

# **AIR FORCE ONE 2**

## **User Manual**

## Before Start to Configure

The WLAN Broadband 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: <empty>

WEB login Password: <empty>

The device has three operation modes (Gateway/Bridge/WISP).  
The default IP addresses for the device are 192.168.1.254, so you need to make sure the IP address of your PC is in the same subnet as the device, such as 192.168.1.X.

**It will take about 55 seconds to complete the boot up sequence after power on.**

## Prepare your PC to configure the WLAN Broadband Router

### For OS of Microsoft Windows 95/ 98/ Me:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.  
**Note:** Windows Me users may not see the Network control panel. If so, select **View all Control Panel options** on the left side of the window
2. Move mouse and double-click the right button on *Network* icon. The *Network* window will appear.
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 and reboot your PC after completes the IP parameters setting.

### **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 completes 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.

This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.

## Broadband Router Status

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

System	
Uptime	0day:0h:23m:9s
Firmware Version	v1.4.2
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	MyWLAN
Channel Number	11
Encryption	Disabled
BSSID	00:02:72:14:81:86
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:02:72:14:81:86
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.0.146
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.10
DNS 1	168.95.1.1
DNS 2	192.168.0.5
DNS 3	0.0.0.0
MAC Address	00:02:72:14:81:87

Item	Description
System	
Uptime	It shows the duration since WLAN Broadband

	Router is powered on.
Firmware version	It shows the firmware version of WLAN Broadband Router.
<b>Wireless configuration</b>	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this WLAN Broadband Router. The SSID is the unique name of WLAN Broadband Router and shared among its service area, so all devices attempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of the WLAN Broadband Router. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
<b>TCP/IP configuration</b>	
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of WLAN Broadband Router.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of WLAN Broadband Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of WLAN Broadband Router.
<b>WAN configuration</b>	
Attain IP Protocol	It shows how the WLAN Broadband Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP connection.
IP Address	It shows the IP address of WAN interface of WLAN Broadband Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of WLAN Broadband Router.
Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
DNS1/DNS2/DNS3	It shows the DNS server information.
MAC Address	It shows the MAC address of WAN interface of WLAN Broadband Router.

## Setup Wizard

This page guides you to configure wireless broadband router for first time

### Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

Next>>

## Operation Mode

This page followed by Setup Wizard page to define the operation mode.

### 1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- ☒ **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
- ☐ **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- ☐ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Cancel

<<Back

Next>>

## Time Zone Setting

This page is used to enable and configure NTP client

### 2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

☐ Enable NTP client update

Time Zone Select : (GMT+08:00)Taipei

NTP server : 192.5.41.41 - North America

Cancel

<<Back

Next>>

## LAN Interface Setup

This page is used to configure local area network IP address and subnet mask

### 3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Cancel

<<Back

Next>>

## WAN Interface Setup

This page is used to configure WAN access type

### 4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

---

WAN Access Type: DHCP Client ▼

Cancel <<Back Next>>

## Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type, SSID, Channel Number, Enable Mac Clone(Single Ethernet Client)

### 5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

---

Band: 2.4 GHz (G) ▼

Mode: AP ▼

Network Type: Infrastructure ▼

SSID: MyWLAN

Channel Number: 11 ▼

☐ Enable Mac Clone (Single Ethernet Client)

Cancel <<Back Next>>




## Wireless Security Setup

This page is used to configure wireless security

### 6. Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: None 

Cancel

<<Back

Finished

## Operation Mode

This page is used to configure which mode wireless broadband router acts

### Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- ☒ **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
- ☐ **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- ☐ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

Apply Change

Reset

Item	Description
Gateway	Traditional gateway configuration. It always connects internet via ADSL/Cable Modem. LAN interface, WAN interface, Wireless interface, NAT and Firewall modules are applied to this mode
Bridge	Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all router's functions are not supported
Wireless ISP	Switch Wireless interface to WAN port and all Ethernet ports in bridge mode. Wireless interface can do all router's functions
Apply Changes	Click the <b><i>Apply Changes</i></b> button to complete the new configuration setting.
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.

## Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Broadband Router. Here you may change wireless encryption settings as well as wireless network parameters.

### Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ **Disable Wireless LAN Interface**

**Band:** 2.4 GHz (B+G) ▼

**Mode:** AP ▼

**Network Type:** Infrastructure ▼

**SSID:** MyWLAN

**Channel Number:** 11 ▼

**Associated Clients:** Show Active Clients

☐ **Enable Mac Clone (Single Ethernet Client)**

☐ **Enable Universal Repeater Mode (Acting as AP and client simultaneously)**

**SSID of Extended Interface:**

Apply Changes

Reset

Item	Description
Disable Wireless LAN Interface	Click on to disable the wireless LAN data transmission.
Band	Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(B+G)
Mode	Click to select the WLAN AP / Client / WDS / AP+WDS wireless mode.
Site Survey	The <b>Site Survey</b> button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled. Refer to <a href="#">3.3.9 Site Survey</a> .
SSID	It is the wireless network name. The SSID can be 32 bytes long.
Channel Number	Select the wireless communication channel from pull-down menu.
Associated Clients	Click the <b>Show Active Clients</b> button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.
Enable Mac Clone (Single Ethernet Client)	Take Laptop NIC MAC address as wireless client MAC address. <b>[Client Mode only]</b>
Enable Universal Repeater Mode	Click to enable Universal Repeater Mode
SSID of Extended Interface	Assign SSID when enables Universal Repeater Mode.
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Wireless - Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your WLAN Broadband Router.

## Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/> (256-2346)
RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Beacon Interval:	<input type="text" value="100"/> (20-1024 ms)
Data Rate:	<input type="button" value="Auto"/> ▾
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IAPP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
802.11g Protection:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
RF Output Power:	<input checked="" type="radio"/> 100% <input type="radio"/> 50% <input type="radio"/> 25% <input type="radio"/> 10% <input type="radio"/> 5%
Turbo Mode:	<input type="radio"/> Auto <input type="radio"/> Always <input checked="" type="radio"/> Off
Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.	
Block Relay Between Clients:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
WMM:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
ACK Timeout:	<input type="text" value="0"/> (0-255) < Current: 11b: 316us / 11g: 72us >
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

Item	Description
Authentication Type	Click to select the authentication type in <b>Open System</b> , <b>Shared Key</b> or <b>Auto</b> selection.
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes.
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes.
Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 11M, 5.5M, 2M or 1Mbps.
Preamble Type	Click to select the <b>Long Preamble</b> or <b>Short Preamble</b> support on the wireless data packet transmission.
Broadcast SSID	Click to enable or disable the SSID broadcast function.
IAPP	Click to enable or disable the IAPP function.

802.11g Protection	Protect 802.11b user.
RF Output Power	To adjust transmission power level.
Turbo Mode	Click to Enable/Disable turbo mode. <i>(Only apply to WLAN IC of Realtek).</i>
Block Relay Between Clients	Click Enabled/Disabled to decide if blocking relay packets between clients.
WMM	Click Enabled/Disabled to init WMM feature.
ACK Timeout	Set ACK timeout value. It shows current time in the end.
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Wireless - Security Setup

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

### Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption:	<input type="text" value="None"/>	<input type="button" value="Set WEP Key"/>
<input type="checkbox"/> Use 802.1x Authentication	<input checked="" type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits	
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)	
Pre-Shared Key Format:	<input type="text" value="Passphrase"/>	
Pre-Shared Key:	<input type="text"/>	
<input type="checkbox"/> Enable Pre-Authentication		
Authentication RADIUS Server:	Port <input type="text" value="1812"/>	IP address <input type="text"/> Password <input type="text"/>

*Note: When encryption WEP is selected, you must set WEP key value.*

Item	Description
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA(TKIP), WPA2 or WPA2 Mixed
Use 802.1x Authentication	While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function.
WPA Authentication Mode	While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key).
Pre-Shared Key Format	While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). <b>[WPA, Personal(Pre-Shared Key) only]</b>
Pre-Shared Key	Fill in the key value. [WPA, Personal(Pre-Shared Key) only]
Enable Pre-Authentication	Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only]
RADIUS Server Authentication	Set the IP address, port and login password information of authentication RADIUS sever.
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## WEP Key Setup

### Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

---

Key Length:

64-bit ▼

Key Format:

Hex (10 characters) ▼

Default Tx Key:

Key 1 ▼

Encryption Key 1:

\*\*\*\*\*

Encryption Key 2:

\*\*\*\*\*

Encryption Key 3:

\*\*\*\*\*

Encryption Key 4:

\*\*\*\*\*

Apply Changes

Close

Reset

Item	Description
Key Length	Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.
Default Tx Key	Set the default secret key for WEP security function. Value can be chose between 1 and 4.
Encryption Key 1	Secret key 1 of WEP security encryption function.
Encryption Key 2	Secret key 2 of WEP security encryption function.
Encryption Key 3	Secret key 3 of WEP security encryption function.
Encryption Key 4	Secret key 4 of WEP security encryption function.
Apply Changes	Click the <b><i>Apply Changes</i></b> button to complete the new configuration setting.
Close	Click to close this WEP Key setup window.
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.

WEP encryption key (secret key) length:			
Format \ Length	Length		
	64-bit	128-bit	
ASCII	5 characters	13 characters	
HEX	10 hexadecimal codes	26 hexadecimal codes	

## Wireless - Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

## Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Allow Listed ▼

MAC Address:  Comment:

Current Access Control List:

MAC Address	Comment	Select
00:02:72:81:86:01	ST-1	<input type="checkbox"/>
00:00:55:66:66:50	ST-2	<input type="checkbox"/>

Item	Description
Wireless Access Control Mode	Click the <i>Disabled</i> , <i>Allow Listed</i> or <i>Deny Listed</i> 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.
MAC Address	Fill in the MAC address of client to register this WLAN Broadband Router access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the <i>Apply Changes</i> button to register the client to new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.
Current Access Control List	It shows the registered clients that are allowed to link to this WLAN Broadband Router.
Delete Selected	Click to delete the selected clients that will be access right removed from this WLAN Broadband Router.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.



## WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.

### WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

---

☒ **Enable WDS**

Add WDS AP:    MAC Address     Comment

Apply Changes

Reset

Set Security

Show Statistics

**Current WDS AP List:**

MAC Address	Comment	Select
00:02:72:81:86:0a	AP-1	<input type="checkbox"/>
00:02:72:81:86:0b	AP-2	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Item	Description
Enable WDS	Click the check box to enable wireless distribution system.
MAC Address	Fill in the MAC address of AP to register the wireless distribution system access capability.
Comment	Fill in the comment tag for the registered AP.
Apply Changes	Click the <b>Apply Changes</b> button to register the AP to new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.
Set Security	Click button to configure wireless security like <b>WEP(64bits)</b> , <b>WEP(128bits)</b> , <b>WPA(TKIP)</b> , <b>WPA2(AES)</b> or <b>None</b>
Show Statistics	It shows the TX, RX packets, rate statistics
Delete Selected	Click to delete the selected clients that will be removed from the wireless distribution system.
Delete All	Click to delete all the registered APs from the wireless distribution system allowed list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## WDS Security Setup

Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS

This page is used to configure the wireless security between APs.

### WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

**Encryption:**

**WEP Key Format:**

**WEP Key:**

**Pre-Shared Key Format:**

**Pre-Shared Key:**

## WDS AP Table

This page is used to show WDS statistics

### WDS AP Table

This table shows the MAC address, transmission, reception packet counters and state information for each configured WDS AP.

MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
00:02:72:81:86:0a	22	0	0	1
00:02:72:81:86:0b	22	14	0	1

Item	Description
MAC Address	It shows the MAC Address within WDS.
Tx Packets	It shows the statistic count of sent packets on the wireless LAN interface.
Tx Errors	It shows the statistic count of error sent packets on the Wireless LAN interface.
Rx Packets	It shows the statistic count of received packets on the wireless LAN interface.
Tx Rate (Mbps)	It shows the wireless link rate within WDS.
Refresh	Click to refresh the statistic counters on the screen.
Close	Click to close the current window.

## Site Survey

This page is used to view or configure other APs near yours.

### Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
MyWLAN	00:02:72:00:81:86	11 (B+G)	AP	no	90	<input type="radio"/>
linux-wlan	00:02:72:f1:02:ad	6 (B)	AP	no	76	<input type="radio"/>
RTL8186-VPN-GW	00:e0:4c:81:86:23	11 (B+G)	AP	no	66	<input type="radio"/>
Sales	00:02:72:04:68:92	11 (B)	AP	yes	53	<input type="radio"/>
Tekom_Office	00:02:72:00:93:fb	9 (B)	AP	yes	35	<input type="radio"/>
alex	d6:4c:fc:0d:2a:d4	1 (B)	Ad hoc	no	32	<input type="radio"/>
MyWLAN	00:02:72:85:15:99	11 (B+G)	AP	no	32	<input type="radio"/>

Refresh

Connect

Item	Description
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Type	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.
Select	Click to select AP or client you'd like to connect.

Refresh	Click the <b>Refresh</b> button to re-scan site survey on the screen.
Connect	Click the <b>Connect</b> button to establish connection.

## LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN Broadband Router. Here you may change the setting for IP address, subnet mask, DHCP, etc.

### LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

---

IP Address:

Subnet Mask:

Default Gateway:

DHCP:

Server ▼

DHCP Client Range:

–

DNS Server:

Domain Name:

802.1d Spanning Tree:

Disabled ▼

Clone MAC Address:

Item	Description
IP Address	Fill in the IP address of LAN interfaces of this WLAN Access Point.
Subnet Mask	Fill in the subnet mask of LAN interfaces of this WLAN Access Point.
Default Gateway	Fill in the default gateway for LAN interfaces out going data packets.
DHCP	Click to select <b>Disabled</b> , <b>Client</b> or <b>Server</b> in different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
Show Client	Click to open the <b>Active DHCP Client Table</b> window that shows the active clients with their

	assigned IP address, MAC address and time expired information. <b>[Server mode only]</b>
DNS Server	Manual setup DNS server IP address.
Domain Name	Assign Domain Name and dispatch to DHCP clients. It is optional field.
802.1d Spanning Tree	Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Apply Changes	Click the <b><i>Apply Changes</i></b> button to complete the new configuration setting.
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.

## WAN Interface Setup

This page is used to configure the parameters for wide area network that connects to the WAN port of your WLAN Broadband Router. Here you may change the access method to *Static IP*, *DHCP*, *PPPoE* or *PPTP* by click the item value of **WAN Access Type**.

### Static IP

## WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

**WAN Access Type:** Static IP

**IP Address:**

**Subnet Mask:**

**Default Gateway:**

**MTU Size:**  (1400-1500 bytes)

**DNS 1:**

**DNS 2:**

**DNS 3:**

**Clone MAC Address:**

☐ Enable uPNP

☐ Enable Ping Access on WAN

☐ Enable Web Server Access on WAN

☒ Enable IPsec pass through on VPN connection

☒ Enable PPTP pass through on VPN connection

☒ Enable L2TP pass through on VPN connection

☐ Set TTL Value  (1-128)

Item	Description
Static IP	Click to select Static IP support on WAN interface. There are IP address, subnet mask and default gateway settings need to be done.
IP Address	If you select the Static IP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the Static IP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the Static IP support on WAN interface, fill in the default gateway for WAN interface out going data packets.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable WAN Echo Reply	Click the checkbox to enable WAN ICMP response.
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPsec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## DHCP Client

### WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

**WAN Access Type:** DHCP Client

**Host Name:**

**MTU Size:**  (1400-1492 bytes)

☒ **Attain DNS Automatically**

☐ **Set DNS Manually**

**DNS 1:**

**DNS 2:**

**DNS 3:**

**Clone MAC Address:**

☐ **Enable uPNP**

☐ **Enable Ping Access on WAN**

☐ **Enable Web Server Access on WAN**

☒ **Enable IPsec pass through on VPN connection**

☒ **Enable PPTP pass through on VPN connection**

☒ **Enable L2TP pass through on VPN connection**

☐ **Set TTL Value**  (1-128)

Item	Description
DHCP Client	Click to select DHCP support on WAN interface for IP address assigned automatically from a DHCP server.
Host Name	Fill in the host name of Host Name. The default value is empty
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400
Attain DNS Automatically	Click to select getting DNS address for <b>DHCP</b> support. Please select <b>Set DNS Manually</b> if the <b>DHCP</b> support is selected.
Set DNS Manually	Click to select getting DNS address for <b>DHCP</b> support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.

	Refer to <a href="#">4.22 What is Universal Plug and Play (uPNP)?</a>
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable WAN Echo Reply	Click the checkbox to enable WAN ICMP response.
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the <b><i>Apply Changes</i></b> button to complete the new configuration setting.
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.

## PPPoE

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

---

**WAN Access Type:** PPPoE ▾

**User Name:**

**Password:**

**Service Name:**

**Connection Type:** Continuous ▾ Connect Disconnect

**Idle Time:** 5 (1-1000 minutes)

**MTU Size:** 1400 (1360-1492 bytes)

☐ **Attain DNS Automatically**

☒ **Set DNS Manually**

**DNS 1:** 168.95.1.1

**DNS 2:** 192.168.0.5

**DNS 3:** 0.0.0.0

**Clone MAC Address:** 000000000000

☐ **Enable uPNP**

☐ **Enable Ping Access on WAN**

☐ **Enable Web Server Access on WAN**

☒ **Enable IPsec pass through on VPN connection**

☒ **Enable PPTP pass through on VPN connection**

☒ **Enable L2TP pass through on VPN connection**

☐ **Set TTL Value** 64 (1-128)

Apply Changes Reset



Item	Description
PPPoE	Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.
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.
Service Name	Fill in the service name of Service Name. The default value is empty.
Connection Type	Select the connection type from pull-down menu. There are <b>Continuous</b> , <b>Connect on Demand</b> and <b>Manual</b> three types to select. <b>Continuous</b> connection type means to setup the connection through PPPoE protocol whenever this WLAN Broadband Router is powered on. <b>Connect on Demand</b> connection type means to setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set. <b>Manual</b> connection type means to setup the connection through the PPPoE protocol by clicking the <b>Connect</b> button manually, and clicking the <b>Disconnect</b> button manually.
Idle Time	If you select the <b>PPPoE</b> and <b>Connect on Demand</b> connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400.
Attain DNS Automatically	Click to select getting DNS address for <b>PPPoE</b> support. Please select <b>Set DNS Manually</b> if the <b>PPPoE</b> support is selected.
Set DNS Manually	Click to select getting DNS address for <b>Static IP</b> support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.

Enable uPNP	Click the checkbox to enable uPNP function.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable WAN Echo Reply	Click the checkbox to enable WAN ICMP response.
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the <b><i>Apply Changes</i></b> button to complete the new configuration setting.
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.

## PPTP

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

**WAN Access Type:** PPTP

**IP Address:** 172.1.1.2

**Subnet Mask:** 255.255.255.0

**Server IP Address:** 172.1.1.1

**User Name:**

**Password:**

**MTU Size:** 1400 (1400-1460 bytes)

☐ Request MPPE Encryption

☐ Attain DNS Automatically

☒ Set DNS Manually

**DNS 1:** 168.95.1.1

**DNS 2:** 192.168.0.5

**DNS 3:** 0.0.0.0

**Clone MAC Address:** 000000000000

☐ Enable uPNP

☐ Enable Ping Access on WAN

☐ Enable Web Server Access on WAN

☒ Enable IPsec pass through on VPN connection

☒ Enable PPTP pass through on VPN connection

☒ Enable L2TP pass through on VPN connection

☐ Set TTL Value 64 (1-128)

Apply Changes

Reset

Item	Description
PPTP	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.
IP Address	If you select the PPTP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the PPTP support on WAN interface, fill in the subnet mask for it.
Server IP Address	Enter the IP address of the PPTP Server.
User Name	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Password	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400.
Request MPPE Encryption	Click the checkbox to enable request MPPE encryption.
Attain DNS Automatically	Click to select getting DNS address for <b>PPTP</b> support. Please select <b>Set DNS Manually</b> if the <b>PPTP</b> support is selected.
Set DNS Manually	Click to select getting DNS address for <b>PPTP</b> support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned.
Enable uPNP	Click the checkbox to enable uPNP function.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable WAN Echo Reply	Click the checkbox to enable WAN ICMP response.
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Firewall - Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

### Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

---

☒ **Enable Port Filtering**

Port Range:  -  Protocol: Both  Comment:

**Current Filter Table:**

Port Range	Protocol	Comment	Select
20-21	TCP+UDP	FTP	<input type="checkbox"/>

Item	Description
Enable Port Filtering	Click to enable the port filtering security function.
Port Range	To restrict data transmission from the local network on certain ports, fill in the range of start-port and end-port, and the protocol, also put your comments on it.
Protocol	The <b>Protocol</b> can be TCP, UDP or Both.
Comments	<b>Comments</b> let you know about whys to restrict data from the ports.
Apply Changes	Click the <b>Apply Changes</b> button to register the ports to port filtering list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Firewall - IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

### IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

---

☒ **Enable IP Filtering**

Local IP Address:  Protocol:  Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
192.168.1.201	TCP-UDP	ST-1	<input type="checkbox"/>
192.168.1.202	TCP	ST-2	<input type="checkbox"/>

Item	Description
Enable IP Filtering	Click to enable the IP filtering security function.
Local IP Address	To restrict data transmission from local network on certain IP addresses, fill in the IP address and the protocol, also put your comments on it. The <b>Protocol</b> can be TCP, UDP or Both. <b>Comments</b> let you know about whys to restrict data from the IP address.
Protocol	
Comments	
Apply Changes	Click the <b>Apply Changes</b> button to register the IP address to IP filtering list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address that will be removed from the IP-filtering list.
Delete All	Click to delete all the registered entries from the IP-filtering list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Firewall - MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

### MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☒ Enable MAC Filtering

MAC Address:  Comment:

Apply Changes

Reset

Current Filter Table:

MAC Address	Comment	Select
00:02:72:00:81:90	ST-1	<input type="checkbox"/>
00:02:72:00:81:91	ST-2	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address Comments	To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it. <b>Comments</b> let you know about whys to restrict data from the MAC address.
Apply Changes	Click the <b>Apply Changes</b> button to register the MAC address to MAC filtering list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected MAC address that will be removed from the MAC-filtering list.
Delete All	Click to delete all the registered entries from the MAC-filtering list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Firewall - Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

### Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☒ Enable Port Forwarding

IP Address:  Protocol:  Port Range:  -  Comment:

Apply Changes

Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.1.201	TCP+UDP	20-21	FTP	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Item	Description
Enable Port Forwarding	Click to enable the Port Forwarding security 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,
Protocol	protocol, port range and your comments. The <b>Protocol</b> can be TCP, UDP or Both.
Port Range	The <b>Port Range</b> for data transmission.
Comment	<b>Comments</b> let you know about whys to allow data packets forward to the IP address and port number.
Apply Changes	Click the <b>Apply Changes</b> button to register the IP address and port number to Port forwarding list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

Delete Selected	Click to delete the selected IP address and port number that will be removed from the port-forwarding list.
Delete All	Click to delete all the registered entries from the port-forwarding list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Firewall – URL Filtering

URL Filtering is used to restrict users to access specific websites in internet.

### URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

---

☒ **Enable URL Filtering**

**URL Address:**

**Current Filter Table:**

URL Address	Select
www.url-filter-list.com	<input type="checkbox"/>

Item	Description
Enable URL Filtering	Click to enable the URL Filtering function.
URL Address	Add one URL address.
Apply Changes	Click the <b>Apply Changes</b> button to save settings.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected URL address that will be removed from the URL Filtering list.
Delete All	Click to delete all the registered entries from the URL Filtering list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.



## Firewall - DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

### DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

---

☒ Enable DMZ

DMZ Host IP Address:

Item	Description
Enable DMZ	Click to enable the DMZ function.
DMZ Host 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.
Apply Changes	Click the <b>Apply Changes</b> button to register the IP address of DMZ host.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## VPN Setting

This page is used to show VPN connection table, configure IPSEC VPN, NAT Traversal, Generate RSA Key, Show RSA Public Key.

## VPN Setup

This page is used to enable/disable VPN function and select a VPN connection to edit/delete.

☒ **Enable IPSEC VPN**

☒ **Enable NAT Traversal**

Generate RSA Key

Apply Changes

Show RSA Public Key

Current VPN Connection Table: WAN IP:192.168.3.254

	#	Name	Active	Local Address	Remote Address	Remote Gateway	Status
	1	site5	Y	192.168.1.0/24	192.168.4.0/24	192.168.3.1	Connected
	2	-	-	-	-	-	-
	3	-	-	-	-	-	-
	4	-	-	-	-	-	-
	5	-	-	-	-	-	-
	6	-	-	-	-	-	-
	7	-	-	-	-	-	-
	8	-	-	-	-	-	-
	9	-	-	-	-	-	-
	10	-	-	-	-	-	-

Edit

Delete

Refresh

Item	Description
Enable IPSEC VPN	Click to enable IPSEC VPN function.
Enable NAT Traversal	Click to enable NAT Traversal function.
Generate RSA Key	Click to generate RSA key.
Show RSA Public Key	Click to show RSA public key that we generate.
Apply Changes	Click the <b>Apply Changes</b> button to enable IPSEC VPN, NAT Traversal settings.
Current VPN Connection Table	It shows current WAN interface information and VPN connection table.
Edit	Click to enter the current VPN tunnel configuration page.
Delete	Click to delete the current VPN tunnel that radio button stay.
Refresh	Click to refresh the current VPN connection table.

## VPN Setup - Edit Tunnel

### VPN Setup

---

☒ **Enable Tunnel 1**

**Connection Name:**

**Auth Type:**

**Local Site:**

Local IP Address/Network

Local Subnet Mask

**Remote Site:**

Remote Secure Gateway

Remote IP Address/Network

Remote Subnet Mask

**Local/Peer ID:**

Local ID Type

Local ID

Remote ID Type

Remote ID

Item	Description
Enable Tunnel #	Click to enable the IPSEC VPN current tunnel.
Connection Name	Assign the connection name tag.
Auth Type	Click to select <b>PSK</b> or <b>RSA</b> .
Local Site	Click to select <b>Single Address</b> or <b>Subnet Address</b> VPN connection.
<b>Local IP Address/Network</b>	Fill in IP address or subnet address depends on which Local Site option you choose.
<b>Local Subnet Mask</b>	Fill in the local subnet mask.
Remote Site	Click to select <b>Single Address</b> , <b>Subnet Address</b> , <b>Any Address</b> or <b>NAT-T Any Address</b> VPN remote connection.
<b>Remote Secure Gateway</b>	Fill in remote gateway IP address
<b>Remote IP Address/Network</b>	Fill in IP address or subnet address depends on which Remote Site option you choose.
<b>Remote Subnet Mask</b>	Fill in remote subnet mask
Local/Peer ID	Define IKE exchange information type
<b>Local ID Type</b>	Click to select <b>IP</b> , <b>DNS</b> or <b>E-mail</b> as local exchange type
<b>Local ID</b>	Fill in local ID except IP selected
<b>Remote ID Type</b>	Click to select <b>IP</b> , <b>DNS</b> or <b>E-mail</b> as remote exchange type
<b>Remote ID</b>	Fill in remote ID except IP selected

**Key Management:** ☒ IKE ☐ Manual [Advanced](#)

Connection Type: [Responder](#) [Connect](#) [Disconnect](#)

ESP: [3DES](#) (Encryption Algorithm)  
[MD5](#) (Authentication Algorithm)

PreShared Key:

Remote RSA Key:

Status: Connected

[Apply Changes](#) [Reset](#) [Refresh](#) [Back](#)

Item	Description
Key Management	Click to select <i><b>IKE</b></i> or <i><b>Manual</b></i> mode.
Advanced	Click <i><b>Advanced</b></i> button to configure more IKE settings.
Connection Type	Click to select <i><b>Initiator</b></i> or <i><b>Responder</b></i> mode.
Connect	Click to connect manually. [ <b>Responder mode only</b> ]
Disconnect	Click to disconnect manually. [ <b>Responder mode only</b> ].
ESP	Click to configure <i><b>3DES</b></i> , <i><b>AES128</b></i> or <i><b>NULL</b></i> encryption. Click to configure <i><b>MD5</b></i> or <i><b>SHA1</b></i> authentication.
PreShared Key	Fill in the key value. [ <b>IKE mode only</b> ]
Remote RSA Key	Fill in the remote gateway RSA key. [ <b>IKE mode only</b> ]
Status	It shows connection status. [ <b>IKE mode only</b> ]
SPI	Fill in Security Parameter Index value. [ <b>Manual mode only</b> ]
Encryption Key	Fill in encryption key. [ <b>Manual mode only</b> ]
Authentication Key	Fill in authentication key. [ <b>Manual mode only</b> ]
Apply Change	Click the <i><b>Apply Changes</b></i> button to save current tunnel settings.
Reset	Click the <i><b>Reset</b></i> button to abort change and recover the previous configuration setting.
Refresh	It shows the current connection status. [ <b>Manual mode only</b> ]
Back	It returns back to VPN Setup page.

## Advanced IKE Setup

### Advanced VPN Setting for IKE

This page is used to provide advanced setting for IKE mode

#### Tunnel 1

##### Phase 1:

Negotiation Mode	Main mode
Encryption Algorithm	3DES
Authenticaiton Algorithm	MD5
Key Group	DH2(modp1024)
Key Life Time	3600

##### Phase 2:

Active Protocol	ESP
Encryption Algorithm	3DES
Authenticaiton Algorithm	MD5
Key Life Time	28800
Encapsulation	Tunnel mode
Perfect Forward Secrecy (PFS)	ON

Ok Cancel

Item	Description
<b>Phase 1</b>	
Negotiation Mode	Main mode.
Encryption Algorithm	Click to select <b>3DES</b> or <b>AES128</b> encryption.
Authentication Algorithm	Click to select <b>MD5</b> or <b>SHA1</b> authentication.
Key Group	Click to select <b>DH1(modp768)</b> , <b>DH2(modp1024)</b> or <b>DH5(modp1536)</b> key group. Default value is DH2
Key Life Time	Fill in the key life time value by seconds.
<b>Phase 2</b>	
Active Protocol	ESP.
Encryption Algorithm	Click to select <b>3DES</b> , <b>AES128</b> or <b>NULL</b> encryption.
Authentication	Click to select <b>MD5</b> or <b>SHA1</b> authentication.

### Algorithm

Key Life Time	Fill in the key life time value by seconds.
Encapsulation	Tunnel mode.
Perfect Forward Secrecy (PFS)	Click to select <i>ON</i> or <i>NONE</i> .
Ok	Click the <i>Ok</i> button to save current tunnel settings.
Cancel	Click the <i>Cancel</i> button to close current window without any changes.

### Management - Statistics

This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.

## Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	<i>Sent Packets</i>	1361
	<i>Received Packets</i>	25883
Ethernet LAN	<i>Sent Packets</i>	1529
	<i>Received Packets</i>	1269
Ethernet WAN	<i>Sent Packets</i>	597
	<i>Received Packets</i>	30386

Refresh

Item	Description
Wireless LAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN <i>Received Packets</i>	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the Ethernet LAN interface.
Ethernet LAN <i>Received Packets</i>	It shows the statistic count of received packets on the Ethernet LAN interface.
Ethernet WAN <i>Sent Packets</i>	It shows the statistic count of sent packets on the Ethernet WAN interface.
Ethernet WAN <i>Received Packets</i>	It shows the statistic count of received packets on the Ethernet WAN interface.
Refresh	Click the refresh the statistic counters on the screen.

## Management - DDNS

This page is used to configure Dynamic DNS service to have DNS with dynamic IP address.

### Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

---

☐ Enable DDNS

Service Provider :

DynDNS ▼

Domain Name :

host.dyndns.org

User Name/Email:

Password/Key:

*Note:*

*For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)*

*For DynDNS, you can create your DynDNS account [here](#)*

Apply Change

Reset

Item	Description
Enable DDNS	Click the checkbox to enable <b>DDNS</b> service.
Service Provider	Click the drop down menu to pickup the right provider.
Domain Name	To configure the Domain Name.
User Name/Email	Configure User Name, Email.
Password/Key	Configure Password, Key.
Apply Change	Click the <b>Apply Changes</b> button to save the enable DDNS service.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Management - Time Zone Setting

This page is used to configure NTP client to get current time.

### Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

---

Current Time : Yr  Mon  Day  Hr  Mn  Sec

Time Zone Select :

☒ Enable NTP client update

NTP server : ☒    
☐  (Manual IP Setting)

Item	Description
Current Time	It shows the current time.
Time Zone Select	Click the time zone in your country.
Enable NTP client update	Click the checkbox to enable NTP client update. R
NTP Server	Click select default or input NTP server IP address.
Apply Change	Click the <b>Apply Changes</b> button to save and enable NTP client service.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.
Refresh	Click the refresh the current time shown on the screen.

## Management – Denial-of-Service

This page is used to enable and setup protection to prevent attack by hacker's program. It provides more security for users.



## Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☐ **Enable DoS Prevention**

<input type="checkbox"/> <b>Whole System Flood: SYN</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>Whole System Flood: FIN</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>Whole System Flood: UDP</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>Whole System Flood: ICMP</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>Per-Source IP Flood: SYN</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>Per-Source IP Flood: FIN</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>Per-Source IP Flood: UDP</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>Per-Source IP Flood: ICMP</b>	<input type="text" value="0"/> <b>Packets/Second</b>
<input type="checkbox"/> <b>TCP/UDP PortScan</b>	<input type="text" value="Low"/> <b>Sensitivity</b>
<input type="checkbox"/> <b>ICMP Smurf</b>	
<input type="checkbox"/> <b>IP Land</b>	
<input type="checkbox"/> <b>IP Spoof</b>	
<input type="checkbox"/> <b>IP TearDrop</b>	
<input type="checkbox"/> <b>PingOfDeath</b>	
<input type="checkbox"/> <b>TCP Scan</b>	
<input type="checkbox"/> <b>TCP SynWithData</b>	
<input type="checkbox"/> <b>UDP Bomb</b>	
<input type="checkbox"/> <b>UDP EchoChargen</b>	

☐ **Enable Source IP Blocking**  **Block time (sec)**

Item	Description
Enable DoS Prevention	Click the checkbox to enable DoS prevention.
Whole System Flood / Per-Source IP Flood...	Enable and setup prevention in details.
Select ALL	Click the checkbox to enable all prevention items.
Clear ALL	Click the checkbox to disable all prevention items.
Apply Changes	Click the <i>Apply Changes</i> button to save above settings.

## Management - Log

This page is used to configure the remote log server and shown the current log.

### System Log

This page can be used to set remote log server and show the system log.

☒ **Enable Log**

☒ **system all**☐ **wireless**☐ **DoS**

☐ **Enable Remote Log**

Log Server IP Address:

Apply Changes

0day 00:02:18 br0: port 2(wlan0) entering disabled state  
0day 00:02:18 device wlan0 left promiscuous mode  
0day 00:02:18 br0: port 1(eth0) entering disabled state  
0day 00:02:18 device eth0 left promiscuous mode  
0day 00:02:18 device eth0 entered promiscuous mode  
0day 00:02:18 eth0:phy is 8305  
0day 00:02:18 device wlan0 entered promiscuous mode  
0day 00:02:18 br0: port 2(wlan0) entering listening state  
0day 00:02:18 br0: port 1(eth0) entering listening state  
0day 00:02:18 entering learning state  
0day 00:02:18 br0: port 2(wlan0) entering forwarding state  
0day 00:02:18 br0: topology change detected, propagating  
0day 00:02:18 br0: port 1(eth0) entering learning state  
0day 00:02:18 br0: port 1(eth0) entering forwarding state  
0day 00:02:18 br0: topology change detected, propagating

RefreshClear

Item	Description
Enable Log	Click the checkbox to enable log.
<i>System all</i>	Show all log of wireless broadband router
<i>Wirelessy</i>	Only show wireless log
<i>DoS</i>	Only show Denial-of-Service log
<i>Enable Remote Log</i>	Click the checkbox to enable remote log service.
<i>Log Server IP Address</i>	Input the remote log IP address
Apply Changes	Click the <i>Apply Changes</i> button to save above settings.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen

## Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

### Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

---

Select File:

Browse...

Upload

Reset

Item	Description
Select File	Click the <b><i>Browse</i></b> button to select the new version of web firmware image file.
Upload	Click the <b><i>Upload</i></b> button to update the selected web firmware image to the WLAN Broadband Router.
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.

## Management Save/ Reload Settings

This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.

### Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

---

Save Settings to File:

Save...

Load Settings from File:

Browse...

Upload

Reset Settings to Default:

Reset

Item	Description
Save Settings to File	Click the <b>Save</b> button to download the configuration parameters to your personal computer.
Load Settings from File	Click the <b>Browse</b> button to select the configuration files then click the <b>Upload</b> button to update the selected configuration to the WLAN Broadband Router.
Reset Settings to Default	Click the <b>Reset</b> button to reset the configuration parameter to factory defaults.

## Management - Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

### Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

---

User Name:

New Password:

Confirmed Password:

Item	Description
User Name	Fill in the user name for web management login control.
New Password	Fill in the password for web management login control.
Confirmed Password	Because the password input is invisible, so please fill in the password again for confirmation purpose.
Apply Changes	Clear the <b>User Name</b> and <b>Password</b> fields to empty, means to apply no web management login control. Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Management - WatchDog

This page is used to do watchdog function using ping command. User set IP address, interval and ping fail count conditions to decide whether router reboots or not.

### WatchDog Setting

Use ping command to identify whether the router is functional or not. User has to set IP address, interval and fail count to decide reboot router.

☐ Enable WatchDog

WatchDog IP Address:

Ping Interval:  (30-600 seconds)

Ping Fail to reboot Counter:  (3-30)

Item	Description
Enable WatchDog	Click to enable watchdog.
WatchDog IP Address	IP address that is referred.
Ping Interval	Fill in the value by seconds.
Ping Fail to reboot Count	Fill in the value that is the threshold to reboot router when ping fails.
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

## Management - Quality of Service

This page is used to do bandwidth control by ip address. User sets total and undefined bandwidth first. Then set bandwidth by range of ip addresses.

## Quality of Service

First, assign total downstream and upstream that you applied from ISP. Second, set up the specific ip address' guarantee downstream, upstream and priority and display current settings in the table.

☐ Enable QoS

ISP Bandwidth: Download  KB/s Upload  KB/s

Undef IP Bandwidth: Download  KB/s Upload  KB/s

Apply Changes

Reset

### Bandwidth Control

IP Address Range:  -

Guarantee Bandwidth: Download  KB/s Upload  KB/s

Priority:

Apply Changes

Reset

### Current Bandwidth Control Table:

From IP Addr	To IP Addr	Downstream (KB/s)	Upstream (KB/s)	Priority	Select
<div>Delete Selected</div> <div>Delete All</div> <div>Reset</div>					

Item	Description
Enable QoS	Click to enable QoS.
ISP Bandwidth	
Download	Fill in the value that is the download stream from ISP by KB/s.
Upload	Fill in the value that is the upload stream from ISP by KB/s.
Undef IP Bandwidth	
Download	Define the download bandwidth that is not defined.
Upload	Define the upload bandwidth that is not defined.
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

Item	Description
------	-------------

### Bandwidth Control

IP Address Range	Set start and end ip address.
Guarantee Bandwidth	
Download	Fill in the value by KB/s.
Upload	Fill in the value by KB/s.
Piority	Click to pick <b>High, Medium</b> or <b>Low</b>
Apply Changes	Click the <b><i>Apply Changes</i></b> button to complete the new configuration setting. It is added into <b>Current Bandwidth Control Table.</b>
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected ip addresses that will be removed from the <b>Current Bandwidth Control Table.</b>
Delete All	Click to delete all the registered entries from the ip addresses <b>Current Bandwidth Control Table.</b>
Reset	Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.

### Logout

This page is used to logout web management page. This item will be activated next time you login after you define user account and password.

### Logout

This page is used to logout.

---

**Do you want to logout ?**

**Change setting successfully!**

Item	Description
Apply Change	Click the <b><i>Apply Change</i></b> button, Then click <b><i>OK</i></b> button to logout.

## Frequently Asked Questions (FAQ)

### 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.

### 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

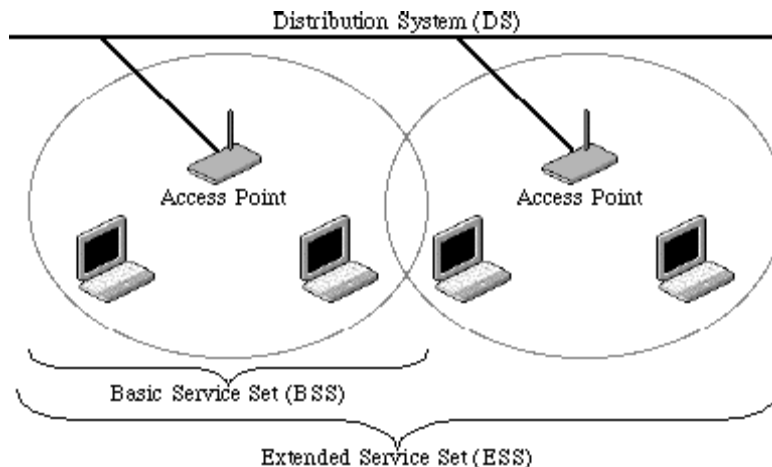
### 3. What are ISM bands?

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.

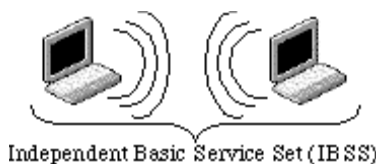
### 4. How does wireless networking work?

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 subnetwork. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in 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. What is BSSID?

A six-byte address that distinguishes a particular access point from others. Also known as just SSID. Serves as a network ID or name.

## 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.

## 7. What are potential factors that may cause 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.

## 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.

## 9. What is WEP?

An optional IEEE 802.11 function 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 encrypt 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.

## 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.

## 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.

## 12. What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes 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).

## 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.

## 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.

## 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.

#### 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.

#### 17. What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). 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.

#### 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.

#### 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.

#### 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.

#### 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.

#### 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.

#### 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. The default is value 1400.

#### 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.

#### 25. What is DDNS?

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

#### 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.

#### 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.

#### 28. What is IPSEC?

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

Notice : The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

## FCC INFORMATION

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

The equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user should not modify or change this equipment without written approval from Advanced Spectrum Technology CO., LTD.. Modification could void authority to use this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation