



# **User's Manual**

## **BOSSW77** **Wireless Radio CPE** **(Client Premises Equipment)**



# Table of Contents

<b>REVISION HISTORY .....</b>	<b>IV</b>
<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 FEATURES.....	1
1.2 PRODUCT SPECIFICATIONS.....	2
1.3 PACKAGE CONTENTS.....	3
1.4 NETWORK LAYOUT .....	3
1.5 INSTALLATION CONSIDERATIONS.....	3
1.6 APPLICATIONS.....	4
<b>2 SOFTWARE CONFIGURATION.....</b>	<b>10</b>
2.1 PREPARE YOUR PC TO CONFIGURE THE WLAN BROADBAND AP.....	10
2.2 CONNECT TO THE WLAN BROADBAND AP .....	11
2.3 MANAGEMENT AND CONFIGURATION ON THE WLAN BROADBAND AP .....	11
2.3.1 Status .....	11
2.3.2 Setup Wizard .....	13
2.3.3 Operation Mode .....	16
2.3.4 Wireless - Basic Settings.....	17
2.3.5 Wireless - Advanced Settings .....	19
2.3.6 Wireless - Security Setup.....	20
2.3.7 Wireless - Access Control.....	23
2.3.8 WDS Settings .....	24
2.3.9 Site Survey .....	26
2.3.10 LAN Interface Setup .....	27
2.3.11 WAN Interface Setup .....	29
2.3.12 Firewall - Port Filtering.....	36
2.3.13 Firewall - IP Filtering .....	37
2.3.14 Firewall - MAC Filtering.....	38
2.3.15 Firewall - Port Forwarding.....	39
2.3.16 Firewall – URL Filtering .....	40
2.3.17 Firewall - DMZ.....	41
2.3.18 VPN Setting .....	42
2.3.19 Management - Statistics.....	47
2.3.20 Management - DDNS.....	48
2.3.21 Management - Time Zone Setting.....	48
2.3.22 Management – Denial-of-Service.....	49
2.3.23 Management - Log .....	50

2.3.24	Management - Upgrade Firmware .....	51
2.3.25	Management Save/ Reload Settings.....	52
2.3.26	Management - Password Setup .....	53
2.3.27	MANAGEMENT-WATCHDOG.....	54
2.3.28	Management - Quality of Service .....	55
2.3.29	Logout .....	57
3	FREQUENTLY ASKED QUESTIONS (FAQ).....	58
3.1	WHAT AND HOW TO FIND MY PC'S IP AND MAC ADDRESS? .....	58
3.2	WHAT IS WIRELESS LAN?.....	58
3.3	WHAT ARE ISM BANDS?.....	58
3.4	HOW DOES WIRELESS NETWORKING WORK? .....	58
3.5	WHAT IS BSSID? .....	58
3.6	WHAT IS ESSID?.....	59
3.7	WHAT ARE POTENTIAL FACTORS THAT MAY CAUSES INTERFERENCE? .....	59
3.8	WHAT ARE THE OPEN SYSTEM AND SHARED KEY AUTHENTICATIONS? .....	59
3.9	WHAT IS WEP? .....	59
3.10	WHAT IS FRAGMENT THRESHOLD? .....	59
3.11	WHAT IS RTS (REQUEST TO SEND) THRESHOLD? .....	60
3.12	WHAT IS BEACON INTERVAL?.....	60
3.13	WHAT IS PREAMBLE TYPE?.....	60
3.14	WHAT IS SSID BROADCAST? .....	60
3.15	WHAT IS WI-FI PROTECTED ACCESS (WPA)? .....	61
3.16	WHAT IS WPA2? .....	61
3.17	WHAT IS 802.1X AUTHENTICATION? .....	61
3.18	WHAT IS TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)? .....	61
3.19	WHAT IS ADVANCED ENCRYPTION STANDARD (AES)? .....	61
3.20	WHAT IS INTER-ACCESS POINT PROTOCOL (IAPP)?.....	61
3.21	WHAT IS WIRELESS DISTRIBUTION SYSTEM (WDS)? .....	61
3.22	WHAT IS UNIVERSAL PLUG AND PLAY (UPNP)?.....	62
3.23	WHAT IS MAXIMUM TRANSMISSION UNIT (MTU) SIZE? .....	62
3.24	WHAT IS CLONE MAC ADDRESS?.....	62
3.25	WHAT IS DDNS? .....	62
3.26	WHAT IS NTP CLIENT? .....	62
3.27	WHAT IS VPN?.....	62
3.28	WHAT IS IPSEC?.....	62
4	TROUBLESHOOTING – Q & A .....	63

## Revision History

DATE	REVISION OF USER'S MANUAL	FIRMWARE
2008/1/10	Version 5.4	(g/v)5.4

## 1. Introduction

### BOSSW77

#### 802.11b/g Outdoor Radio CPE with 12dBi Antenna & N-type Connector

BOSSW77 outdoor CPE is an 802.11b/g low cost device for wireless solution. The device with integrated 12dBi patch antenna and N-Type female antenna connector for higher gain antenna offers a cost-effective solution for hotspot to make Point-to-Point and Point to Multi-Point applications.



#### All-in-One Device with Integrated 12 dBi Antenna and N-Female Connector

BOSSW77 is an all-in-one device with integrated Power Over Ethernet (PoE), 12dBi patch antenna, and the special designed waterproof cap for Ethernet RJ-45 connector to access long distance of network without extra power adapter and extra booster to enlarge the output power. The built-in N-Female connector provides option for higher gain or type of antenna on your request. A complete package with a DC injector / 48V DC Power adapter , waterproof cap, and standard pole mount kit are included.

#### 802.11B/G

The BOSSW77 complies with IEEE802.11b/g 2.4GHz specifications. Through the Web management interface, you can run in Client, AP, Bridge, or WDS function. A multiples security functions including 64/128 bit WEP, WPA, Port filtering, IP filtering, MAC filtering, Port forwarding and DMZ Hosting to prevent unauthorized access are in protected. The QoS settings provide different levels of quality to different types of network traffic with WMM stands to improve audio, video and voice applications. The VPN function can be used to communicate many branch office. The unique ACK timeout value can be adjusted according to distance to ensure optimal throughput at various distances.

#### 1.1 Features

- ✚ Integrated Powerful Radio and Antenna in an weatherproof enclosure
- ✚ Complies with IEEE 802.11b/g standard for 2.4GHz Wireless LAN
- ✚ Supports 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption function to protect the wireless data transmission.
- ✚ Supports IEEE 802.1x Authentication.
- ✚ Support Wi-Fi Protected Access Authentication with Radius and Pre-Shared Key mode.
- ✚ Supports Inter-Access Point Protocol (IAPP).
- ✚ Supports Wireless Distribution System (WDS).
- ✚ Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- ✚ Supports DHCP server to provide clients auto IP addresses assignment.
- ✚ Supports DHCP client for WAN interface auto IP address assignment from ISP.
- ✚ Supports PPPoE on WAN interface.
- ✚ Supports PPTP Client on Ethernet WAN interface.
- ✚ Supports clone MAC address function.
- ✚ Supports firewall security with port filtering, IP filtering, MAC filtering, port forwarding, trigger port, DMZ hosting and URL filtering functions.
- ✚ Supports WEB based management and configuration.
- ✚ Supports UPnP for automatic Internet access.
- ✚ Supports Dynamic DNS service.
- ✚ Supports NTP client service.

- ✚ Supports Log table and remote Log service.
- ✚ Support Setup Wizard mode.
- ✚ Support DoS (Denial of Service) function.
- ✚ Support WMM function.
- ✚ Support Ping watchdog.
- ✚ Support QoS/Bandwidth Control function.

## 1.2 Product Specifications

<b>Interfaces</b>	<ul style="list-style-type: none"> <li>● 10/100Mbps auto crossover Ethernet WAN Port (RJ45) (For connecting to 3rd party network device)</li> <li>● Built-in N-Type female connector for higher gain antenna</li> </ul>
<b>Standard</b>	<ul style="list-style-type: none"> <li>● IEEE802.11b</li> <li>● IEEE802.11g</li> <li>● IEEE802.3</li> <li>● IEEE802.3u</li> </ul>
<b>Frequency Band</b>	<ul style="list-style-type: none"> <li>● FCC : 2.412-2.462 GHz (1-11 channels)</li> <li>● Europe (ETSI) : 2.412-2.472 GHz (1-13 channels)</li> <li>● Japan : 2.412-2.482 GHz (1-13 channels)</li> <li>● France : 2.457-2.472 GHz (10-13 channels)</li> </ul>
<b>Modulation Technology</b>	<ul style="list-style-type: none"> <li>● 802.11b: Direct Sequence Spread Spectrum (PBCC, CCK, DQPSK, DBPSK)</li> <li>● 802.11g: Orthogonal frequency division multiplexing</li> </ul>
<b>Data Rate</b>	<ul style="list-style-type: none"> <li>● 802.11b: 11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps</li> <li>● 802.11g: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps</li> </ul>
<b>Transmit Power</b>	<ul style="list-style-type: none"> <li>● 26dBm/11b</li> </ul>
<b>Sensitivity</b>	<ul style="list-style-type: none"> <li>● -80 dBm (11Mbps), -68 dBm(54Mbps)</li> </ul>
<b>Operation Modes</b>	<ul style="list-style-type: none"> <li>● AP, Client, Bridge, and Repeater Modes</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>● 64bit/128 bit WEP, WPA, WPA2, IEEE802.1x Authentication, port filtering, IP filtering, MAC filtering, port forwarding, and DMZ hosting</li> </ul>
<b>Firmware</b>	<ul style="list-style-type: none"> <li>● Web-Based Management Tool</li> <li>● Firmware upgrade via HTTP browser</li> <li>● RADIUS server support</li> <li>● Multi-SSID</li> <li>● WMM</li> <li>● Dos (Denial of Service)</li> <li>● Site Survey</li> </ul>
<b>Antenna Type</b>	<ul style="list-style-type: none"> <li>● Integrated 12dBi flat panel antenna</li> </ul>
<b>Dimension &amp; Weight</b>	<ul style="list-style-type: none"> <li>● 165*150*75mm (0.7KGS)</li> </ul>
<b>Environment</b>	<ul style="list-style-type: none"> <li>● Operating Temperature:-30 ~ +70°C</li> <li>● Humidity: C95%@55°C</li> </ul>
<b>Enclosure</b>	<ul style="list-style-type: none"> <li>● IP65 UV resistant weatherproof enclosure</li> </ul>
<b>Power Adapter</b>	<ul style="list-style-type: none"> <li>● 100-240V(50-60Hz) universal AC adapter (DC 48V)</li> <li>● Power over Ethernet DC injector included</li> </ul>
<b>Mounting</b>	<ul style="list-style-type: none"> <li>● Pole Mounting</li> </ul>

The specifications listed above are subject to change without prior notice

### 1.3 Package contents

1. CPE
2. Waterproof Connector
3. Plastic cover for N-type connector
4. 48V DC Power Adapter with base unit for PoE
5. Mount kit
6. *User Manual CD*



### 1.4 Network Layout

BOSSW77 is compatible with 802.11g and 802.11b adapters. Since the 802.11g shares the same 2.4GHz radio band with the 802.11b technology, it can inter-operate with existing 802.11b devices. Therefore, it can reserve your existing investment in 802.11b client cards such as the PC cards for laptop computers, PCI Card for the desktop PC, and USB Adapters. When connecting to wired network with wireless network, it's network port can be used to connect any of switches, routers, and wireless Print Server.

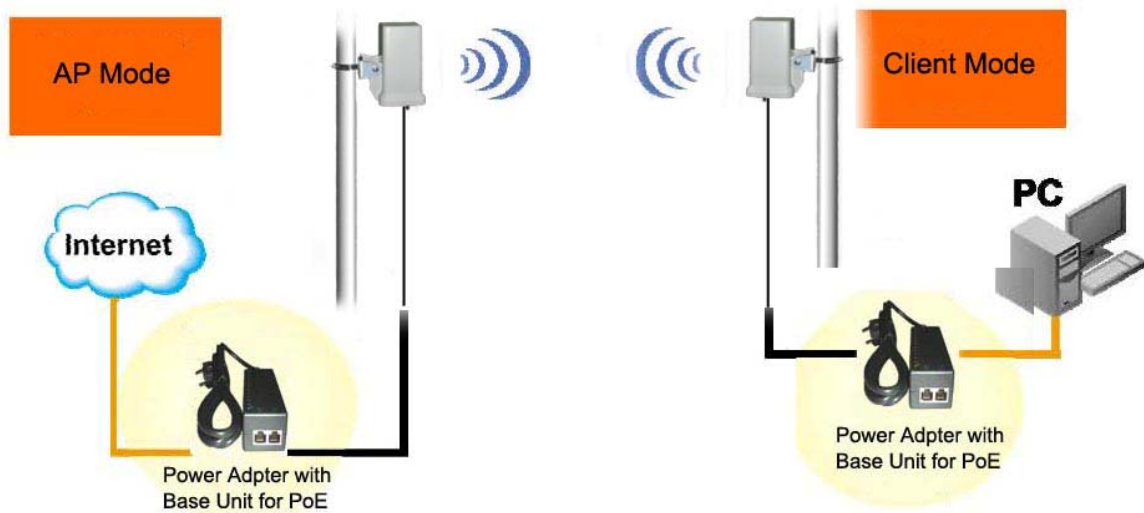
### 1.5 Installation Considerations

The WLAN device allow to access a network with a wireless connection from anywhere with its operating range. However, the effectively and efficiently range of WLAN device is affected by not only the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, but also the types of materials and background RF (radio frequency) noise in your home or business. To maximizing wireless range, follow up these basic guidelines:

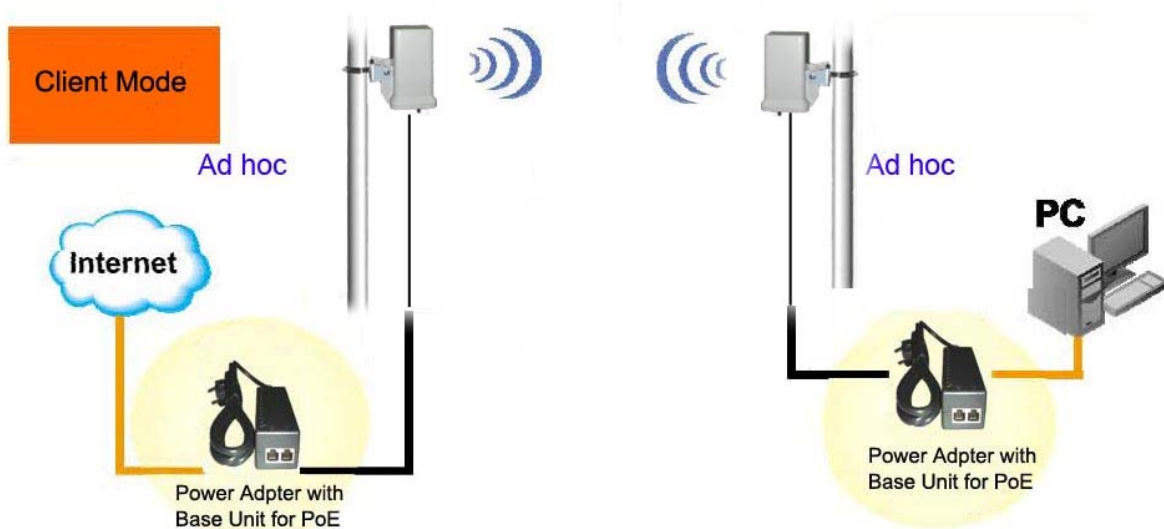
- Keep the WLAN device away (at least 3-6 feet or 1-2 meters) from other electrical devices or appliances that generate RF noise such as microwaves, monitors, electric motors.
- Minimizing the numbers of walls and ceilings between the WLAN device and other network devices. Each wall or ceiling can reduce the WLAN device's range from 3-90 feet (1-30 meters).
- Position the WLAN antenna in a direct line to network devices for the best reception. A wall with 1.5 feet thick (.5 meters) at a 45-degree angle is equal to 3 feet (1 meter) thick, at a 2-degree angle is equal to 42 feet (14meters) thick. Positing the WLAN antenna that the signal will go straight through a wall or ceiling (instead of at an angle) for better reception.
- Building Materials such as metal door and aluminum studs can impede the wireless signal. Try to best position WLAN device and computers to avoid the signal passes through those obstacles.

## 1.6 Applications

### Network Topology – AP Mode and Client Mode

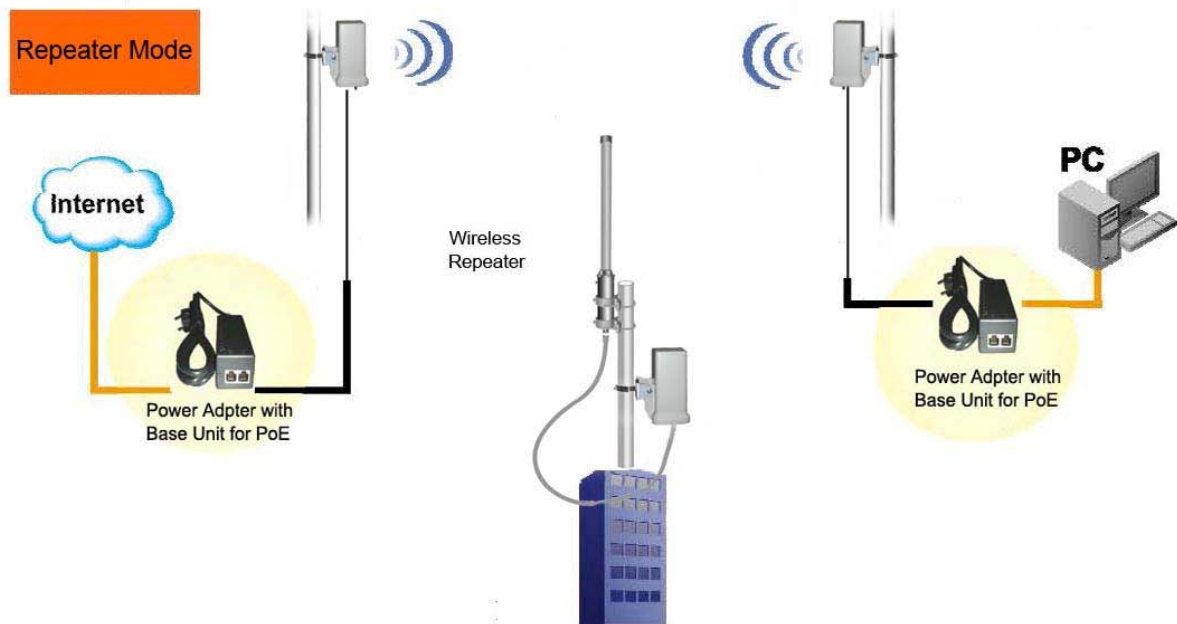


### Network Topology – Peer to Peer Bridge Mode

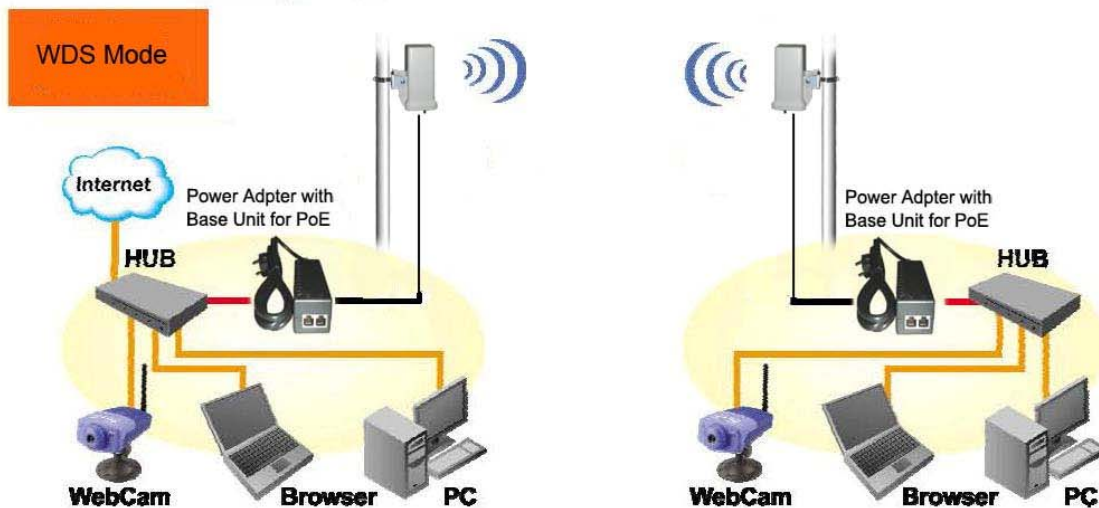


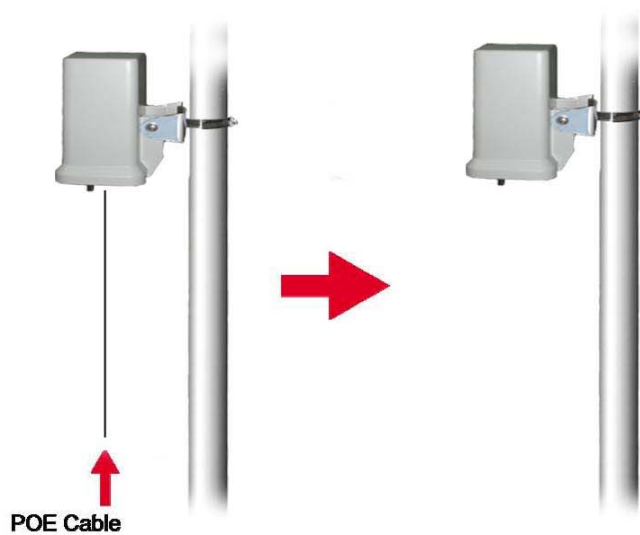
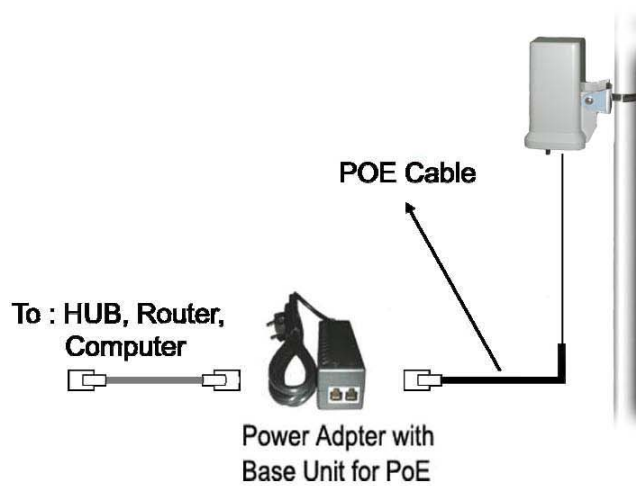


## Network Topology – Repeater Mode



## Network Topology – WDS Point to Point Mode

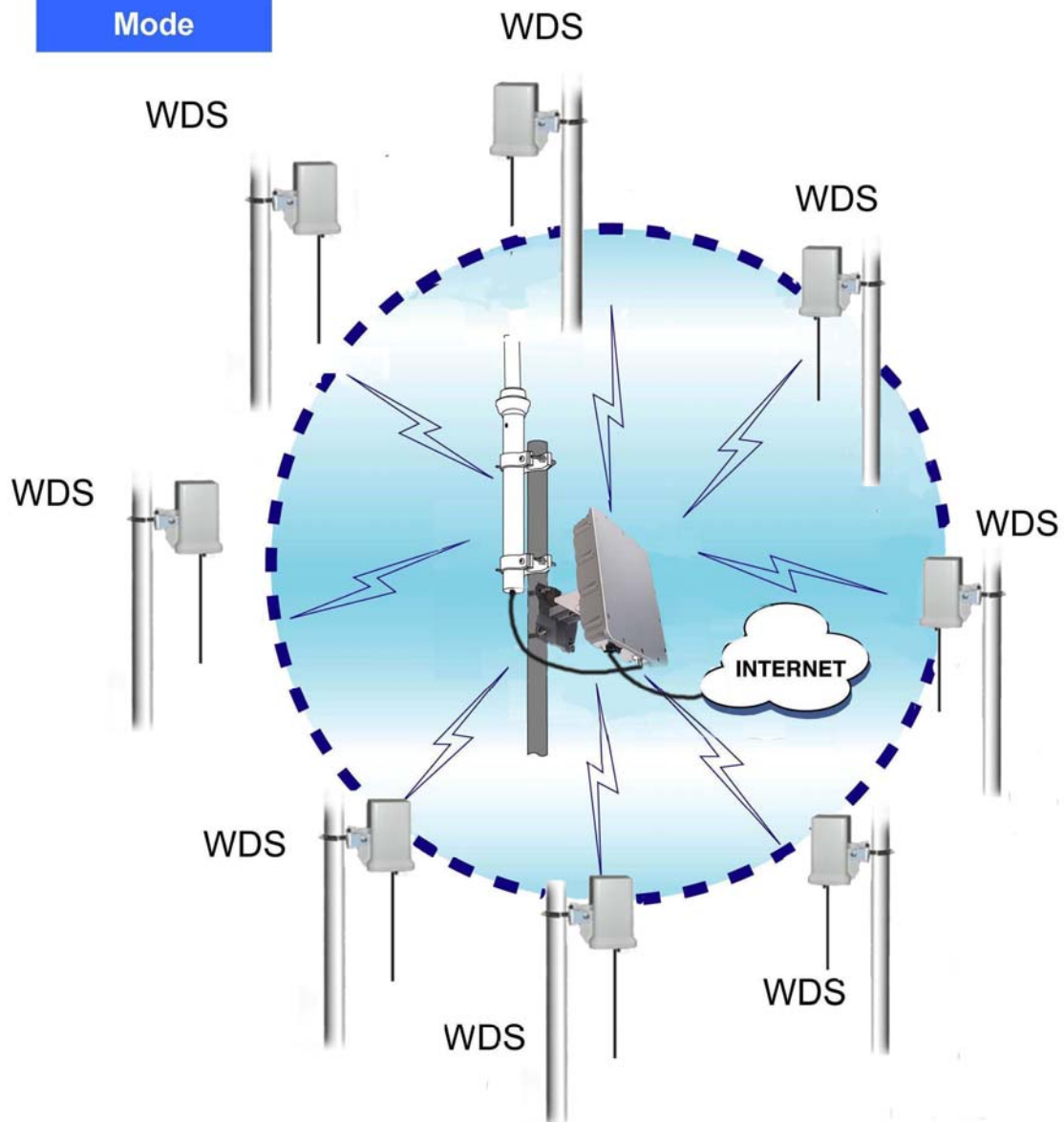




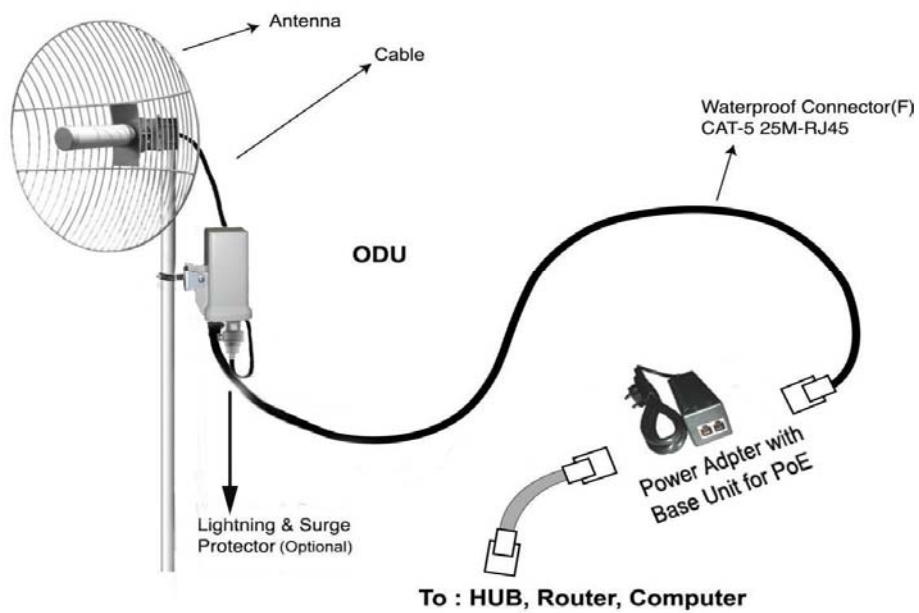
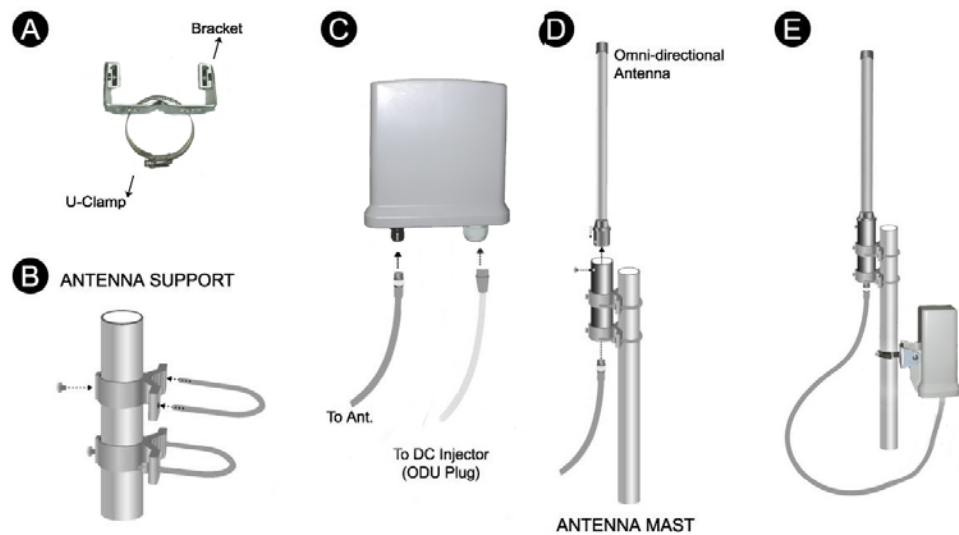
CPE Installation Diagram

## Network Topology – WDS Point to Multi-Point Mode

WDS P2MP  
Mode



### ***Omni-Directional Antenna Installation Diagram***



CPE Installation Diagram

**Installation Diagram**



**Attention:**

- The cable distance between the Router and PC/hub/Switch should not exceed 100 meters.
- Make sure the wiring is correct. To reliably operate your network at 100Mbps, you must use Category 5 cable, or better Data Grade.

## 2 Software configuration

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

The WLAN device 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>**

### 2.1 Prepare your PC to configure the WLAN Broadband AP

**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.
2. **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
3. Move mouse and double-click the right button on **Network** icon. The **Network** window will appear.
4. 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.
5. Select **Protocol** in the **Network Component Type** dialog box and click **Add** button.
6. 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.
7. Select **TCP/IP** and click the **properties** button on the **Network** dialog box.
8. Select **Specify an IP address** and type in values as following example.
  - ✓ IP Address: **192.168.1.254**, 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**
9. 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: **192.168.1.254**, 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 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: **192.168.1.254**, 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.

## 2.2 Connect to the WLAN Broadband AP

Open a WEB browser, i.e. Microsoft Internet Explore, then enter 192.168.1.254 on the URL to connect the WLAN device.

## 2.3 Management and configuration on the WLAN Broadband AP

### 2.3.1 Status

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

**BOSSLAN**  
IP TECHNOLOGY

Site contents:  
 Status  
 Setup Wizard  
 Operation Mode  
 Wireless  
 TCP/IP Settings  
 Firewall  
 VPN Setting  
 Management

## Broadband Router Status

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

System	
Uptime	18day:2h:20m:12s
Firmware Version	v5.3

Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	MyWLAN
Channel Number	11
Encryption	WEP 64bits
BSSID	00:02:72:5d:35:5f
Associated Clients	0

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DHCP Server	Enabled
MAC Address	00:02:72:5d:35:5f

WAN Configuration	
Attain IP Protocol	PPPoE Connected
IP Address	125.225.136.17
Subnet Mask	255.255.255.255
Default Gateway	125.225.128.254
DNS 1	168.95.192.1
DNS 2	168.95.1.1
DNS 3	0.0.0.0
MAC Address	00:02:72:5d:35:60

Screen snapshot – Status

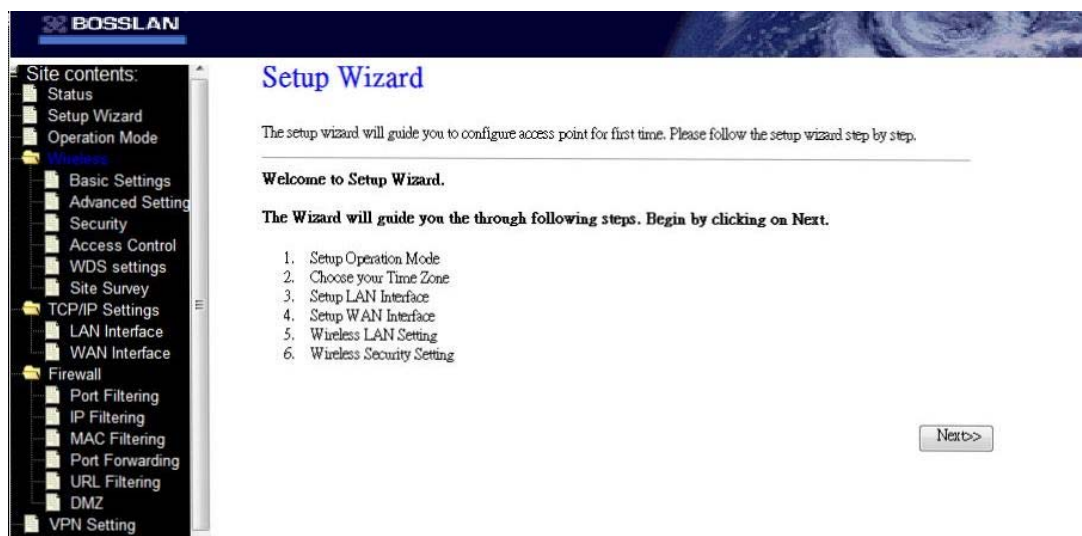
Item	Description
System	
Uptime	It shows the duration since WLAN device is powered on.
Firmware version	It shows the firmware version of WLAN device.
Wireless configuration	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this WLAN device. The SSID is the unique name of WLAN device 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 device. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
TCP/IP configuration	
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of WLAN device.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of WLAN



	device.
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 device.
WAN configuration	
Attain IP Protocol	It shows how the WLAN device 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 device.
Subnet Mask	It shows the IP subnet mask of WAN interface of WLAN device.
Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
DNS1/DNS2/DNS3	It shows the DNS service information
MAC Address	It shows the MAC address of WAN interface of WLAN device.

### 2.3.2 Setup Wizard

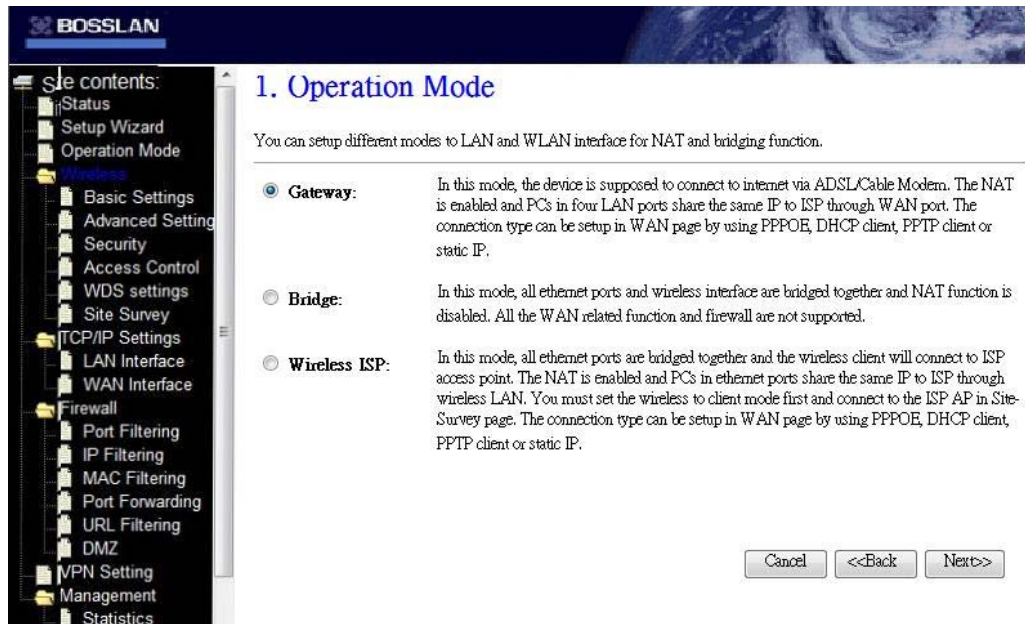
This page guides you to configure wireless broadband router for first time



Screen snapshot – Setup Wizard

### I Operation Mode

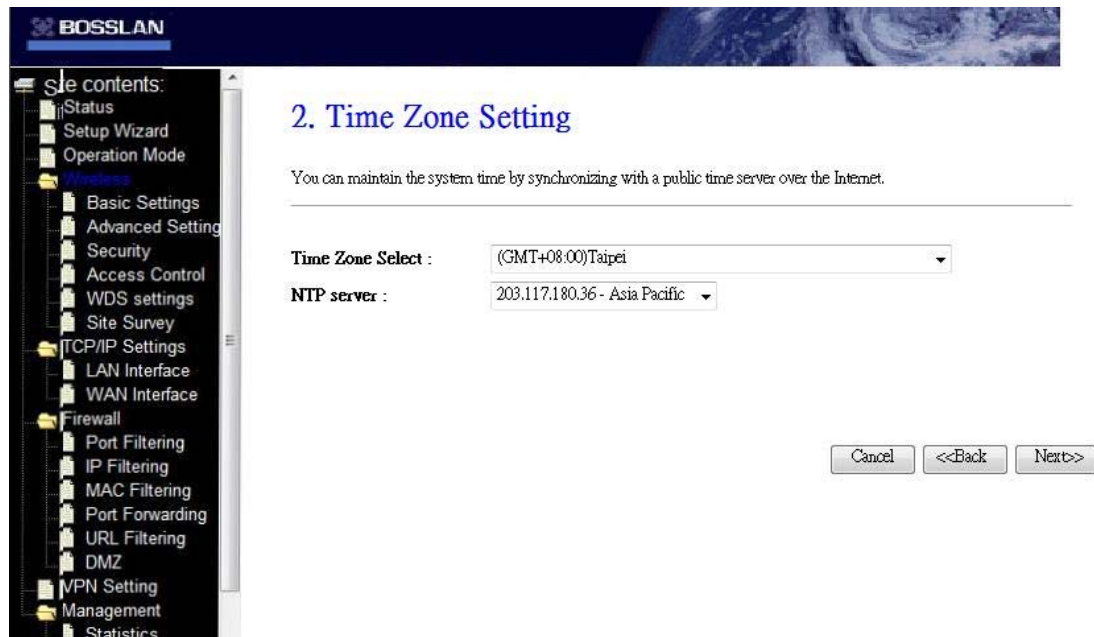
This page is used to configure which mode wireless broadband router acts



Screen snapshot – Operation Mode

## II Time Zone Setting

This page is used to enable and configure NTP client



Screen snapshot – Time Zone Settings

## III LAN Interface Setup

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

The screenshot shows the BOSSLAN web interface. On the left is a tree menu with categories like 'Site contents', 'Wireless', 'TCP/IP Settings', 'Firewall', and 'VPN Setting'. The 'LAN Interface' option under 'TCP/IP Settings' is selected. The main content area is titled '3. LAN Interface Setup'. It contains a description: '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..'. Below this are two input fields: 'IP Address' with the value '192.168.2.1' and 'Subnet Mask' with the value '255.255.255.0'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

Screen snapshot – LAN Interface Setup

#### IV WAN Interface Setup

This page is used to configure WAN access type

The screenshot shows the BOSSLAN web interface with the 'WAN Interface' option selected in the tree menu. The main content area is titled '4. WAN Interface Setup'. It contains a description: '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.'. Below this are three input fields: 'WAN Access Type' with a dropdown menu showing 'PPPoE', 'User Name' with the value '88277535@hinet.net', and 'Password' with a masked input (dots). At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

Screen snapshot – WAN Interface Setup

#### V 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)

Screen snapshot – Wireless Basic Settings

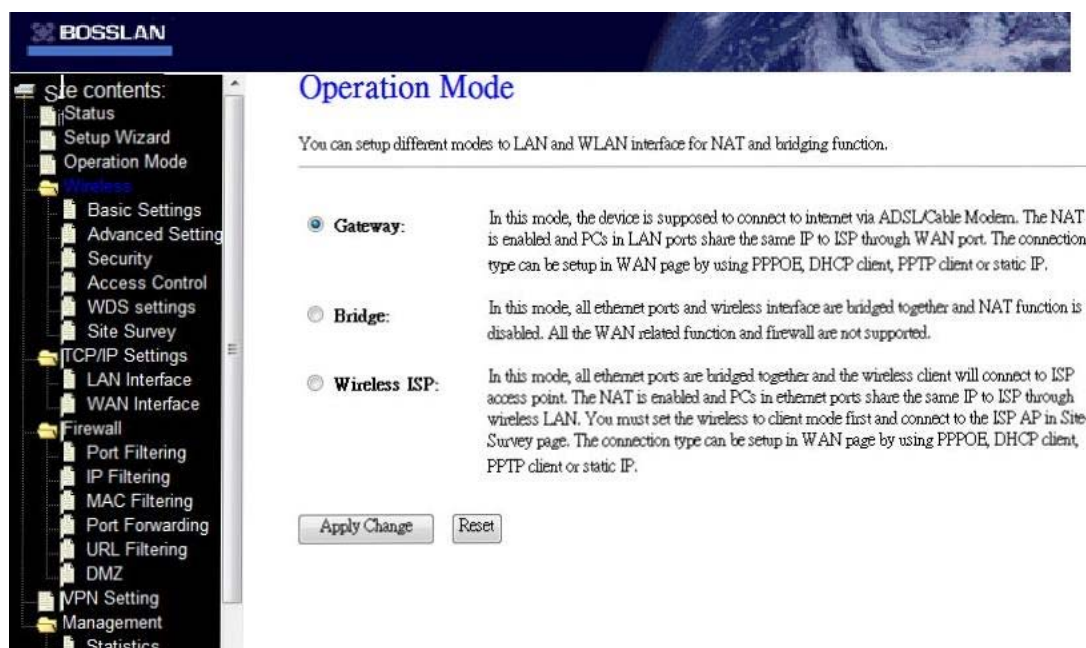
## VI Wireless Security Setup

This page is used to configure wireless security

Screen snapshot – Wireless Security Setup

### 2.3.3 Operation Mode

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



Screen snapshot – Operation Mode

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>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.

#### 2.3.4 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.





Screen snapshot – Wireless Basic Settings

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.
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.

### 2.3.5 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 device.

**BOSSLAN**

## 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:** ☐ Open System ☐ Shared Key ☒ Auto

**Fragment Threshold:**  (256-2346)

**RTS Threshold:**  (0-2347)

**Beacon Interval:**  (20-1024 ms)

**Data Rate:**

**Preamble Type:** ☒ Long Preamble ☐ Short Preamble

**Broadcast SSID:** ☒ Enabled ☐ Disabled

**IAPP:** ☒ Enabled ☐ Disabled

**802.11g Protection:** ☒ Enabled ☐ Disabled

**Turbo Mode:** ☐ Auto ☐ Always ☒ Off  
 Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

**Block Relay Between Clients:** ☐ Enabled ☒ Disabled

**WMM:** ☒ Enabled ☐ Disabled

**ACK Timeout:**  (0-255) < Current: 11b: 316us / 11g: 72us >

**CCK Level:** ☒ Default(18-19dbm) ☐ Enhanced(20-23dbm) ☐ Maximum(24-26dbm)

Screen snapshot – Wireless Advanced Settings

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. Refer to <a href="#">4.10 What is Fragment Threshold?</a>
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes. Refer to <a href="#">4.11 What is RTS(Request To Send) Threshold?</a>
Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms. Refer to <a href="#">4.12 What is Beacon Interval?</a>
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. Refer to <a href="#">4.13 What is Preamble Type?</a>

Broadcast SSID	Click to enable or disable the SSID broadcast function. Refer to <a href="#">4.14 What is SSID Broadcast?</a>
IAPP	Click to enable or disable the IAPP function. Refer to <a href="#">4.20 What is Inter-Access Point Protocol(IAPP)?</a>
802.11g Protection	Protect 802.11b user.
Turbo Mode	Click to enable/disable turbo mode. ( <b>Only apply to WLAN IC of Realtek</b> ).
Block Relay Between Clients	Click Enabled/Disabled to decide if blocking relay packets between clients.
WMM	Click Enable/Disabled to init WMM feature.
ACK Timeout	Set ACK timeout value. It shows current time in the end.
CCK Level	To adjust transmission power level.
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.

### 2.3.6 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.

**BOSSLAN**

## 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:

☐ Use 802.1x Authentication ☒ WEP 64bits ☐ WEP 128bits

WPA Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

Pre-Shared Key Format:

Pre-Shared Key:

☐ Enable Pre-Authentication

Authentication RADIUS Server: Port  IP address  Password

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

Screen snapshot – Wireless Security Setup



Item	Description
Encryption	<p>Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA(TKIP), WPA2 or WPA2 Mixed</p> <p>Refer to <a href="#">4.9 What is WEP?</a>  <a href="#">4.15 What is Wi-Fi Protected Access (WPA)?</a>  <a href="#">4.16 What is WPA2(AES)?</a>  <a href="#">4.17 What is 802.1X Authentication?</a>  <a href="#">4.18 What is Temporal Key Integrity Protocol (TKIP)?</a> <a href="#">4.19 What is Advanced Encryption Standard (AES)?</a></p>
Use 802.1x Authentication	<p>While Encryption is selected to be WEP.</p> <p>Click the check box to enable IEEE 802.1x authentication function.</p> <p>Refer to <a href="#">4.16 What is 802.1x Authentication?</a></p>
WPA Authentication Mode	<p>While Encryption is selected to be WPA.</p> <p>Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key).</p> <p>Refer to <a href="#">4.15 What is Wi-Fi Protected Access (WPA)?</a></p>
Pre-Shared Key Format	<p>While Encryption is selected to be WPA.</p> <p>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></p>
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]
Authentication RADIUS Server	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.

## I 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

Screen snapshot – WEP Key Setup

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>Apply Changes</b> button to complete the new configuration setting.
Close	Click to close this WEP Key setup window.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

WEP encryption key (secret key) length

Format \ Length	64-bit	128-bit
	64-bit	128-bit
ASCII	5 characters	13 characters
HEX	10 hexadecimal codes	26 hexadecimal codes

### 2.3.7 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.

**BOSSLAN**

Site contents:

- Status
- Setup Wizard
- Operation Mode
- Wireless
  - Basic Settings
  - Advanced Settings
  - Security
  - Access Control
  - WDS settings
  - Site Survey
- TCP/IP Settings
- LAN Interface
- WAN Interface
- Firewall
  - Port Filtering
  - IP Filtering
  - MAC Filtering
  - Port Forwarding
  - URL Filtering
  - DMZ
- VPN Setting
- Management
  - Statistics
  - DDNS
  - Time Zone Setting
  - Denial-of-Service
- Log

## 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:

MAC Address:  Comment:

Current Access Control List:

MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>		

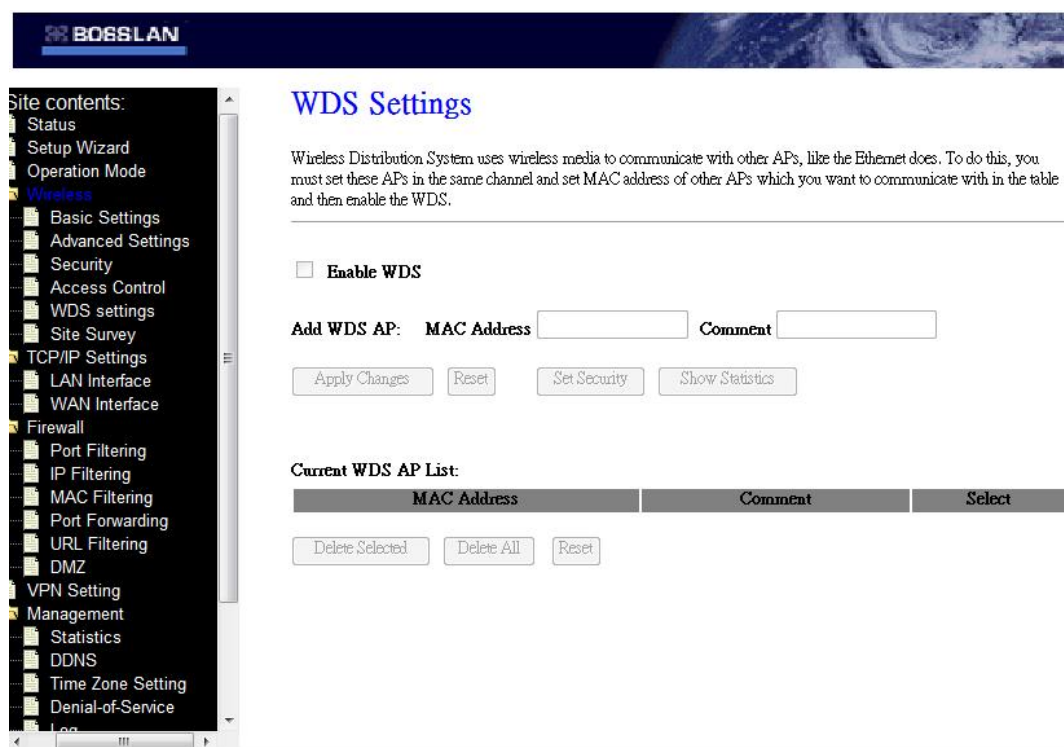
Screen snapshot – Wireless Access Control

Item	Description
Wireless Access Control Mode	Click the <b>Disabled</b> , <b>Allow Listed</b> or <b>Deny Listed</b> 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 device.
MAC Address	Fill in the MAC address of client to register this WLAN device access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the <b>Apply Changes</b> button to register the client to new configuration setting.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.
Current Access Control	It shows the registered clients that are allowed to link to this

List	WLAN device.
Delete Selected	to delete the selected clients that will be access right removed from this WLAN device.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the <b>Reset</b> button to abort change and recover the previous configuration setting.

### 2.3.8 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.



Screen snapshot – WDS Setup

Item	Description
Enable WDS	the check box to enable wireless distribution system. Refer to <a href="#">4.21 What is Wireless Distribution System (WDS)?</a>
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	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.

## I WDS Security Setup

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

This page is used to configure the wireless security between APs. Refer to [3.3.6 Wireless Security Setup](#).

Screen snapshot – WDS Security Setup

## II 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

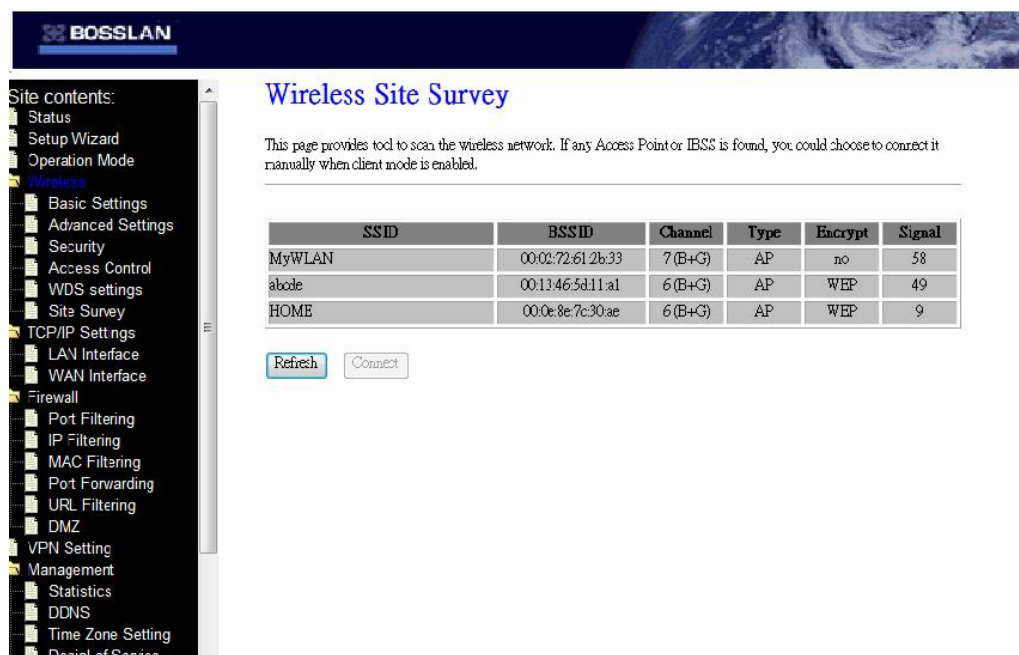


Screen snapshot – WDS AP Table

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 Rare (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.

### 2.3.9 Site Survey

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



Screen snapshot – Wireless Site Survey

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.

### 2.3.10 LAN Interface Setup

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

**BOSSLAN**

**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:   
 DHCP Client Range:  -    
 Domain Name:   
 802.1d Spanning Tree:   
 Clone MAC Address:

Screen snapshot – LAN Interface Setup

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>
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. Refer to <a href="#">4.24 What is Clone MAC Address?</a>
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.



### I Active DHCP Client Table

This table shows the assigned IP address, MAC address, and time expired for each DHCP leased client.

#### Active DHCP Client Table

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
192.168.2.2	00:16:17:4e:8e:c2	856124
192.168.2.3	00:00:e2:6b:fa:56	511641
192.168.2.4	00:0f:fe:22:4f:6c	857677
192.168.2.10	00:1a:a0:29:7c:31	857720
192.168.2.5	00:02:72:5fa0:be	80286
192.168.2.6	00:15:b7:40:54:5c	856130

Screen snapshot – WAN Interface Setup – Active DHCP Client Table

### 2.3.11 WAN Interface Setup

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

## I Static IP

**BOSSLAN**

## 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:** 172.1.1.1

**Subnet Mask:** 255.255.255.0

**Default Gateway:** 172.1.1.254

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

**DNS 1:** 168.95.192.1

**DNS 2:** 168.95.1.1

**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

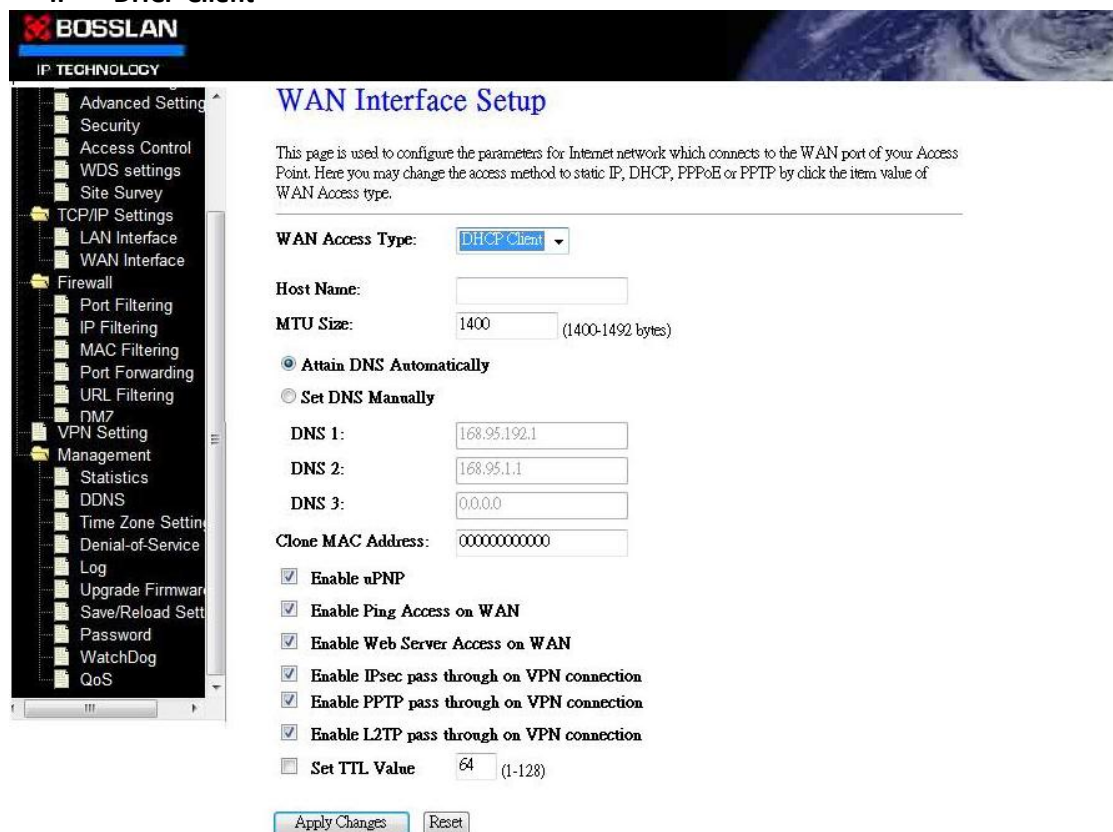
☐ Set TTL Value 64 (1-128)

Screen snapshot – WAN Interface Setup – Static IP

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. Refer to 4.24 What is Clone MAC Address?

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 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.

## II DHCP Client



**BOSSLAN**  
IP TECHNOLOGY

**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)

Screen snapshot – WAN Interface Setup – DHCP Client

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. Refer to <a href="#">4.24 What is Clone MAC Address?</a>
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 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.

### III PPPoE

**BOSSLAN**

## 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:** PPPoE

**User Name:**

**Password:**

**Service Name:**

**Connection Type:** Continuous Connect Disconnect

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

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

Apply Changes Reset

Screen snapshot – WAN Interface Setup – PPPoE

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.

**Continuous** connection type means to setup the connection through PPPoE protocol whenever this WLAN device is powered on.

**Connect on Demand** 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.

**Manual** connection type means to setup the connection through the PPPoE protocol by clicking the **Connect** button manually, and clicking the **Disconnect** 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. Refer to <a href="#">4.23 What is Maximum Transmission Unit (MTU) Size?</a>
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. Refer to <a href="#">4.24 What is Clone MAC Address?</a>
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 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.

## IV PPTP

**BOSSLAN**

**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:** 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:** 168.95.192.1

**DNS 2:** 168.95.1.1

**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)

Screen snapshot – WAN Interface Setup – PPTP

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.

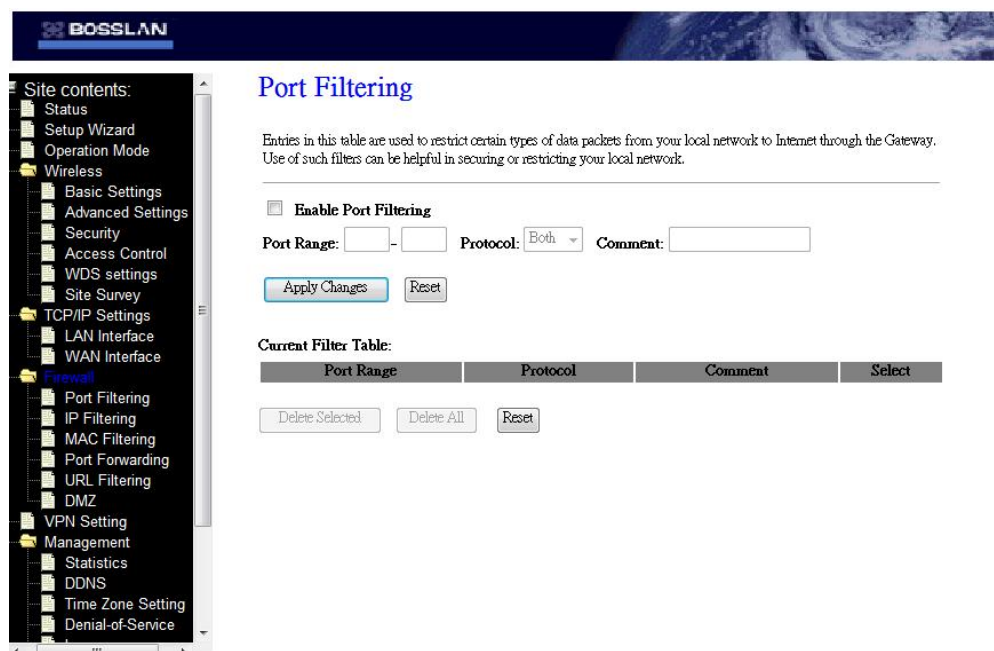


Password	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1400. Refer to <a href="#">4.23 What is Maximum Transmission Unit (MTU) Size?</a>
Request MPPE Encryption	Click the checkbox 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. Refer to <a href="#">4.24 What is Clone MAC Address?</a>
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 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.

### 2.3.12 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.



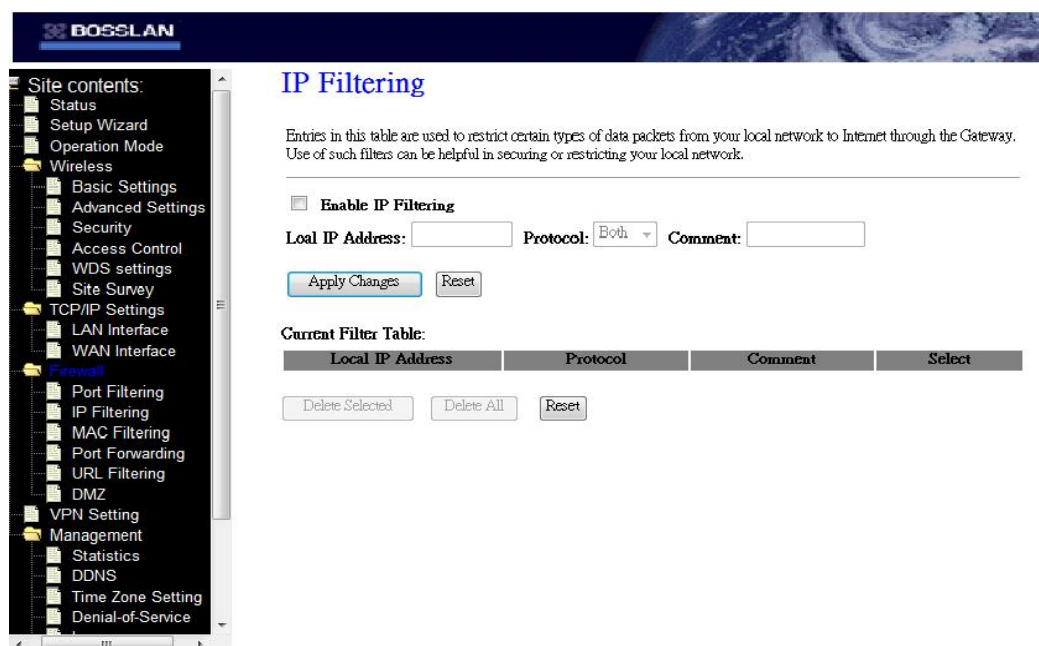


Screen snapshot – Firewall - Port Filtering

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. The <b>Protocol</b> can be TCP, UDP or Both. <b>Comments</b> let you know about whys to restrict data from the ports.
Protocol	
Comments	
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.

### 2.3.13 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.

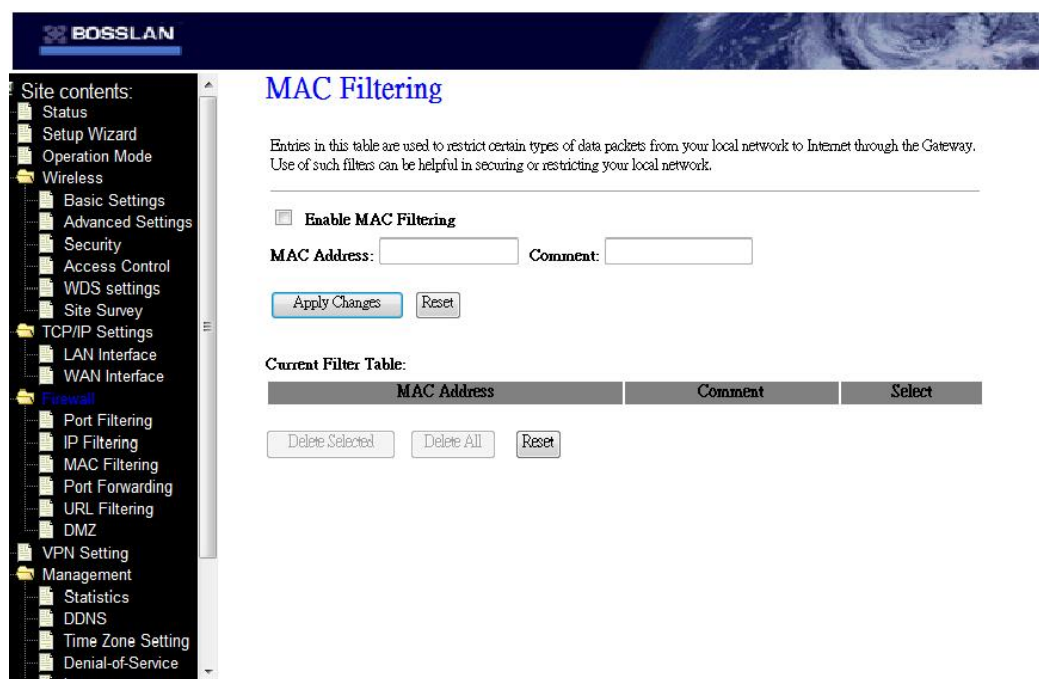


Screen snapshot – Firewall - IP Filtering

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.
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 IP address.
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.

### 2.3.14 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.

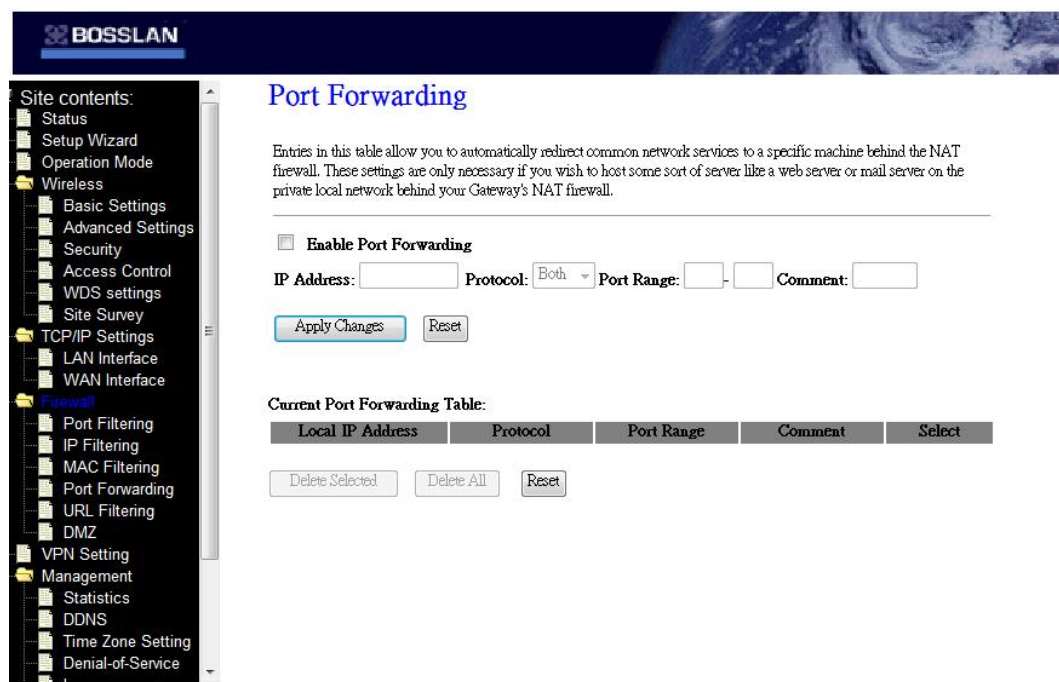


Screen snapshot – Firewall - MAC Filtering

Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address	To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it.
Comments	<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.

### 2.3.15 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.



Screen snapshot – Firewall - Port Forwarding

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,
Protocol	fill in the IP address, protocol, port range and your comments.
Port Range	The <b>Protocol</b> can be TCP, UDP or Both.
Comment	The <b>Port Range</b> for data transmission.
	<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.

### 2.3.16 Firewall – URL Filtering

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

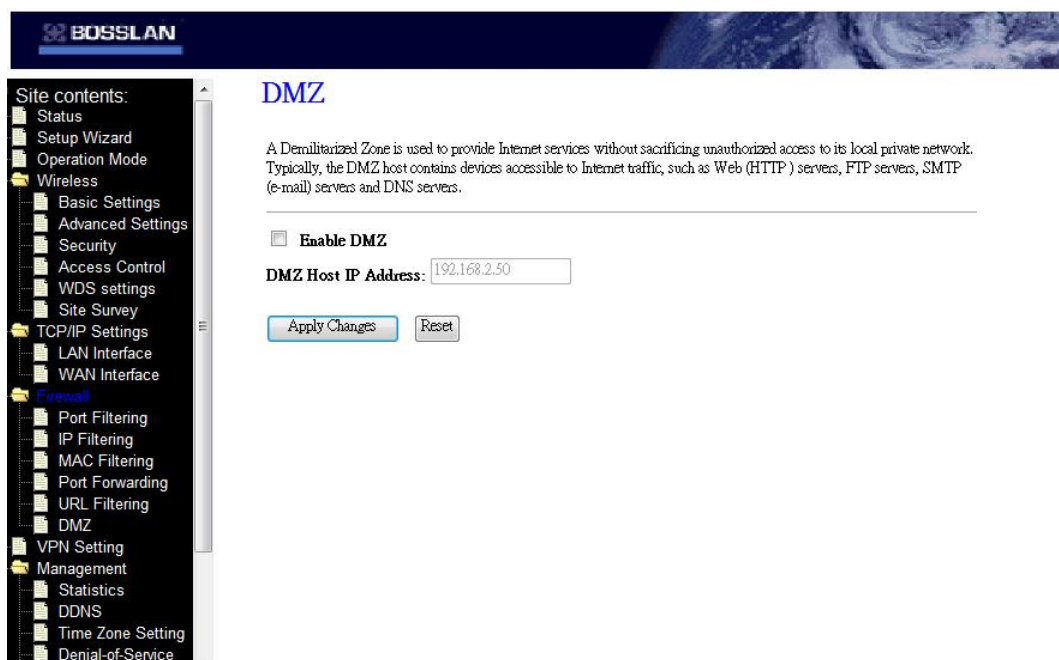


Screen snapshot – Firewall – URL Filtering

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.

### 2.3.17 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.

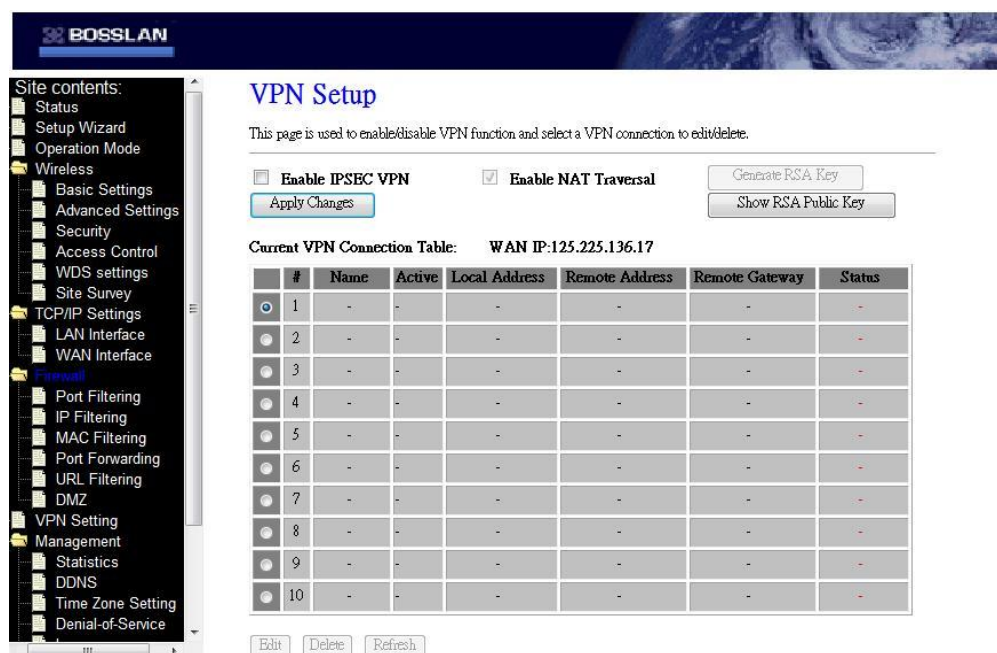


Screen snapshot – Firewall - DMZ

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.

### 2.3.18 VPN Setting

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



Screen snapshot – VPN Setup

Item	Description
Enable IPSEC VPN	Click to enable IPSEC VPN function. Refer to <a href="#">4.27 What is VPN?</a> And <a href="#">4.28 What is IPSEC?</a>
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.



## I VPN Setup - Edit Tunnel

**BOSSLAN**

**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:

**Key Management:** ☒ IKE ☐ Manual

Connection Type:

ESP:  (Encryption Algorithm)

MD5:  (Authentication Algorithm)

PreShared Key:

Remote RSA Key:

Status: Disconnected

Screen snapshot – VPN Setup-Edit Tunnel

Item	Description
Enable Tunnel 1	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	Click to select <b>IKE</b> or <b>Manual</b> mode.
Advanced	Click <b>Advanced</b> button to configure more IKE settings.
Connection Type	Click to select <b>Initiator</b> or <b>Responder</b> 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 <b>3DES</b> , <b>AES128</b> or <b>NULL</b> encryption. Click to configure <b>MD5</b> or <b>SHA1</b> 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 <b>Apply Changes</b> button to save current tunnel settings.
Reset	Click the <b>Reset</b> 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.

## II 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 ▼

Screen snapshot – Advanced VPN Settings for IKE

Item	Description
Phase 1	
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.
Phase 2	
Active Protocol	ESP.
Encryption Algorithm	Click to select <b>3DES</b> , <b>AES128</b> or <b>NULL</b> encryption.
Authentication Algorithm	Click to select <b>MD5</b> or <b>SHA1</b> authentication.

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

### 2.3.19 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	Sent Packets	678663
	Received Packets	3966059
Ethernet LAN	Sent Packets	8416440
	Received Packets	5419685
Ethernet WAN	Sent Packets	5394470
	Received Packets	7620150

Refresh

Screen snapshot – Management - Statistics

Item	Description
Wireless LAN <b>Sent Packets</b>	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN <b>Received Packets</b>	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN <b>Sent Packets</b>	It shows the statistic count of sent packets on the Ethernet LAN interface.
Ethernet LAN <b>Received Packets</b>	It shows the statistic count of received packets on the Ethernet LAN interface.
Ethernet WAN <b>Sent Packets</b>	It shows the statistic count of sent packets on the Ethernet WAN interface.
Ethernet WAN	It shows the statistic count of received packets on the

**Received Packets**

Ethernet WAN interface.

**Refresh**

Click the refresh the statistic counters on the screen.

**2.3.20 Management - DDNS**

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

Screen snapshot – Management – DDNS

Item	Description
Enable DDNS	Click the checkbox to enable <b>DDNS</b> service. Refer to <a href="#">4.25 What is DDNS?</a>
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.

**2.3.21 Management - Time Zone Setting**

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

Screen snapshot – Management – Time Zone Settings

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. Refer to <a href="#">4.26 What is NTP Client?</a>
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.

### 2.3.22 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.

**BOSSLAN**

**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**

☐ Whole System Flood: SYN  Packets/Second

☐ Whole System Flood: FIN  Packets/Second

☐ Whole System Flood: UDP  Packets/Second

☐ Whole System Flood: ICMP  Packets/Second

☐ Per-Source IP Flood: SYN  Packets/Second

☐ Per-Source IP Flood: FIN  Packets/Second

☐ Per-Source IP Flood: UDP  Packets/Second

☐ Per-Source IP Flood: ICMP  Packets/Second

☐ TCP/UDP PortScan  Sensitivity

☐ ICMP Smurf

☐ IP Land

☐ IP Spoof

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

☐ UDP Bomb

☐ UDP EchoChargen

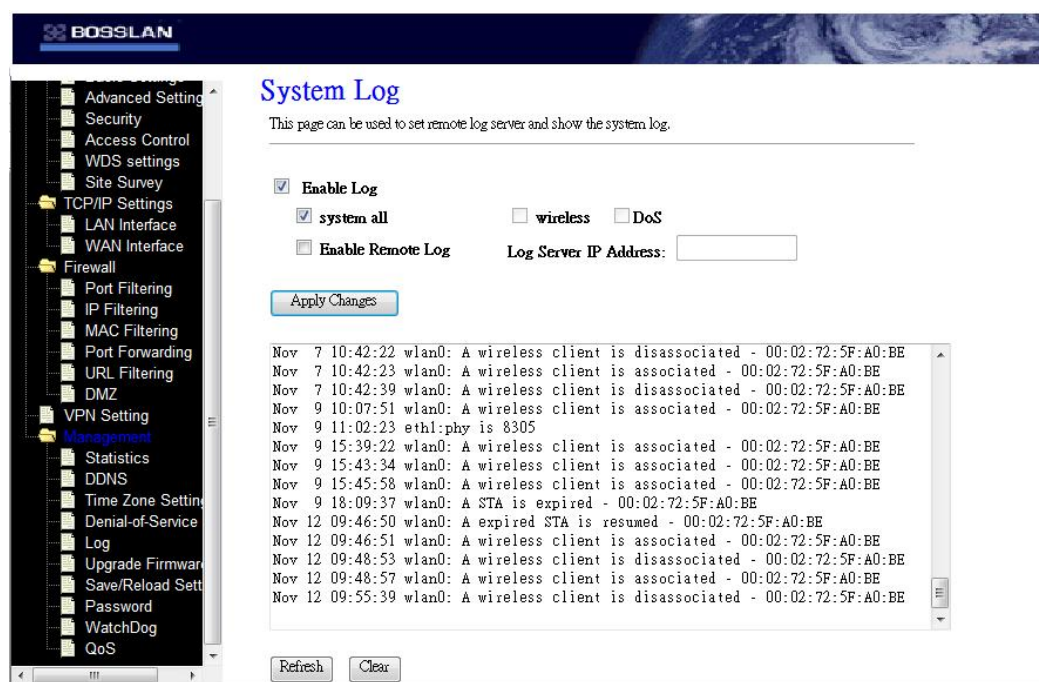
☐ Enable Source IP Blocking  Block time (sec)

Screen snapshot – Management – Denial-of-Service

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 <b>Apply Changes</b> button to save above settings.

### 2.3.23 Management - Log

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



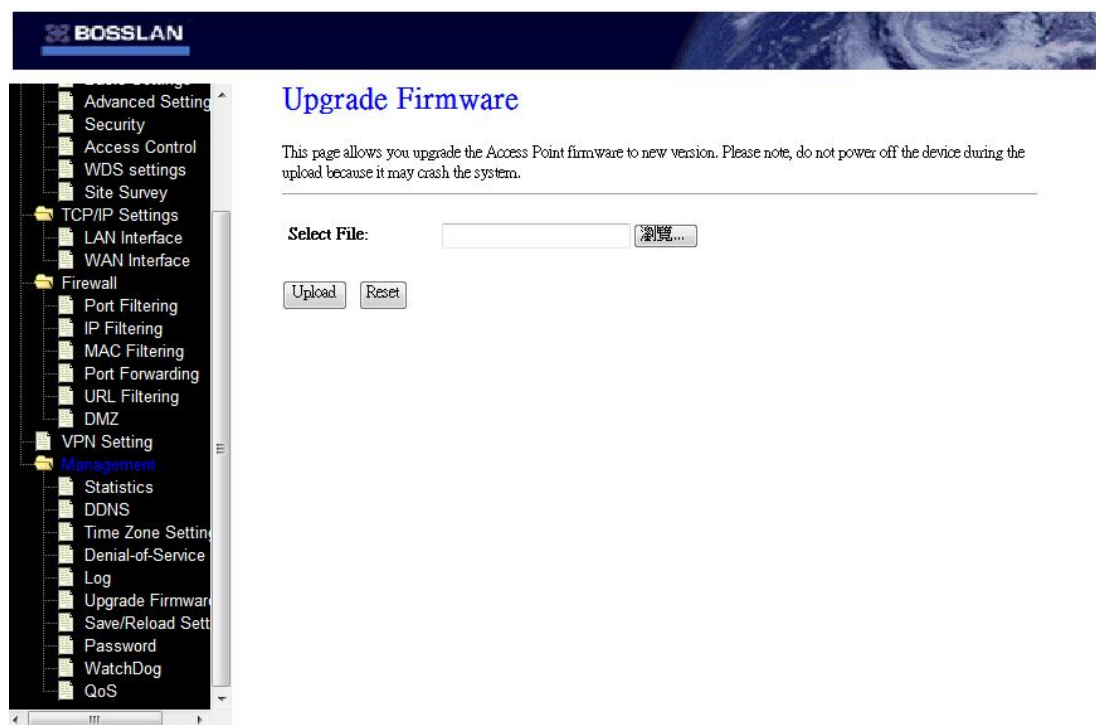
Screen snapshot – Management – Log

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

### 2.3.24 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.





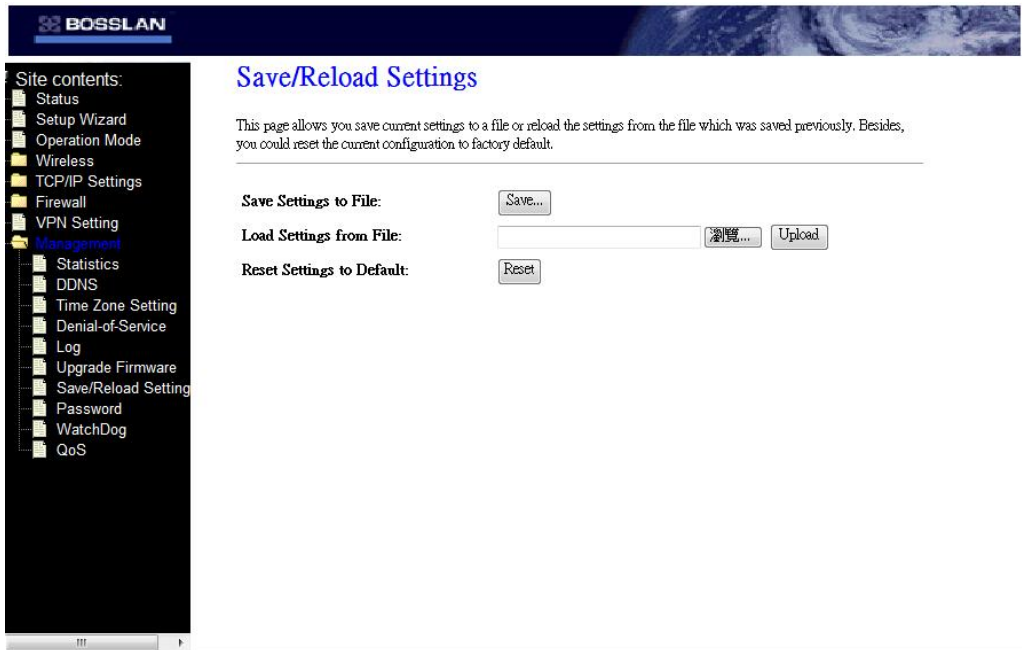
Screen snapshot – Management - Upgrade Firmware

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

### 2.3.25 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.





Screen snapshot – Management - Save/Reload Settings

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 device.
Reset Settings to Default	Click the <b>Reset</b> button to reset the configuration parameter to factory defaults.

2.3.26 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.

Screen snapshot – Management - Password Setup

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.

### 2.3.27 Management-WatchDog

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

**BOSSLAN**

**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)

Screen snapshot – Management – WatchDog Setting

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.

### 2.3.28 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.

**BOSSLAN**

**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

**Bandwidth Control**

IP Address Range:  -

Guarantee Bandwidth: Download  KB/s Upload  KB/s

Priority:

**Current Bandwidth Control Table:**

From IP Addr	To IP Addr	Downstream (KB/s)	Upstream (KB/s)	Priority	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

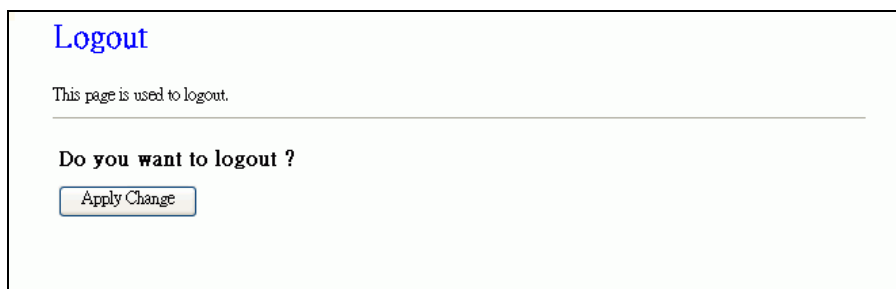
Screen snapshot – Management – Quality of Service

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.
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.
Priority	Click to pick <b>High</b> , <b>Medium</b> or <b>Low</b>
Apply Changes	Click the <b>Apply Changes</b> button to complete the new configuration setting. It is added into <b>Current Bandwidth Control Table</b> .
Reset	Click the <b>Reset</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>Reset</b> button to abort change and recover the previous configuration setting.

### 2.3.29 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.



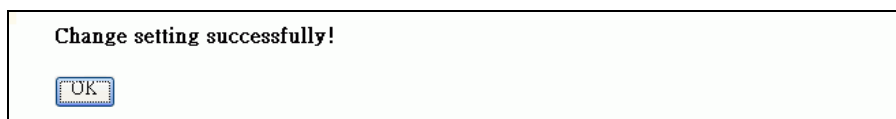
Logout

This page is used to logout.

---

Do you want to logout ?

Screen snapshot – Logout



Change setting successfully!

Screen snapshot – Logout - OK

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

### 3 Frequently Asked Questions (FAQ)

#### 3.1 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, 192.168.1.254 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.

#### 3.2 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.

#### 3.3 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.

#### 3.4 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).

#### 3.5 What is BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just

SSID. Serves as a network ID or name.

### 3.6 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.

### 3.7 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.

### 3.8 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.

### 3.9 What is WEP?

An optional IEEE 802.11 function 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.

### 3.10 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.

### **3.11 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.

### **3.12 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).

### **3.13 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.

### **3.14 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.



### 3.15 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.

### 3.16 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.

### 3.17 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.

### 3.18 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.

### 3.19 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.

### 3.20 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.

### 3.21 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.

### **3.22 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.

### **3.23 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.

### **3.24 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 device, so have the cloned MAC address set on the WLAN device will solve the issue.

### **3.25 What is DDNS?**

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

### **3.26 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.

### **3.27 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.

### **3.28 What is IPSEC?**

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

## 4 Troubleshooting – Q & A

### 4.1 I am trying to log on the AP's Web configuration page, but I do not see the login screen.

**Answer:**

1. Please make sure the IP address that you input on address field of IE browser is correct.
2. Make sure the physical layer connection is established. If you are using wired to connect this AP, check the relevant LAN LED whether is list or not.
3. On Dos Prompt screen, using "ping" command to probe this AP, check if you got reply from it.
4. Command: ping < Destination IP address>

### 4.2 I forgot my password, how to log on this AP for configuration?

**Answer:**

1. Reset the AP to factory default by pressing the Reset button for 5 seconds then releasing it.
2. After release the Reset button, the AP will get back all setting to factory default and reboot system.

### 4.3 How to set the AP to factory default setting?

**Answer:**

1. Open the Enclosure.
2. Reset the AP to factory default by pressing the Reset button for 10 seconds then releasing it.
3. After release the Reset button, the AP will get back all setting to factory default and reboot system.

### 4.4 My AP will not turn on.

**Answer:**

1. Usually it is caused by the power is not connected.
2. Please double check the power adapter if it connected to your AP and the other side is plugged into the power outlet. If it still has no power, please contact your reseller.

### 4.5 I can't access the AP from a wireless client.

**Answer:**

Generally to make the wireless client unable to access AP with following possible issues:

1. Settings are not the same among each wireless adapter.
2. Out of range.
3. IP Address is not set correctly.

**Resolution:**

Make sure that the mode, SSID, Channel and encryption settings are set the same on each wireless adapter. Make sure that your computer is within range and free from any electrical devices that may cause interference.