ▼ |
| WPA | |
| WPA Cipher Suite | <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES |
| Key Renewal Interval | <input type="text" value="3600"/> seconds (60 ~ 9999) |
| Radius Server | |
| IP Address | <input type="text"/> |
| Port | <input type="text" value="1812"/> |
| Shared Secret | <input type="text"/> |
| Session Timeout | <input type="text" value="0"/> |
| Idle Timeout | <input type="text"/> |

If you set Security Mode to “**WPA-RADIUS**”, please fill in the related configurations as below.

| Item | Description |
|----------------------|---|
| WPA Cipher Suite | Select TKIP , AES , or TKIPAES for WPA algorithms. |
| Key Renewal Interval | Please fill in a number for Group Key Renewal interval time. |
| IP Address | Enter the RADIUS Server’s IP Address provided by your ISP. |
| Port | Enter the RADIUS Server’s port number provided by your ISP. (The Default is 1812.) |
| Shared Secret | Enter the password that the Wireless Router shares with the RADIUS Server. |
| Session Timeout | Session timeout interval is for 802.1x re-authentication setting. Set to zero to disable 802.1x re-authentication service for each session. Session timeout interval unit is second and must be larger than 60. |
| Idle Timeout | Enter the idle timeout in the column. |

f. 802.1X

| Security Wireless | |
|-------------------|---|
| Security Mode | 802.1X <input type="button" value="v"/> |

| 802.1x WEP | |
|------------|--|
| WEP | <input type="radio"/> Disable <input type="radio"/> Enable |

| Radius Server | |
|-----------------|---------------------------|
| IP Address | <input type="text"/> |
| Port | 1812 <input type="text"/> |
| Shared Secret | <input type="text"/> |
| Session Timeout | 0 <input type="text"/> |
| Idle Timeout | <input type="text"/> |

| Item | Description |
|-----------------|---|
| IP Address | Enter the RADIUS Server's IP Address provided by your ISP. |
| Port | Enter the RADIUS Server's port number provided by your ISP. (The Default is 1812.) |
| Session Timeout | Session timeout interval is for 802.1x re-authentication setting. Set to zero to disable 802.1x re-authentication service for each session. Session timeout interval unit is second and must be larger than 60. |
| Idle Timeout | Enter the idle timeout in the column. |
| Shared Secret | Enter the password that the Wireless Router shares with the RADIUS Server. |

g. Access Policy

| Access Policy | |
|--------------------|---|
| Policy | Disabled <input type="button" value="v"/> |
| Add a station Mac: | <input type="text"/> |

| Item | Description |
|-------------------|---|
| Policy | Select the Disabled , Allow or Reject of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this WLAN Broadband Router. |
| Add a station MAC | Fill in the MAC address of client to register this router access capability. |

4.3.4.4 WPS

| WPS Config | |
|------------|--|
| WPS: | Enabled <input type="button" value="v"/> |

| WPS Summary | |
|--|--|
| WPS Current Status: | Not used |
| WPS Configured: | Yes |
| WPS SSID: | 802.11n_Router |
| WPS Auth Mode: | Open |
| WPS Encryp Type: | None |
| WPS Default Key Index: | 1 |
| WPS Key(ASCII) | |
| AP PIN: | 16259799 <input type="button" value="Generate"/> |
| <input type="button" value="Reset OOB"/> | |

| WPS Progress | |
|--------------------------------------|--|
| WPS mode | <input checked="" type="radio"/> PIN <input type="radio"/> PBC |
| PIN | <input type="text"/> |
| <input type="button" value="Apply"/> | |

| Item | Description |
|-------------|---|
| WPS | Select Enable or Disable the Wi-Fi Protected Setup function. Then click Apply button to take effect function after change. |
| WPS Summary | After enabling the WPS function, if there is connection the WPS Summary will show related information and status. |
| AP PIN | Here shows the AP's PIN code (Personal Identification Number) that the enrollee should enter the registrar's PIN code to make a connection. Click Generate button to generate a new AP PIN code. |
| Reset OOB | Click Reset OOB button to reset WPS AP to the OOB (out-of-box) configuration. |
| WPS mode | Select WPS mode. PIN : Personal Identification Number. PBC : Push Button Communication. |
| PIN | Input enrollee's PIN code to AP-registrar. |

4.3.5 Firewall

4.3.5.1 MAC/IP/Port Filtering

MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

| Basic Settings | |
|-----------------------|-----------|
| MAC/IP/Port Filtering | Disable ▾ |

| Item | Description |
|-----------------------|--|
| MAC/IP/Port Filtering | Select Enable or Disable the MAC/IP/Port Filtering function. |

| MAC/IP/Port Filter Settings | |
|-----------------------------|---|
| Source MAC address | <input type="text"/> |
| Dest IP Address | <input type="text"/> |
| Source IP Address | <input type="text"/> |
| Protocol | None <input type="button" value="v"/> |
| Dest Port Range | <input type="text"/> - <input type="text"/> |
| Source Port Range | <input type="text"/> - <input type="text"/> |
| Action | Accept <input type="button" value="v"/> |
| Comment | <input type="text"/> |

(The maximum rule count is 32.)

| Item | Description |
|--------------------|---|
| Source MAC address | Fill in the MAC address of source NIC, to restrict data transmission. |
| Dest IP Address | Fill in the IP address of destination, to restrict data transmission. |
| Source IP Address | Fill in the IP address of source, to restrict data transmission. |
| Protocol | Select the protocol that you want to restrict. There are four options: None, TCP, UDP and ICMP. |
| Dest Port Range | Fill in the start-port and end-port number of destination, to restrict data transmission. |
| Source Port Range | Fill in the start-port and end-port number of source, to restrict data transmission. |
| Action | Select Accept or Drop to specify the action of filtering policies. |
| Comment | Make a comment for the filtering policy. |

| Current MAC/IP/Port filtering rules in system: | | | | | | | | | |
|--|--------------------|-----------------|-------------------|----------|-----------------|-------------------|--------|---------|---------|
| No. | Source MAC address | Dest IP Address | Source IP Address | Protocol | Dest Port Range | Source Port Range | Action | Comment | Pkt Cnt |
| Others would be dropped | | | | | | | | | - |

| Item | Description |
|--------------------------|--|
| <input type="checkbox"/> | Make a mark for next action. |
| Delete Selected | Click Delete Selected button to delete all that you selected. |
| Reset | Click Reset button to clear selected items. |

4.3.5.2 Port Forwarding

| Port Forwarding | |
|-----------------|---|
| Port Forwarding | Disable ▾ |
| IP Address | <input type="text"/> |
| Port Range | <input type="text"/> - <input type="text"/> |
| Protocol | TCP&UDP ▾ |
| Comment | <input type="text"/> |

(The maximum rule count is 32.)

| Item | Description |
|-----------------|--|
| Port Forwarding | Select Enable or Disable the Port Forwarding function. |
| IP Address | To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address. |
| Port Range | To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the port range. |
| Protocol | Specify protocol, TCP&UDP, TCP or UDP. |
| Comment | Make a comment for the port forwarding policy. |

4.3.5.3 DMZ

DMZ Settings

You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

| DMZ Settings | |
|----------------|----------------------|
| DMZ Settings | Disable ▼ |
| DMZ IP Address | <input type="text"/> |

| Item | Description |
|----------------|---|
| DMZ Settings | Enable or Disable the DMZ function. |
| DMZ IP Address | To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface. |

4.3.5.4 System Security

System Security Settings

You may configure the system firewall to protect AP/Router itself from attacking.

| Remote management | |
|-----------------------------|--------|
| Remote management (via WAN) | Deny ▼ |

| Ping form WAN Filter | |
|----------------------|-----------|
| Ping form WAN Filter | Disable ▼ |

| Stateful Packet Inspection (SPI) | |
|----------------------------------|-----------|
| SPI Firewall | Disable ▼ |

| Item | Description |
|----------------------|--|
| Remote management | Select Deny or Allow for remote management function. |
| Ping form WAN Filter | Select Disable or Enable for Ping permit from WAN. |
| SPI Firewall | Select Disable or Enable for SPI firewall function. |

4.3.5.5 Content Filtering

Webs URL Filter Settings

Add a URL filter:

URL:

Add
Reset

Current Webs URL Filters:

| No | URL |
|----------------------------|----------------|
| 1 <input type="checkbox"/> | www.google.com |

Delete
Reset

| Item | Description |
|--------------------------|--|
| Filters | Select an option or multi-option for Webs content filter. Then click Apply button to save or click Reset button to clear all. |
| URL | Fill in a URL string for URL filter. Then click Add button to save the URL filter policy or click Reset button to clear the field. |
| <input type="checkbox"/> | Make a mark for next action. |
| Delete | Click Delete button to delete all that you selected. |
| Reset | Click Reset button to clear selected items. |

Webs Host Filter Settings

| Add a Host(keyword) Filter: | |
|------------------------------------|--------------------------------------|
| Keyword | <input type="text"/> |
| <input type="button" value="Add"/> | <input type="button" value="Reset"/> |

| Current Website Host Filters: | |
|---------------------------------------|--------------------------------------|
| No | Host(Keyword) |
| 1 <input type="checkbox"/> | test |
| <input type="button" value="Delete"/> | <input type="button" value="Reset"/> |

| Item | Description |
|--------------------------|---|
| Keyword | Fill in a word for Webs Host Filter policy. |
| <input type="checkbox"/> | Make a mark for next action. |
| Delete | Click Delete button to delete all that you selected. |
| Reset | Click Reset button to clear selected items. |

4.3.6 Administration

4.3.6.1 Management

System Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

| Language Settings | |
|--|-----------|
| Select Language | English ▼ |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| Administrator Settings | |
|--|-------|
| Username | admin |
| Password | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| NTP Settings | |
|--|--|
| Current Time | Sat Jan 1 03:11:35 UTC 2000 <input type="button" value="Sync with host"/> |
| Time Zone: | (GMT-11:00) Midway Island, Samoa ▼ |
| NTP Server | <input type="text"/> ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw |
| NTP synchronization(hours) | <input type="text"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

| Item | Description |
|---------------------|---|
| Username | Fill in the user name for web management login control. |
| Password | Fill in the password for web management login control. |
| Current Time | It shows the current time. |
| Time Zone | Select the time zone in your country from pull-down menu.. |
| NTP Server | Fill in NTP server IP address. |
| NTP synchronization | Fill in a number to decide the synchronization frequency with NTP server. |

| DDNS Settings | |
|----------------------|--------------------------|
| Dynamic DNS Provider | None ▼ |
| Account | <input type="text"/> |
| Password | <input type="password"/> |
| DDNS | <input type="text"/> |

| Item | Description |
|----------------------|---|
| Dynamic DNS Provider | Click the drop down menu to pick up the right DDNS provider you registered. |
| Account | Fill in the account of DDNS you registered. |
| Password | Fill in the password of DDNS you registered. |
| DDNS | Fill in the domain name that you registered. |

4.3.6.2 QOS

Quality of Service Settings

You may setup rules to provide Quality of Service guarantees for specific applications.

| QoS Setup | | | | |
|--------------------------------------|---|-------------------------|---------------------------|--------|
| Quality of Service | Enable ▼ | | | |
| QoS Rules Setting | | | | |
| Local IP Address: | <input type="text"/> - <input type="text"/> | | | |
| Uplink BandWidth(Kbps): | <input type="text"/> | | | |
| Downlink BandWidth(Kbps): | <input type="text"/> | | | |
| <input type="button" value="Apply"/> | | | | |
| No. | Local IP Address | Uplink BandWidth(Kbps): | Downlink BandWidth(Kbps): | Select |

| Item | Description |
|--------------------|-------------------------------|
| Local IP Address | Fill in the local IP address |
| Uplink Bandwidth | Fill limit upload bandwidth |
| Downlink Bandwidth | Fill limit downlink bandwidth |

4.3.6.3 Upload Firmware

Firmware Upgrade

Upgrade the Device firmware to obtain new functionality. It takes about 1 minute to upload upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

| Update Firmware | |
|--------------------------------------|--|
| Location: | <input type="text"/> <input type="button" value="Browse"/> |
| <input type="button" value="Apply"/> | |

| Item | Description |
|----------|---|
| Location | Click the <i>Browse</i> button to select the new firmware image file on PC. And click the <i>Apply</i> button to upgrade firmware. |

4.3.6.4 Backup & Restore

Backup & Restore

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

| Export Settings | |
|-----------------|---------------------------------------|
| Export Button | <input type="button" value="Export"/> |

| Import Settings | |
|---|--|
| Settings file location | <input type="text"/> <input type="button" value="Browse"/> |
| <input type="button" value="Import"/> <input type="button" value="Cancel"/> | |

| Load Factory Defaults | |
|-----------------------|---|
| Load Default Button | <input type="button" value="Load Default"/> |

| Item | Description |
|------------------------|--|
| Export Button | Click Export button to export the current configuration to your PC. |
| Settings file location | Click Browse button to select the configuration file from your PC, then click Import button to update the configuration. |
| Load Default Button | Click the Load Default button to reset the configuration parameter to factory defaults. |

4.3.6.5 Status

This page shows the current status and some basic settings of the device, includes system info, Internet Configurations and Local Network.

Access Point Status

This page show the current status and some basic settings of the device.

| System Information | |
|----------------------|---------------------------|
| Firmware Version | 1.0.22-3G |
| System Up Time | 2 hours, 12 mins, 58 secs |
| Operation Mode | AP Client Mode |
| Wireless Information | |
| Status | Radio ON |
| Mode | AP+WDS |
| SSID | 802.11n_Router |
| Channel | 2 |
| Encryption | OPEN |
| BSSID | 00:1A:EF:18:CF:7B |
| WAN Information | |
| Connected Type | 3G |
| WAN IP Address | |
| Subnet Mask | |
| Default Gateway | |
| DNS1 | |
| DNS2 | |
| MAC Address | 00:1A:EF:18:CF:7C |
| LAN Information | |
| DHCP Server | Enabled |
| LAN IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| MAC Address | 00:1A:EF:18:CF:7B |

4.3.6.6 System Log

This page is used to view system logs.

System Log

Syslog:

System Log

```

Jan  1 01:30:07 ralink syslog.info syslogd started: BusyBox v1.12.1
Jan  1 01:30:08 ralink user.notice kernel: klogd started: BusyBox v1.12.1 (2011-
Jan  1 01:30:11 ralink user.info kernel: br0: topology change detected, propagat
Jan  1 01:30:11 ralink user.info kernel: br0: port 2(eth2) entering forwarding s
Jan  1 01:30:11 ralink user.info kernel: br0: topology change detected, propagat
Jan  1 01:30:11 ralink user.info kernel: br0: port 1(ra0) entering forwarding st
Jan  1 01:30:14 ralink user.debug kernel: apcli0: no IPv6 routers present
Jan  1 01:48:14 ralink user.warn kernel: Rcv Wcid(1) AddBAREq
Jan  1 01:48:14 ralink user.warn kernel: Start Seq = 00000000
Jan  1 01:48:24 ralink user.warn kernel: 43, flush one!

```

| Item | Description |
|---------|--|
| Refresh | Click the <i>Refresh</i> button to refresh the log shown on the screen. |
| Clear | Click the <i>Clear</i> button to clear the log display screen. |

4.4 Configuration Examples

4.4.1 Example one – PPPoE on the WAN

Sales division of Company ABC likes to establish a WLAN network to support mobile communication on sales' Notebook PCs. MIS engineer collects information and plans the WLAN Broadband Router implementation by the following configuration.

WAN configuration:PPPoE

| | |
|-----------|-------------|
| User Name | user123 |
| Password | password123 |

Note: User Name and password that ISP provided.

LAN configuration:

| | |
|-------------------|------------------------------|
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| DHCP Client Range | 192.168.1.100 –192.168.1.200 |

WLAN configuration:

| | |
|----------------|------------|
| SSID | AP |
| Channel Number | AutoSelect |

1. Configure the WAN interface:

Open “Wide Area Network (WAN) Settings” page, select PPPoE then enter the User Name “user123” and Password “password123”, the password is encrypted to display on the screen.

Press “Apply” button to confirm the configuration setting.

Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: PPPoE (ADSL) ▼

| PPPoE Mode | |
|-----------------|--|
| User Name | <input type="text" value="User123"/> |
| Password | <input type="password" value="••••••••"/> |
| Verify Password | <input type="password" value="••••••••"/> |
| Operation Mode | Keep Alive ▼ |
| | Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds |
| | On demand Mode: Idle Time <input type="text" value="5"/> minutes |
| MAC Clone | |
| Enabled | Disable ▼ |

Apply Cancel

2. Configure the LAN interface:

Open “Local Area Network (LAN) settings” page, enter the IP Address “192.168.1.254”, Subnet Mask “255.255.255.0”. Enable DHCP Server, DHCP client range “192.168.1.100” to “192.168.1.200”, default Gateway “10.10.10.254” .

Press “Apply” button to confirm the configuration setting.

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

| LAN Setup | |
|----------------------|--|
| MAC Address | 00:1A:EF:18:CF:7B |
| IP Address | <input type="text" value="192.168.1.254"/> |
| Subnet Mask | <input type="text" value="255.255.255.0"/> |
| DHCP Type | Server <input type="button" value="v"/> |
| Start IP Address | <input type="text" value="192.168.1.100"/> |
| End IP Address | <input type="text" value="192.168.1.200"/> |
| Lease Time | <input type="text" value="86400"/> |
| 802.1d Spanning Tree | Disable <input type="button" value="v"/> |
| LLTD | Disable <input type="button" value="v"/> |
| IGMP Proxy | Disable <input type="button" value="v"/> |
| UPNP | Disable <input type="button" value="v"/> |
| DNS Proxy | Disable <input type="button" value="v"/> |

3. Configure the WLAN interface:

Open “Basic Wireless Settings” page, enter the SSID “AP”, Channel Number “AutoSelect”.

Press “Apply” button to confirm the configuration setting.

| Wireless Network | |
|-------------------------------|---|
| Wireless On/Off | <div>Wireless OFF</div> <div>Current Status:Radio ON</div> |
| Wireless Mode | AP+WDS |
| Wireless Band | 802.11B/G/N |
| SSID | AP |
| Broadcast Network Name (SSID) | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| AP Isolation | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| MBSSID AP Isolation | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| BSSID | 00:1A:EF:18:CF:7B |
| Frequency (Channel) | <div>AutoSelect</div> <div>Current Channel: 1</div> |
| HT Physical Mode | |
| Operating Mode | <input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Guard Interval | <input type="radio"/> Long <input checked="" type="radio"/> Auto |
| MCS | Auto |

Apply

Cancel

4.4.2 Example two – fixed IP on the WAN

Company ABC likes to establish a WLAN network to support mobile communication on all employees' Notebook PCs. MIS engineer collects information and plans the WLAN Broadband Router implementation by the following configuration.

WAN configuration : Fixed IP

| | |
|---------------------|---------------|
| IP Address | 10.10.10.10 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.10.10.1 |
| Primary DNS Address | 168.95.1.1 |

LAN configuration:

| | |
|-------------------|------------------------------|
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| DHCP Client Range | 192.168.1.50 – 192.168.1.150 |

WLAN configuration:

| | |
|----------------|---------------------|
| SSID | RalinkInitAP_1906B8 |
| Channel Number | AutoSelect |

1. Configure the WAN interface:

Open “Wide Area Network (WAN) Settings” page, select STATIC(fixed IP) then enter IP Address

“10.10.10.10”, subnet mask “255.255.255.0”, Default gateway “10.10.10.1”.

Press “Apply” button to confirm the configuration setting.

Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: STATIC (fixed IP) ▼

| Static Mode | |
|----------------------|--|
| IP Address | <input type="text" value="10.10.10.10"/> |
| Subnet Mask | <input type="text" value="255.255.255.0"/> |
| Default Gateway | <input type="text" value="10.10.10.1"/> |
| Primary DNS Server | <input type="text" value="168.95.1.1"/> |
| Secondary DNS Server | <input type="text"/> |
| MAC Clone | |
| Enabled | Disable ▼ |

Apply Cancel

2. Configure the LAN interface:

Open "Local Area Network (LAN) settings" page, enter the IP Address

"192.168.1.254", Subnet Mask

"255.255.255.0". Enable DHCP Server, DHCP client range "192.168.1.50" to

"192.168.1.150", default

Gateway "192.168.1.254" .

Press "Apply" button to confirm the configuration setting

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

| LAN Setup | |
|----------------------|--|
| MAC Address | 00:1A:EF:19:06:B8 |
| IP Address | <input type="text" value="192.168.1.254"/> |
| Subnet Mask | <input type="text" value="255.255.255.0"/> |
| DHCP Type | Server <input type="button" value="v"/> |
| Start IP Address | <input type="text" value="192.168.1.50"/> |
| End IP Address | <input type="text" value="192.168.1.150"/> |
| Lease Time | <input type="text" value="86400"/> |
| 802.1d Spanning Tree | Disable <input type="button" value="v"/> |
| LLTD | Disable <input type="button" value="v"/> |
| IGMP Proxy | Disable <input type="button" value="v"/> |
| UPNP | Disable <input type="button" value="v"/> |
| PPPoE Relay | Disable <input type="button" value="v"/> |
| DNS Proxy | Disable <input type="button" value="v"/> |

3. Configure the WLAN interface:

Open “Basic Wireless Settings” page, enter the SSID ” RalinkInitAP_1906B8”, Channel Number ”AutoSelect”.Press “Apply” button to confirm the configuration setting.

Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

| Wireless Network | |
|-------------------------------|--|
| Wireless On/Off | <input type="button" value="Wireless OFF"/> Current Status:Radio ON |
| Antenna Switch | <input type="radio"/> External <input checked="" type="radio"/> Internal |
| Wireless Mode | <input type="text" value="AP"/> |
| Wireless Band | <input type="text" value="802.11B/G/N"/> |
| SSID | <input type="text" value="RalinkInitAP_1906B8"/> |
| Broadcast Network Name (SSID) | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| AP Isolation | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| MBSSID AP Isolation | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| BSSID | <input type="text" value="00:1A:EF:19:06:B8"/> |
| Frequency (Channel) | <input type="text" value="AutoSelect"/> Current Channel: 11 |
| HT Physical Mode | |
| Operating Mode | <input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Guard Interval | <input type="radio"/> Long <input checked="" type="radio"/> Auto |
| MCS | <input type="text" value="Auto"/> |

4.4.3 Example three –set WLAN to be WAN as WiFi Client

User Mr. ABC likes to configure this WLAN Broadband Router to be a WiFi client. In order to communicate with another AP. Mr. ABC collects information and plans the WLAN Broadband Router implementation by the following configuration.

WAN configuration: DHCP (Auto config)

| | |
|---------------------|-----|
| IP Address | n/a |
| Subnet Mask | n/a |
| Default Gateway | n/a |
| Primary DNS Address | n/a |

LAN configuration:

| | |
|-------------------|------------------------------|
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| DHCP Client Range | 192.168.1.100 –192.168.1.200 |

WLAN configuration:

| | |
|----------------|---------------------|
| SSID | RalinkInitAP_1906B8 |
| Channel Number | 1 |

WISP configuration:

| | |
|---------------------|------------------------------|
| SSID | TEST AP |
| Channel Number | Channel 1 |
| Wireless Encryption | n/a |
| DHCP server | 192.168.88.50~192.168.88.150 |

1. Configure the Operation Mode:

Open “Operation Mode Configuration” page, select **Ethernet Converter**, then click “**Apply**” button to confirm the configuration setting and reboot the WLAN Broadband Router. After reboot, the wireless LAN will become to WAN interface.

Operation Mode Configuration

You may configure the operation mode suitable for you environment.

☐ Bridge:

All ethernet and wireless interfaces are bridged into a single bridge interface.

☐ Gateway:

The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

☒ Wireless ISP:

The wireless apcli interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LAN ports.

:

Apply

Cancel

2. Site Survey:

Open “Site Survey” page under Wireless Settings, and select the AP “testap”.

Press “**Connect**” button to connect with the AP.

Site Survey

You could configure AP Client parameters here.

| | SSID | BSSID | RSSI | Channel | Authentication | Wireless Mode |
|-----------------------|--------|-------------------|------|---------|----------------|---------------|
| <input type="radio"/> | TestAP | 00:0c:42:66:45:6a | 76% | 165 | NONE | 11a |
| <input type="radio"/> | EL | 00:1a:ef:1e:81:84 | 5% | 149 | NONE | 11a/n |

Scan AP

Next



3. Wireless encryption setting:

If the AP has encryption setting, it will pop out a window for you filling the encryption setting.

Please fill up the encryption code and click “***Apply***” button to connect with the AP.

Site Survey

You could configure AP Client parameters here.

| | SSID | BSSID | RSSI | Channel | Authentication | Wireless Mode |
|-----------------------|--------|-------------------|------|---------|----------------|---------------|
| <input type="radio"/> | TestAP | 00:0c:42:66:45:6a | 76% | 165 | NONE | 11a |
| <input type="radio"/> | EL | 00:1a:ef:1e:81:84 | 5% | 149 | NONE | 11a/n |

Scan AP

Next

4. Station Link Status:

After connection with AP, you can open “Link Status” page under Wireless Settings to check Link Status.

Access Point Status

This page show the current status and some basic settings of the device.

| System Information | |
|----------------------|--------------------|
| Firmware Version | 1.0.18-N_H |
| System Up Time | 7 mins, 19 secs |
| Operation Mode | AP Client Mode |
| Wireless Information | |
| Status | Radio ON |
| Mode | AP |
| SSID | RalinknitAP_1906B8 |
| Channel | 1 |
| Encryption | OPEN |
| BSSID | 00:1A:EF:19:06:B8 |
| WAN Information | |
| Connected Type | DHCP |
| WAN IP Address | 192.168.88.187 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.88.1 |
| DNS1 | 168.95.1.1 |
| DNS2 | 168.95.1.1 |
| MAC Address | 00:1A:EF:19:06:B9 |
| LAN Information | |
| DHCP Server | Enabled |
| LAN IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| MAC Address | 00:1A:EF:19:06:B8 |

5. FREQUENTLY ASKED QUESTIONS (FAQ)

Enter topic text here.

5.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- ✓ Open the Command program in the Microsoft Windows.
- ✓ Type in "ipconfig /all", then press the Enter button.
- ✓ Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

5.2 What is Wireless LAN?

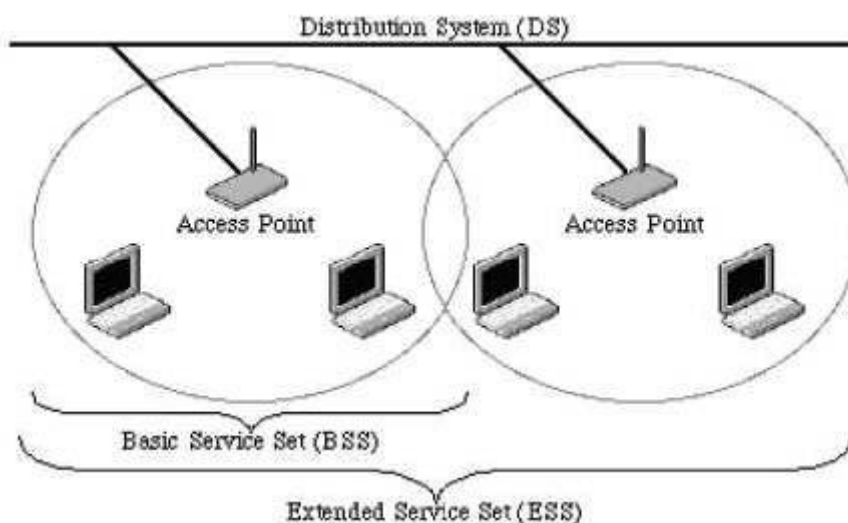
A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

5.3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/-13 MHz, 2450 +/-50 MHz and 5800 +/-75 MHz.

5.4 How does wireless networking work?

The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single sub-network. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Example 2: wireless Ad Hoc Mode

5.5 What is BSSID?

A six-byte address is that distinguish a particular access point from others. Also know as just SSID. Serve as a network ID or name.

5.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

5.7 What are potential factors that may causes interference?

Factors of interference:

- ✎ Obstacles: walls, ceilings, furniture... etc.
- ✎ Building Materials: metal door, aluminum studs.
- ✎ Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- ✓ Minimizing the number of walls and ceilings.
- ✓ Position the WLAN antenna for best reception.
- ✓ Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors...etc.
- ✓ Add additional WLAN Access Points if necessary.

5.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

5.9 What is WEP?

An option of IEEE 802.11 function is that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

5.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

5.11 What is RTS (Request to Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

5.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 include management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

5.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

5.14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's



not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

5.15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the Wi-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

5.16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

5.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (EAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

5.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

5.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

5.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

5.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

5.22 What is Universal Plug and Play (uPnP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The



ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

5.23 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU.

5.24 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address. Since that all the clients will communicate outside world through the WLAN Broadband Router, so have the cloned MAC address set on the WLAN Broadband Router will solve the issue.

5.25 What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user owned the DNS server with dynamic WAN IP address.

5.26 What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

5.27 What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to point private link via shared or public network.

5.28 What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

5.29 What is WLAN Block Relay between Clients?

An Infrastructure Basic Service Set is a BSS with a component called an Access Point (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS.

5.30 What is WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

5.31 What is WLAN ACK TIMEOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

5.32 What is Modulation Coding Scheme (MCS)?

MCS is Wireless link data rate for 802.11n. The throughput/range performance of an AP will depend on its implementation of coding schemes. MCS includes variables such as the number of spatial streams,

modulation, and the data rate on each stream. Radios establishing and maintaining a link must automatically negotiate the optimum MCS based on channel conditions and then continuously adjust the selection of MCS as conditions change due to interference, motion, fading, and other events.

5.33 What is Frame Aggregation?

Every 802.11 packet, no matter how small, has a fixed amount of overhead associated with it. Frame Aggregation combines multiple smaller packets together to form one larger packet. The larger packet can be sent without the overhead of the individual packets. This technique helps improve the efficiency of the 802.11n radio allowing more end user data to be sent in a given time.

5.34 What is Guard Intervals (GI)?

A GI is a period of time between symbol transmission that allows reflections (from multipath) from the previous data transmission to settle before transmitting a new symbol. The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive.