User Guide

AIP-W512

802.11n Packet Travel Router



FCC STATEMENT

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

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1) This device may not cause harmful interference.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

(())

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Reframing of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

CONTENTS

Package Co	ontents	1
Chapter 1.	Introduction	2
1.1	Overview	2
1.2	Main Features	3
1.3	Product Overview	4
	1.3.1 LED definitions	4
	1.3.2 Router outlook	4
Chapter 2.	Connecting the router	6
2.1	System Requirement	6
2.2	Installation Environment Requirements	6
2.3	Connecting the router	6
Chapter 3.	Quick Installation Guide	B
3.1	TCP/IP Configuration	8
3.2	Quick Installation Guide1	0
Chapter 4.	Configuring the router1	6
4.1	Login1	ô
4.2	Status1	6
4.3	Quick Setup1	7
4.4	WPS1	7
4.5	TCP/IP Settings1	9
	4.5.1 LAN1	9
	4.5.2 WAN Interface2	1
4.6	Wireless	9
	4.6.1 Basic Settings	9
	4.6.2 Advanced Settings	1
	4.6.3 Security	2
	4.6.4 Access Control	6
	4.6.5 WDS Settings	7
	4.6.6 Site Survey	8
	4.6.7 WPS	9

		4.6.8	Schedule	39
4	.7	Firewal	ΙΙ	40
		4.7.1	Port Filtering	40
		4.7.2	IP Filtering	41
		4.7.3	MAC Filtering	41
		4.7.4	Port Forwarding	42
		4.7.5	URL Filtering	43
		4.7.6	DMZ	43
		4.7.7	VLAN	44
4	.8	QoS		45
4	.9	Route	Setup	46
4	.10	Manag	ement	47
		4.10.1	Status	47
		4.10.2	Statistics	48
		4.10.3	DDNS	48
		4.10.4	Time Zone Setting	50
		4.10.5	Denial-of-Service (DoS)	51
		4.10.6	Log	52
		4.10.7	Upgrade Firmware	53
		4.10.8	Save/Reload Setting	54
		4.10.9	Password	54
Append Append	ix A: ix B:	: FAQ : Config	guring the PC	55
Append		: Speci	incations	
Append		. 01033	у	

Package Contents

The following items should be found in your package:

- ➢ AIP-W512
- USB power adapter x 1
- Quick Installation Guide x 1
- ► RJ-45 Ethernet cable x1

P Note:

If any of the listed items are damaged or missing, please contact your distributor.

Chapter 1. Introduction

Thank you for choosing the AIP-W512.

1.1 Overview

The AIP-W512 delivers exceptional range and speed, which can fully meet the need of residential / home Internet access and users that demand mobile network access.

Incredible Speed

The AIP-W512 provides up to 150M wireless connection with other 802.11n wireless clients. The speed makes it ideal for handling multiple data streams at the same time ensuring your network stability. It is compatible with all IEEE 802.11g and IEEE 802.11b products.

Multiple Security Protections

The multiple protection measures include SSID broadcast control and wireless LAN 64/128-bit WEP encryption, Wi-Fi protected Access (WPA2- PSK, WPA- PSK), as well as advanced firewall protections.

Flexible Access Control

AIP-W512 provides IP/MAC address control, URL, communication port filtering for parents and network administrators to apply network restriction for children or staff members. The network administrators can manage and monitor the network in real time with the remote management function.

Product Installation

AIP-W512 is compatible with all the major operating systems, it is easy to manage and operate. With built-in wizard, Internet access or WLAN connections can be established in minutes.

More setup information can be referred in quick installation guide, and detailed step by step instructions are documented in this user guide. Before installing the router, please look through the user guide to know all the router's functions.

1.2 Main Features

- > IEEE 802.11n wireless technology to provide a wireless data rate of up to 150Mbps.
- One 10/100M auto-negotiation RJ45 WAN port, one 10/100M Auto-Negotiation RJ45 LAN port, supporting auto MDI/MDIX.
- > Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting dynamic IP/Static IP/PPPoE Internet access.
- > Supports port forwarding, and DMZ host.
- Supports UPnP, dynamic DNS (DDNS), static routing, dynamic routing (RIPv1, RIPv2).
- Up/downstream QoS with limit control, plus guaranteed bandwidth mode for IP/MAC addresses, providing smooth network experience.
- > Built-in NAT and DHCP server supporting static IP address distribution.
- > Supports stateful packet inspection (SPI).
- > Supports IPSec / PPTP / L2TP VPN pass-through.
- > Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports IPv6 pass-through
- > Supports firmware upgrade and web management.
- > Powered by micro-USB interface.

1.3 Product Overview

1.3.1 LED definitions

The router's LEDs and the WPS Button are located on the side panel.

Name	Status	Indication
PWR	Off	Power is off.
(Blue)	On	Power is on.
WLAN	Off	The Wireless function is disabled or not active
(Blue)	Flashing	The Wireless active
LAN,	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port but
		there is no activity.
(Orange)	Flaching	Data is being transmitted or received via the
	riasning	corresponding port.
	Off	There is no device linked to the corresponding port.
ΜΑΝ	0n	There is a device linked to the corresponding port but
(Orange)	01	there is no activity.
(Orange)	Flashing	Data is being transmitted or received via the
	riashing	corresponding port.

Table 1-1 LEDs Description

1.3.2 Router outlook



Figure 1-2 AIP-W512 outlook

Connectivity interfaces are shown below:



- > **WAN:** The WAN port is where you will connect the xDSL/cable modem.
- **LAN:** One LAN 10/100Mbps RJ45 port connects to a network device, such as a switch.
- **WPS:** Press for 5 seconds to activate WPS (Wi-Fi Protected Setup) configuration

REST button is located in the bottom of router, position is shown below:



Chapter 2. Connecting the router

2.1 System Requirement

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the router is connected directly to the Ethernet.)
- > PCs with a working Ethernet adapter and an Ethernet cable with RJ45 connectors
- > PCs with a working wireless adapter, which should be complied to IEEE802.11 b/g/n standards.
- > TCP/IP protocol on each PC
- > Web browser, such as Microsoft Internet Explorer.

2.2 Installation Environment Requirements

- > Place the router in a well-ventilated place away from any heater or heating vent
- > Avoid direct irradiation of any strong light (such as sunlight)
- > Keep at least 2 inches (5 cm) of clear space around the router
- > Operating Temperature: -20°C ~60°C
- > Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the router

Before installing the router, make sure your PC is connected to the Internet through the broadband service successfully. If there is any problem, please contact your ISP. Install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

- 1. Turn the power off for your PC, Cable/DSL Modem, and the router.
- 2. Locate an optimum location for the router. The best place is usually at the center of your wireless network environment.
- 3. Adjust the direction of the antenna. Normally, upright is a good direction.
- Connect the PC(s) and each Switch/Hub in your LAN to the LAN Ports on the router, shown in Figure 2-1. (If you have the wireless NIC and want to use the wireless function, you can skip this step.)
- 5. Connect the DSL/Cable Modem to the WAN port on the router, shown in Figure 2-1.
- 6. Connect the power adapter to the power socket on the router, and the other end into an electrical outlet. Press the power switch, and then the router will start to work.

7. Turn the power on for your PC and Cable/DSL Modem.



Figure 2-1 Hardware Installation of the AIP-W512

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your AIP-W512 using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address for AIP-W512 is **192.168.11.1**, default subnet mask is 255.255.255.0. These values can be changed to your preference.

Connect the local PC to the LAN port of AIP-W512. You can configure the IP address for your PC with the following options.

- Configure the IP address manually
 - 1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to <u>Appendix B: Configuring the PC</u>.
 - Configure the network parameters. The IP address is 192.168.11.x ("x" represents any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.11.1 (The router's default IP address).
- > Obtain an IP address automatically
 - Set up the TCP/IP Protocol in "Obtain an IP address automatically" mode on your PC. If you need instructions as to how to do this, please refer to <u>Appendix B: Configuring the</u> <u>PC</u>.
 - 2) The built-in DHCP server will assign an IP address for the PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. The following example is in Windows XP OS.

Open a command prompt, and type *ping 192.168.11.1*, and then press **Enter**.

If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the router has been established well.

```
Administrator: Command Prompt

C: \Users \TEST>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=6ms TTL=64

Reply from 192.168.11.1: bytes=32 time=3ms TTL=64

Reply from 192.168.11.1: bytes=32 time=2ms TTL=64

Reply from 192.168.11.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.11.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 6ms, Average = 3ms
```

Figure 3-1 Success result of Ping command

If the result displayed is similar to the Figure 3-2, it means the connection between your PC and the router has failed.

🛋 Administrator: Command Prompt
C:\Users\TEST>ping 192.168.11.1
Pinging 192.168.11.1 with 32 bytes of data: Request timed out. Request timed out.
Request timed out. Request timed out.
Ping statistics for 192.168.11.1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Figure 3-2 Failure result of Ping command

To check the connection follows these steps:

1. Is the connection between your PC and the router correct?

Solution Note:

LAN LED will be lit when you link the router with your PC's via Ethernet (RJ-45) cable.

2. Is the TCP/IP configuration for your PC correct?

P Note:

The router's default IP address is 192.168.11.1. Your PC's IP address must be configured in the range of 192.168.11.2 ~ 192.168.11.254. Or automatically obtain IP address from router via DHCP service in both parties.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage AIP-W512. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type in the default address http://192.168.11.1 in the address field of the browser.

http://192.168.11.1/home.htm

Figure 3-3 Log in the router

2. After successfully logging in, click the **Setup Wizard** in left control panel to start router configurations.

Setup Wizard	
The setup wizard will guide you to configure access point for first time. Please follow the setup wiz step by step.	ard
Welcome to Setup Wizard.	
The Wizard will guide you the through following steps. Begin by clicking on Next	
 Setup Operation Mode Choose your Time Zone Setup LAN Interface Setup WAN Time Zone Wireless LAN Setting Wireless Security Setting 	
1	lext>>

Figure 3-4 Setup Wizard

3. Click Next, and then Operation Mode page will appear, shown in Figure 3-5.

'ou can setup different	modes to LAN and WLAN interface for NAT and bridging function.
Gateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modern. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
O Bridge:	In this mode, all ethemet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
○ Wireless ISP:	In this mode, all ethemet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethemet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Figure 3-5 WAN Connection Type

The router provides three popular ways **Gateway**, **Bridge** and **Wireless ISP** to connect to the Internet. In most scenarios, it's recommended to select **Gateway** function. If you are sure of what kind of connection type your ISP provides, you can select the connection type and click **Next** to go on configuring.

4. If you are sure of what kind of NTP server your router, you can select the very type and click **Next** to go on configuring as shown in Figure 3-6.

Time Zo	one Setting
You can maintair	n the system time by synchronizing with a public time server over the Internet.
Enable NAutomatic	IP client update cally Adjust Daylight Saving
Time Zone Select :	(GMT+08:00)Taipei
NTP server :	192.5.41.41 - North America 💌
	Cancel < <back next="">></back>

Figure 3-6 Time Zone Setting

5. Confirm the IP address for your router and click **Next** to continue configuration.

IP Address:	192.168.11.1		
Subnet Mask:	255.255.255.0		

Figure 3-7 LAN Interface Setting

- 6. If you select Gateway, the router provides five connection types for Internet access. Make
 - sure the carrier device is securely connected to the WAN interface on the router.
 - a) If the connection type is **PPPoE**, then select it from drop down menu as shown below. Enter the **User Name** and **Password** provided by your ISP, and click **Next**.

WAN Interfa	ce Setup			
This page is used to configu your Access Point. Here yo L2TP by click the item valu	ue the parameters for Intern u may change the access m e of WAN Access type.	et network which co ethod to static IP, DF	nnects to the WA ICP, PPPoE, PP	N port of IP or
WAN Access Type:	DHCP Client Static IP DHCP Client PPPoE PPTP L2TP			
		Cancel	< <back< th=""><th>Next>></th></back<>	Next>>

Figure 3-8 WAN connection type menu

User Name/Password - Enter the User Name and Password provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

WAN Interfa	ce 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, PPTP or L2TP by click the item value of WAN Access type.					
WAN Access Type:	PPPoE	•			
User Name:]		
Password:					
			Cancel	< <back< td=""><td>Next>></td></back<>	Next>>

b) If selected connection type is **DHCP Client**, the next screen will appear as shown in Figure 3-9. You can then proceed with the wireless configuration.

WAN Interfac	e Setup
This page is used to configur Point. Here you may change of WAN Access type.	e the parameters for Internet network which connects to the WAN port of your Access the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value
WAN Access Type:	DHCP Client -
Host Name:	
MTU Size:	1492 (1400-1492 bytes)
Attain DNS Automa Attain DNS Automa Attain Att	tically
C Set DNS Manually	
DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	0000000000
🗆 Enable uPNP	
Enable IGMP Prox	у
Enable Ping Access	s 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
🗆 Enable IPv6 pass t	hrough on VPN connection
Apply Changes	Reset



c) If selected connection type is **Static IP**, the next screen will appear as shown in Figure 3-10.

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, PPTP or L2TP 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:	1500 (1400-1500 bytes)	
DNS 1:		
DNS 2:		
DNS 3:		
Clone MAC Address:	0000000000	
🗆 Enable uPNP		
 Enable IGMP Prox 	у	
Enable Ping Access on WAN		
Enable Web Server Access on WAN		
 Enable Irsec pass through on VPN connection Fnable PPTP pass through on VPN connection 		
 Enable I 2TP rass through on VPN connection 		
Enable IPv6 pass through on VPN connection		
-		
Apply Changes	Reset	

Figure 3-10 Static IP

- IP Address This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- Subnet Mask The Subnet Mask is used for the WAN IP address, usually 255.255.255.0.
- > **Default Gateway -** Enter the gateway IP address into the box if required.
- > **Primary DNS -** Enter the DNS Server IP address into the box if required.
- 7. Click **Next** to continue, the Wireless settings page will appear as shown in Figure 3-11.

Wireless	Rasic Settings	
WILCIESS Dasic Settings		
This page is used to Access Point, Here y	configure the parameters for wireless LAN clients which may connect to your you may change wireless encryption settings as well as wireless network param	eters.
🛛 🗆 Disable Wi	reless LAN Interface	
Band:	2.4 GHz (B+G+N)	
Mode:	AP Multiple AP	
Network Type:	Infrastructure 💌	
SSID:	11n AP Add to Profile	9
Channel Width:	40MHz 💌	
Control Sideband:	Upper 💌	
Channel Number:	11 💌	
Broadcast SSID:	Enabled 💌	
WMM:	Enabled v	
Data Rate:	Auto 💌	
Associated Clients:	Show Active Clients	
🔲 Enable Ma	c Clone (Single Ethernet Client)	
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)		
SSID of Extend	ed Add to Broff	
Interface:	Add to Profile	
Apply Chang	ges Reset	

Figure 3-11 Wireless

- Band: Keep the default setting: 2.4GHz (B+G+N). If you just want to use a specific protocol, please use the drop down menu to select it.
- > Mode: This field determines the wireless mode which the AIP-W512 works on.
- Network Type: Keep the default setting: Infrastructure. If you just want to use another operation mode, please use the drop down menu to select it.
- SSID: Create a unique and easy way to remember the name of your wireless network. You can also keep default settings without the device being affected.
- Channel Width Select any channel width from the pull-down list. The default setting is automatic therefore it can adjust the channel width for your clients automatically.

- Channel Number- This field determines which operating frequency will be used. The default channel is set to Auto allowing the AIP-W512 to choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- 8. Set your security preference then click the **Finished** button.

Wireless Security: Recommend to choose **WPA-PSK/WPA2-PSK** and enter a Security Key using ASCII characters between 8 and 63 characters or 64 hexadecimal characters in the **PSK Password** filed. For advanced settings, please refer to <u>Section 4.6: "Wireless".</u>

- > WPA-PSK/WPA2-PSK Select WPA based on pre-shared passphrase.
 - **PSK Password** You can enter **ASCII** or **Hexadecimal** characters.

For **ASCII**, the key can be made up of any numbers from 0 to 9 and any letters from A to Z, the length should be between 8 and 63 characters.

For **Hexadecimal**, the key can be made up of any numbers 0 to 9 and letters A to F, the length should be between 8 and 64 characters.

Please note the key is case sensitive, therefore the upper and lower case keys will affect the outcome. It is highly recommended to write down the key and all related wireless security settings.

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.		
Select SSID: Root AP - 11n AP	Apply Changes Reset	
Encryption:	Disable 💌	
802.1x Authentication:		

Figure 3-12 WLAN Security configurations

Chapter 4. Configuring the router

This chapter will show each Web page's key functions and configuration.

4.1 Login

After successfully logging in, you will see the seven main menus on the left hand-side of the Web-based utility. On the right, there are corresponding explanations and instructions.



Figure 4-1 the main menu

The detailed explanations for each Web page's key function are listed below.

4.2 Status

The Status page provides the current status information about the router. All information is read-only.

This page shows the current	status and some basic settings of the device.
System	
Uptime	Oday:2h:Om:49s
Firmware Version	v3.2.2.2.2
Build Time	Mon Jun 10 04:32:25 EDT 2013
Wireless Configuration	1
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	AIP-W512
Channel Number	11
Encryption	Disabled
BSSID	00:c0:ca:6f:9c:48
Associated Clients	2
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.11.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.11.1
DHCP Server	Enabled
MAC Address	00:c0:ca:6f:9c:46
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:c0:ca:6f:9c:47

Figure 4-2 router Status

4.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide".

4.4 WPS

This section will help guide you into adding a new wireless device to an existing network quickly with the **WPS (Wi-Fi Protect Setup)** function.

a) Choose **WPS** from the **Security** menu in the next screen (shown in Figure 4-3).

Wi-Fi Protected Setup					
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.					
Disable WPS Apply Changes Re	Disable WPS Apply Changes Reset				
WPS Status:	🖲 Co	nfigured	UnConfigured		
		Reset to	UnConfigured		
Auto-lock-down state: unlocke	d Unio	ock			
Self-PIN Number:	687951	46			
Push Button Configuration: Start PBC					
STOP WSC	Sto	p WSC			
Client PIN Number:			Start PIN		
Current Key Info:					
Authentication Enc.	ryption	Кеу			
Open Non	9	N/A			

Figure 4-3 WPS

- > WPS Status Configure or Un-configured the WPS function here.
- > Self-PIN Number The current value of the router's PIN is displayed here.
- Push Button Configuration Push this button to synchronize the router and your Wi-Fi adapter
- > Client PIN Number To synchronize the Wi-Fi adapter by entering adapter's PIN.
- b) To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between the wireless adapter and router using either Push Button Configuration (PBC) method or PIN method.

P Note:

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function.

Configuring a new device (ex. AWUS036NHR), please follow the steps below.

Step 1: Press **PBC** button from the Wireless LAN Utility then the **Wi-Fi Protected Setup – PBC method** will pop up and wait for an authentication.

REALTEK 11n USB Wireless LAN Utility		Wi-Fi Protected Setup - PBC method
Refresh(<u>R)</u> Mode(<u>M</u>) Abou	t(<u>A</u>)	Wi-Ei Protected Setup - PBC method
MyComputer	General Profile Available Network Status Statistics Wi-Fi Protect Setup	WH I Flotected Setup - FDC memor
	Wi-Fi Protected Setup (WPS)	If there is more than one AP on the PBC mode, there will be [Session
	An easy and secure setup solution for Wi-Fi network	Overlap J. Please use PIN method or wait for a while and use PBC method again.
	Pin Input Config (PIN)	Status : Initial WPS
	After pushing the PIN button.Please enter the PIN code into yo	
	PIN Code: 274362	Complete :
	Pin Input Config (PIN)	
	Push Button	Push Button Config (PBC)
	After pushing the PBC button.Please push the physical button o	
	or visual button on the WPS config page.	
	Push Button Config (PBC)	

Step 2: Press Start PBC button on your router for authentication.

Start PBC successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

OK

Step 3: Wait for a minute then you'll discover your AWUS036NHR is connected to AIP-W512 automatically.

REALTER 116 USB W	ireless LAN Utility	
Refreeh(E) Mode(M) Abou	#(<u>B)</u>	
Realter RTLB101	Benetal Pholie Available Network. Status Statistics WiFi Protect Setup	
	Status: Associated	
	Speeck Tx:150 Mbps Rx:150 Mbps	
	Type: Infrastructure	
	Encryption: None	
	SSID: AIP-W525	
	Signal Strength: 98%	
	Link Quality: 000000000000000000000000000000000000	
	Tx Power = 100 % 100 % Apply	
	1 % 100 %	
	Network Address:	
	MVC Address: OD:C0:CA-52:CD:58	
	IP Address: 0.0.0.0	
	Subnet Mask: 0.0.0.0	
	Gabewayt	
	ReNew IP	
El Show Tray Iron	Ficable Adaptor	-
Radio Off	Windows Zero Config	Close

4.5 TCP/IP Settings



Figure 4-5 The Network Menu

There are two submenus under the TCP/IP Settings menu (shown in Figure 4-5): **LAN Interface**, and **WAN** Interface. Click any of them, and you will be able to configure the corresponding function.

4.5.1 LAN

Choose menu "**TCP/IP Settings** \rightarrow **LAN**", to configure the IP parameters of the LAN on the screen as shown below.

LAN Interface Setup		
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc		
IP Address:	192.168.11.1	
Subnet Mask:	255.255.255.0	
Default Gateway:	0.0.0.0	
DHCP:	Server -	
DHCP Client Range:	192.168.11.100 - 192.168.11.200 Show Client	
DHCP Lease Time:	480 (1 ~ 10080 minutes)	
Static DHCP:	Set Static DHCP	
Domain Name:	Alfasetup	
802.1d Spanning Tree:	Disabled -	
Clone MAC Address:	0000000000	
Apply Changes	Reset	

Figure 4-6 LAN Interface

- IP Address Enter the IP address of your router or reset it in dotted-decimal notation (factory default: 192.168.11.1).
- Subnet Mask An address code that determines the size of the network. Normally used, 255.255.255.0 as the subnet mask.

Note:

- 1. If you change the IP Address of LAN, you must use the new IP Address to log into the router.
- 2. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP

server will change accordingly at the same time, while the Virtual Server and DMZ Host will not take effect until they have been re-configured.

- Default Gateway Enter the gateway IP address in dotted-decimal notation provided by your system administrator.
- > **DHCP** Select Disabled, Client or Server in different operation mode for AIP-W512
- 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 automatically.
- Show Client Press open to active the DHCP Client Table window that shows the active clients with their assigned IP address, MAC address and time expired information. [Server mode only]
- > **DHCP Lease Time** Amount of time the IP address is leased for.
- Set Static DHCP Manual setup Static DHCP IP address for specific MAC address. [Server mode only]
- > **Domain Name -** Assign Domain Name and dispatch to DHCP clients [optional]
- 802.1d Spanning Tree Enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
- > Clone MAC Address Fill in the MAC address for the MAC address to be cloned.

4.5.2 WAN Interface

Choose menu "**TCP/IP Settings** \rightarrow **WAN**", you can configure the IP parameters of the WAN on the screen shown below.

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, PPTP or L2TP by click the item value of WAN Access type. WAN Access Type: DHCP Client Host Name: MTU Size: 1492 (1400-1492 bytes) Clone MAC 00000000000 Address: Enable uPNP Enable IGMP Proxy Enable IGMP Proxy Enable Ping Access on WAN Enable Ping Access on WAN Enable Pring Access on WAN Enable IPsec pass through on VPN connection Enable IP pass through on VPN connection Enable L2TP pass through on VPN connection Enable IPv6 pass through on VPN connection	WAN Interface Setup		
WAN Access Type: DHCP Client Host Name: Host Name: Host Name: Hight Light Lig	This page is used to Access Point. Here item value of WAN.	configure the parameters for Internet network which connects to the WAN port of your you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the Access type.	
Host Name:	WAN Access Type:	DHCP Client	
MTU Size: 1492 (1400-1492 bytes) Clone MAC 00000000000 Address: 000000000000 Enable uPNP Fable IGMP Proxy Enable IGMP Proxy Enable Ping Access on WAN Enable Web Server Access on WAN Fable IPsec pass through on VPN connection Ø Enable IPTP pass through on VPN connection Ø Enable L2TP pass through on VPN connection Ø Enable IPv6 pass through on VPN connection Ø Enable IPv6 pass through on VPN connection Ø Attain DNS Automatically Set DNS Manually DNS 1: DNS 2: DNS 3: Image: Set Discourse of the set of	Host Name:		
Clone MAC 00000000000 Address: • Enable uPNP • ✓ Enable IGMP Proxy • ■ Enable Ping Access on WAN • ● Enable IPsec pass through on VPN connection • ✓ Enable L2TP pass through on VPN connection • ✓ Enable L2TP pass through on VPN connection • ✓ Enable IPv6 pass through on VPN connection • ✓ Attain DNS Automatically • ● Set DNS Manually DNS 1: DNS 2: • DNS 3: •	MTU Size:	1492 (1400-1492 bytes)	
 Enable uPNP Enable IGMP Proxy 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 Enable IPv6 pass through on VPN connection Apply Changes Reset Attain DNS Automatically Set DNS Manually DNS 1: DNS 2: DNS 3: 	Clone MAC Address:	0000000000	
Image: Second state of the second s	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 ✓ Enable IPv6 pass through on VPN connection ✓ Attain DNS Automatically ● Attain DNS Automatically DNS 1: DNS 2: DNS 3:	Enable IGMP P	roxy	
Enable Web Server Access on WAN ✓ Enable IPsec pass through on VPN connection ✓ Enable L2TP pass through on VPN connection Enable IPv6 pass through on VPN connection Apply Changes Reset • Attain DNS Automatically • Set DNS Manually DNS 1: DNS 2: DNS 3:	Enable Ping Ac	cess on WAN	
Imable IPsec pass through on VPN connection Imable PPTP pass through on VPN connection Imable I2TP pass through on VPN connection Imable IPv6 pass through on VPN connection Apply Changes Reset Imable Attain DNS Automatically Imable Set DNS Manually DNS 1: DNS 2: DNS 3:	Enable Web Ser	rver Access on WAN	
Apply Changes Reset Attain DNS Automatically Set DNS Manually DNS 1: DNS 2: DNS 3:	Enable IPsec pa	ss through on VPN connection	
Enable I2 11 pass through on VPN connection Apply Changes Reset Attain DNS Automatically Set DNS Manually DNS 1: DNS 2: DNS 3:	Enable L 2TP pa	iss through on VPN connection	
Apply Changes Reset Attain DNS Automatically Set DNS Manually DNS 1: DNS 2: DNS 3: 	Finable IPv6 nas	s through on VPN connection	
Apply Changes Reset • Attain DNS Automatically • Set DNS Manually DNS 1: DNS 2: DNS 3: • • • • • • • • • • • • • • •			
Attain DNS Automatically Set DNS Manually DNS 1: DNS 2: DNS 3:	Apply Changes	Reset	
Set DNS Manually DNS 1: DNS 2: DNS 3:	Attain DNS Auto	omatically	
DNS 1: DNS 2: DNS 3:	© Set DNS Manua	Цу	
DNS 2: DNS 3:	DNS 1:		
DNS 3:	DNS 2:		
	DNS 3:		

Figure 4-7 WAN – Static IP

- > Clone MAC Address Fill in the MAC address for the MAC address to be cloned
- > Enable uPNP Click the checkbox to enable uPNP function.
- > Enable IGMP Proxy Click the checkbox to enable IGMP proxy
- > Enable Ping Access on WAN Click the checkbox to enable WAN IGMP response.
- > Enable Web server Access on WAN Click the checkbox to enable web configuration from
- 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

- 1. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear, shown in Figure 4-7.
 - > IP Address Enter the IP address in dotted-decimal notation provided by your ISP.
 - Subnet Mask Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually 255.255.255.0.
 - Default Gateway (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
 - MTU Size The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
 - DNS 1 / DNS 2 / DNS 3 (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

Click the Apply Changes button to save your settings.

2. If your ISP provides the DHCP service, please choose **DHCP Client** type, and the router will automatically get IP parameters from your ISP (shown in Figure 4-8).

WAN Interface Setup			
This page is used Access Point. He item value of WA	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, PPTP or L2TP by click the item value of WAN Access type.		
WAN Access Ty	pe: DHCP Client 💌		
Host Name:			
MTU Size:	1492 (1400-1492 bytes)		
Clone MAC Address:	0000000000		
Enable uPNF			
Enable IGME	Proxy		
Enable Ping	Access on WAN		
Enable Web	Server Access on WAN		
Enable IPsec	pass through on VPN connection		
Fnable L2TF	pass through on VPN connection		
Enable IPv6	Enable ID: 6 pass through on VPN connection		
Apply Changes) Reset		
Attain DNS A	utomatically		
© Set DNS Man	ually		
DNS 1:			
DNS 2:			
DNS 3:			

Figure 4-8 WAN – Dynamic IP

- > Host Name Enter the host name provided by your ISP, default value is blank.
- MTU Size The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
- > Attain DNS Automatically Receives DNS address automatically from the ISP.

Set DNS Manually - If your ISP gives you one or two DNS addresses, select Set DNS Manually and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

P Note:

If you find an error message on the website after entering the DNS addresses, it is likely that your DNS server has been set up improperly. You should contact your ISP to get DNS server addresses.

3. If your ISP provides a PPPoE connection, select **PPPoE** option and enter the following parameters (Figure 4-9):

WAN Interfa	ce Setup	
This page is used to config Point. Here you may chang of WAN Access type.	ure the parameters for Internet network which connects to the WAN port of your Access e the access method to static IP, DHCP, PPPoE, PPIP or L2TP by click the item value	
WAN Access Type:	PPPoE 💌	
User Name:		
Password:		
Service Name(AC):		
Connection Type:	Continuous Connect Disconnect	
Idle Time:	5 (1-1000 minutes)	
MTU Size:	1452 (1360-1492 bytes)	
• Attain DNS Auton	natically	
C Set DNS Manually		
DNS 1:		
DNS 2:		
DNS 3:		
Clone MAC Address:	0000000000	
🗆 Enable uPNP		
Enable IGMP Proxy		
Enable Ping Access on WAN		
Enable Web Server Access on WAN		
 Enable IPsec pass through on VPN connection Enable DDTD pass through on VDN connection 		
 Enable L2TP pass through on VPN connection 		
□ Enable IPv6 pass through on VPN connection		
Apply Changes	Reset	

Figure 4-9 WAN setting - PPPoE

- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Service Name The service name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank.
- Connection Type
 - Continuous Continuous connection type means to setup the connection through PPPoE protocol whenever this WLAN Broadband router is powered on.

- Connect on Demand In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again.
- Manual You can click the Connect/Disconnect button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

• 🖙 Note:

Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

- Idle Time If you want your Internet connection to be active constantly, please enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- MTU Size The default MTU size is "1452" bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
- > Attain DNS Automatically Receives DNS address automatically from the ISP.
- Set DNS Manually If your ISP gives you one or two DNS address, select Set DNS Manually and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

P Note:

If you find an error on the website after entering the DNS addresses, it is likely that your DNS server has been set up improperly. You should contact your ISP to get DNS server addresses.

Click the **Apply Changes** button to save your settings.

4. If your ISP provides PPTP connection, please select **PPTP** option and enter the following parameters (Figure 4-11):

WAN Interface Setup		
This page is used to configure the para Point. Here you may change the access WAN Access type.	meters for Internet network which connects to the WAN port of your Access s method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of	
WAN Access Type:	•	
Clone MAC Address: 00000000000		
Enable uPNP		
Enable IGMP Proxy		
Enable Ping Access on WAN		
Enable Web Server Access on V	WAN	
Enable IPsec pass through on V	/PN connection	
Enable PPTP pass through on Finable I 2TP pass through on 1	VPN connection	
Enable IPv6 pass through on V	PN connection	
Apply Changes Reset		
Attain DNS Automatically		
© Set DNS Manually		
DNS 1:		
DNS 2:		
DNS 3:		
Oynamic IP (DHCP)		
© Static IP		
IP Address: 172.1.1.2		
Subnet Mask: 255.255.255.0		
Default Gateway: 0.0.0.0		
Address(Or 172.1.1.1		
Domain Name):		
User Name:		
Password:		
Connection Type:	 Connect 	
Disconnect		
Idle Time: 5	(1-1000 minutes)	
MTU Size: 1460	(1400-1460 bytes)	
Compression	Compression	

Figure 4-11 L2TP Settings

- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Dynamic IP/ Static IP Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

If you choose static IP, enter the domain name and enter the DNS assigned by your ISP. Click the **Save** button.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

- Connection Type
 - Connect on Demand You can configure the router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet

connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Continuous -** Connect automatically after the router is disconnected. To use this option, check the radio button.
- Connect Manually You can configure the router to connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from your Internet connection. You will not be able to re-establish your connection automatically when attempting to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications are visiting the Internet continually in the background.

MTU Size - The default MTU size is "1460" bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.

Click the **Save** button to save your settings.

5. If your ISP provides L2TP connection, please select **L2TP** option. Enter the following parameters (Figure 4-12):

I his page is used to	o configure the parameters for Internet network which connects to the WAN port of your Access
Point. Here you ma NAN Access type	ay change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of
, in the case type	~
WAN Access	L2TP 💌
Lype: Clone MAC	
Address:	0000000000
Enable uPNF	
Enable IGME	P Proxy
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 L21P	pass through on VPN connection
Enable IFvo	pass through on vriv connection
Apply Changes	Reset
Attain DNS A	Automatically
C Set DNS Mar	nually
D 2101 1	
DNS I:	
DNS 1: DNS 2:	
DNS 1: DNS 2: DNS 3:	
DNS 1: DNS 2: DNS 3: Oynamic IP ()	DHCP)
DNS 1: DNS 2: DNS 3: Dynamic IP () Static IP	DHCP)
DNS 1: DNS 2: DNS 3: Oynamic IP () Static IP IP Address:	DHCP)
DNS 1: DNS 2: DNS 3: DNS 3: Static IP () Static IP IP Address: Subnet Mask:	DHCP) 172.1.1.2 255.255.255.0
DNS 1: DNS 2: DNS 3: Opynamic IP (1) Static IP IP Address: Subnet Mask: Default Gateway	DHCP) 172.1.1.2 255.255.255.0 : 0.0.0.0
DNS 1: DNS 2: DNS 3: DNS 3: Static IP IP Address: Subnet Mask: Default Gateway Server IP	DHCP) 172.1.1.2 255.255.255.0 : 0.0.0
DNS 1: DNS 2: DNS 3: DNS 3: Static IP IP Address: Subnet Mask: Default Gateway Server IP Address(Or Domain Name):	DHCP) 172.1.1.2 255.255.255.0 : 0.0.0 172.1.1.1
DNS 1: DNS 2: DNS 3: DNS 3: Dramic IP (1) Address: Subnet Mask: Default Gateway Server IP Address(Or Domain Name): User Name:	DHCP) 172.1.1.2 255.255.255.0 : 0.0.0 172.1.1.1
DNS 1: DNS 2: DNS 3: DNS 3: Dynamic IP (1) Static IP IP Address: Subnet Mask: Default Gateway Server IP Address(Or Domain Name): User Name: Password:	DHCP) 172.1.1.2 255.255.255.0 172.1.1.1 172.1.1.1
DNS 1: DNS 2: DNS 3: DNS 3: DS tatic IP IP Address: Subnet Mask: Default Gateway Server IP Address(Or Domain Name): User Name: Password:	DHCP) 172.1.1.2 255.255.255.0 : 0.0.0 172.1.1.1 Continuous Continuous Continuous Continuous
DNS 1: DNS 2: DNS 3: DNS 3: DS tatic IP IP Address: Subnet Mask: Default Gateway Server IP Address(Or Domain Name): User Name: Password: Connection Type	DHCP) 172.1.1.2 255.255.255.0 : 0.0.0 172.1.1.1 Continuous Connect Disconnect
DNS 1: DNS 2: DNS 3: DNS 3: DNS 3: Default Green Default Gateway Server IP Address(Or Domain Name): User Name: Password: Connection Type Idle Time:	DHCP) 172.1.1.2 255.255.255.0 : 0.0.0 172.1.1.1 Continuous Connect Disconnect 5 (1-1000 minutes)
DNS 1: DNS 2: DNS 3: DNS 3: DNS 3: DS tatic IP IP Address: Subnet Mask: Default Gateway Server IP Address(Or Domain Name): User Name: Password: Connection Type Idle Time: MTU Size:	DHCP) 172.1.1.2 255.255.255.0 172.1.1.1 Continuous Continuous Disconnect 5 (1-1000 minutes) 1460 (1400-1460 bytes)



- User Name/Password Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Dynamic IP/ Static IP Choose either as you are given by your ISP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.
- Connection Type
 - Connect on Demand You can configure the router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access

the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Continuous -** Connect automatically after the router is disconnected. To use this option, check the radio button.
- Connect Manually You can configure the router to connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically when attempting to access the Internet again. To use this option, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time**, because some applications are visiting the Internet continually in the background.

MTU Size - The default MTU size is "1460" bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.

Click the **Save** button to save your settings.

4.6 Wireless



Figure 4-15 Wireless menu

There are eight submenus under the Wireless menu (shown in Figure 4-15): **Basic Settings**, **Advanced Settings**, **Security, Access Control, WDS Setting, Site Survey, WPS**, and **Schedule.** Click any of them, and you will be able to configure the corresponding function.

4.6.1 Basic Settings

Choose menu "Wireless \rightarrow Basic Settings", you can configure the basic settings for the wireless network on this page.

Wireless Basic Settings
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.
Disable Wireless LAN Interface
Band: 2.4 GHz (B+G+N)
Mode: AP Multiple AP
Network Type:
SSID: 11N_AP Add to Profile
Channel 40MHz •
Control Sideband: Upper -
Channel Number: Auto
Broadcast SSID: Disabled
WMM: Enabled -
Data Rate: Auto
Associated Clients: Show Active Clients
Enable Mac Clone (Single Ethernet Client)
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Interface:
Apply Changes Reset

Figure 4-16 Wireless Settings

- Band Select the desired protocol. The default setting is 2.4GHz (B+G+N).
 2.4GHz (B) Select if all of your wireless clients are 802.11b.
 2.4GHZ (G) Select if all of your wireless clients are 802.11g.
 2.4GHz (N) Select if all of your wireless clients are 802.11n.
 2.4GHz (B+G) Select if you are using both 802.11b and 802.11g wireless clients.
 2.4GHz (G+N) Select if you are using both 802.11g and 802.11n wireless clients.
 2.4GHz (B+G+N) Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.
- Mode Select the desired wireless mode. AIP-W512 offers AP, Client, WDS, and AP + WDS. When 802.11g mode is selected, only 802.11g wireless stations can connect to the router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to 2.4GHz (B+G+N) and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the router.
- Network Type After network mode is selected to "Client" set network type as infrastructure or Ad-Hoc.
- SSID Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.
- Channel width Select the channel width from the pull-down list. The default setting is 40MHz.

P Note:

If **2.4GHz (B)**, **2.4GHz (G)**, or **2.4GHz (B+G)** is selected in the **Mode** field, the **Channel Width** selecting field will disappear and the value will become 20M, which is unable to be changed.

- > Control Sideband Select the sideband with upper or lower for channel width 40MHz.
- Channel Number- This field determines which operating frequency will be used. The default channel is CH11. You can set to Auto where the AP will choose the best channel automatically, it is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Broadcast SSID When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the router. If you select Enable for Broadcast SSID then router will broadcast its name (SSID) on the air.
- > WMM Click on Enable or Disable Wireless Multimedia (WMM).
- Data Rate Select transmission data rate from pull-down menu. Data rate can be auto select, 1M to 54Mbps or MCS. The default option is AUTO.

- Associate Clients Click Show Active Clients 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) Copy your system's NIC MAC address as wireless client's MAC address, this function only works if Client mode is selected.
- Enable Universal Repeater Mode Check to enable Universal Repeater Mode where router acts as AP and client simultaneously in this mode).
- > **SSID for Extended Interface** Assign a SSID when Universal Repeater Mode is enabled.

4.6.2 Advanced Settings

Choose menu "Wireless \rightarrow Security", you can configure the security settings of your wireless network.

Wireless Ad	lvanced Settings
These settings are or settings should not b	ly for more technically advanced users who have a sufficient knowledge about wireless LAN. These be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Preamble Type:	Long Preamble Short Preamble
IAPP:	Enabled
Protection:	© Enabled 💿 Disabled
Aggregation:	Enabled Object Disabled
Short GI:	Enabled Object Disabled
WLAN Partition:	Enabled Object Disabled
20/40MHz Coexist:	© Enabled O Disabled
RF Output Power:	● 100% ○ 70% ○ 50% ○ 35% ○ 15%
Apply Changes	Reset

- Fragmentation Threshold This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance due to excessive packets, 2346 is the recommended default setting.
- RTS Threshold Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- Beacon Interval Enter a value between 20-1000 milliseconds for the Beacon Interval. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.

4.6.3 Security

Choose menu "Wireless \rightarrow Security", you can configure the security settings of your wireless network.

There are four wireless security modes supported by the router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA-Mixed (Pre-Shared Key or Enterprise).

Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent iny unauthorized access to your wireless network.
Select SSID: Root AP - 11n AP Apply Changes Reset
Encryption: Disable
802.1x Authentication:

Figure 4-18 Wireless Security

- Disable If you do not want to use wireless security, check this radio button. It's strongly recommended to choose one of the following modes to enable security.
- WEP It is based on the IEEE 802.11 standard. If you check this radio button, you will find a notice in red as shown in Figure 4-19.

Encryption:	WEP
802.1x Authentication:	
Authentication:	◎ Open System ◎ Shared Key ◎ Auto
Key Length:	64-bit 💌
Key Format:	Hex (10 characters)
Encryption Key:	*****

Figure 4-19

- 802.1x Authentication Check to enable 802.1x authentication via RADIUS server.
- Authentication You can choose the type for the WEP security on the pull-down list. The default setting is Auto, which can select Shared Key or Open System authentication type automatically based on the wireless station's capability and request.
- Key Length You can select the WEP key length (64-bit, or 128-bit) for encryption.

64-bit - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not recommended) or 5 ASCII characters.

128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not recommended) or 13 ASCII characters.

Note:

If you do not set the key, the wireless security function will still be disabled even if you have selected Shared Key as Authentication Type.

- Key Format Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
 ASCII format stands for any combination of keyboard characters in the specified length.
- Encryption Key Select which of the four keys will be used and enter the matching WEP key you have created. Make sure these values are identical on all the wireless stations in your network.
- Radius Server IP Address Enter the IP address of the Radius server, if 802.1x Authentication is selected.
- Radius Server Port Enter the port number of the Radius server, if 802.1x Authentication is selected.
- Radius Server Password Enter the password for the Radius server, if 802.1x Authentication is selected.

Be sure to click the Apply Changes button to save your settings on this page

> WPA - It's the WPA authentication type based on pre-shared passphrase or RADIUS server.

Encryption:	IPA 💌
Authentication	© Enterprise (RADIUS)
Mode:	(Pre-Shared Key)
WPA Cipher Suite:	TKIP AES
Pre- Shared Key Format:	Passphrase
Pre-Shared Key:	



- Authentication Mode You can choose either Enterprise (RADIUS) or Personal (Pre-Shared Key). The default setting is Personal (Pre-Share Key), it's a passphrase between 8 and 63 characters. Enterprise (RADIUS), is an authentication via RADIUS server.
- WPA Cipher Suite When WPA is set as the Authentication Type, you can select TKIP or AES or AUTO if both encryptions are checked.
- Pre-Shared Key Format You can enter chose either Passphrase (8 ~ 63 characters) or HEX(64 Characters).
- **Pre-Shared Key** Enter the matching WEP key you created. Make sure these values are identical on all the wireless stations in your network.
- Radius Server IP Address Enter the IP address of the Radius server, if Enterprise (RADIUS) is selected.
- Radius Server Port Enter the port number of the Radius server, if Enterprise (RADIUS) is selected.

• Radius Server Password - Enter the password for the Radius server, if Enterprise (RADIUS) is selected.

Be sure to click the **Apply Changes** button to save your settings on this page.

> WPA2 - Authentication type based on pre-shared passphrase or RADIUS server.

Encryption:	NPA2 💌
Authentication Mode:	© Enterprise (RADIUS)
WPA2 Cipher Suite:	TKIP 🖉 AES
Pre- Shared Key Forma	t: Passphrase
Pre-Shared Key:	

Figure 4-21

- Authentication Mode You can choose either Enterprise (RADIUS) or Personal (Pre-Shared Key). The default setting is Personal (Pre-Share Key), it's a passphrase between 8 and 63 characters. Enterprise (RADIUS), is an authentication via RADIUS server.
- WPA2 Cipher Suite When WPA2 is set as the Authentication Type, you can select TKIP or AES or AUTO if both encryption is checked..
- Pre-Shared Key Format You can enter either Passphrase (8 ~ 63 characters) or HEX (64 Characters).
- **Pre-Shared Key** Enter the matching WEP key that you've create. Make sure these values are identical on all the wireless stations in your network.
- Radius Server IP Address Enter the IP address of the Radius server, if Enterprise (RADIUS) is selected.
- Radius Server Port Enter the port number of the Radius server, if Enterprise (RADIUS) is selected.
- Radius Server Password Enter the password for the Radius server, if Enterprise (RADIUS) is selected.

Be sure to click the **Apply Changes** button to save your settings on this page.

> WPA-Mixed - Authentication type based on pre-shared passphrase or RADIUS server.

Encryption: V	VPA-Mixed 💌
Authentication Mode:	© Enterprise (RADIUS) Personal (Rep Shared Kari)
WPA Cipher Suite:	TKIP AES
WPA2 Cipher Suite:	TKIP AES
Pre- Shared Key Format	Passphrase
Pre-Shared Key:	

Figure 4-22

- Authentication Mode You can choose either Enterprise (RADIUS) or Personal (Pre-Shared Key). The default setting is Personal (Pre-Share Key), it is a passphrase between 8 and 63 characters. Enterprise (RADIUS) is an authentication via RADIUS server.
- WPA Cipher Suite When WPA is set as the Authentication Type, you can select either TKIP or AES as Encryption.
- WPA2 Cipher Suite When WPA2 is set as the Authentication Type, you can select either TKIP or AES as Encryption.
- Pre-Shared Key Format You can enter either Passphrase (8 ~ 63 characters) or HEX (64 Characters).
- **Pre-Shared Key** Enter the matching WEP key that you have create. Make sure these values are identical on all the wireless stations in your network.
- Radius Server IP Address Enter the IP address of the Radius server, if Enterprise (RADIUS) is selected.
- Radius Server Port Enter the port number of the Radius server, if Enterprise (RADIUS) is selected.
- Radius Server Password Enter the password for the Radius server, if Enterprise (RADIUS) is selected.

Be sure to click the **Apply Changes** button to save your settings on this page.

4.6.4 Access Control

Choose menu "Wireless \rightarrow Access Control", you can control the wireless access by configuring the Wireless Access Control function, shown in Figure 4-23.

Wireless Access	Control					
If you choose 'Allowed Liste to connect to your Access P the Access Point.	ed', only those clients oint. When 'Deny Li	whose wireles sted' is selected	ss MAC addr I, these wirele	resses are in the a ess clients on the	ccess control list list will not be a	t will be able ble to connect
Wireless Access Control N	fode: Allow Lis	ted 💌				
MAC Address:	Comme	nt:				
Apply Changes Res	et					
Current Access Control Li	ist:					
MAC Address	Comment	Select				
00:c0:ca:12:34:58						
00:c0:ca:11:11:11						
Delete Selected Dele	ete All Reset					

Figure 4-23 Wireless Access Control

To allow wireless users by MAC Address, click **Allow Listed**, or prohibited wireless users by MAC Address by click **Deny Listed**. The default setting is **Disable**.

- > MAC Address The wireless station's MAC address that you want to filter.
- **Comment -** A simple description of the wireless station.

Be sure to click the Apply Changes button to save your settings on this page

Current Access Control List - Displays the registered clients that are allowed to link to this WLAN Broadband router.

4.6.5 WDS Settings

Choose menu "Wireless \rightarrow WDS Settings", you can configure the advanced settings of your wireless network.

WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
Data Rate: Auto 🖵
Comment:
Apply Changes Reset Set Security Show Statistics
Current WDS AP List:
MAC Address Tx Rate (Mbps) Comment Select
[Delete Selected] [Delete All] [Reset]

Figure 4-24 Wireless Advanced

To add wireless AP by MAC Address, click Enable WDS.

- > **MAC Address -** The wireless station's MAC address that you want to add.
- Data Rate Select transmission data rate from the drop down menu. Data rate can be auto-selected, 1Mbps to 54Mbps or MCS.
- Set Security There are two wireless security modes supported by the WDS: WEP (Wired Equivalent Privacy), and WPA2 (Wi-Fi Protected Access 2).

WDS Security	Setup	
This page allows you setup the WDS device has adopted the sa	wireless security for WDS. When me encryption algorithm and Key.	enabled, you must make sure each
Encryption:	None 🔻	
WEP Key Format:	ASCII (5 characters) 👻	
WEP Key:		
Pre-Shared Key Format:	Passphrase 👻	
Pre-Shared Key:		
	_	
Apply Changes Re	set	

- Encryption Use drop down menu to configure WDS security, you can select it from None, WEP 64-bits, WEP 128-bits, or WPA2 (AES).
- WEP Key Format Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length. 64-bit You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters. 128-bit You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters. 128-bit You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

- Encryption Key Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your WDS network
- Pre-Shared Key Format You can enter chose either Passphrase (8 ~ 63 characters) or HEX(64 Characters).
- **Pre-Shared Key** Enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your WDS network

Comment - A simple description of the wireless station.

Be sure to click the Apply Changes button to save your settings on this page

Current WDS AP List - Displays the registered APs that are allowed to link to this WLAN Broadband router.

4.6.6 Site Survey

Choose menu "Wireless \rightarrow Site Survey", you scan and connect nearby APs when operate at client mode.

Wireless Site S	urvey					
This page provides tool to s choose to connect it manua	scan the wireless 11y when client m	network. I ode is ena	lf any bled.	Access Point	t or IBS	S is found, you could
Site Survey						_
SSID	BSSID	Channel	Туре	Encrypt	Signal	
ALFA	00:c0:ca:60:c7:6e	6 (B+G+N)	AP	no	46	
HTC Portable Hotspot	7c:61:93:8e:c9:84	1 (B+G)	AP	WPA-PSK	38	
ALFA_free	00:c0:ca:65:aa:02	2 (B+G+N)	AP	WPA2-PSK	30	
Laservideo TP-LINK	b0:48:7a:b5:01:c4	4 (B+G+N)	AP	WPA- PSK/WPA2- PSK	28	

- SSID(to be WDS) The SSID of the AP your router is going to connect to as a client. You can also use the search function to select the SSID to join.
- BSSID(to be WDS) The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- Channel This field displayed operating frequency of the AP your router is going to connect to as a client.
- **Type –** Type of the AP your router is going to connect to as a client, AP or AD-HOC.
- > **Encryption –** Shows encryption type of the AP your router is going to connect to as a client.
- **Signal –** Shows the signal strength of the AP your router is going to connect to as a client.

4.6.7 WPS

Choose menu "Wireless \rightarrow WPS", where you to add a new wireless device to an existing network quickly.

Wi-Fi Protecte	d Setup
This page allows you to ch automically syncronize its	name the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client setting and connect to the Access Point in a minute without any hassle.
Disable WPS	
Apply Changes Re	set
WPS Status:	Configured @UnConfigured [Reset to UnConfigured]
Auto-lock-down state: unlocked	Unlock
Self-PIN Number:	77886156
Push Button Configuration:	[Start PBC]
STOP WSC	Stop WSC
	Stort DIN

- > Self-PIN Number The current value of the router's PIN is displayed here.
- PIN Configuration You will need to enter Self-PIN Number into adapter's configuration utility or on the adapter itself. Press the Start PIN button on the router and on the adapter.

Note: You will have two minutes to push the PIN button on the router and device(s) you want to connect.

Push Button Configuration - You will need an adapter that supports it via a utility or on the adapter itself. Press the Start PBC button on the router and on the adapter.

Note: You will have two minutes to push the PIN button on the router and device(s) you want to connect.

4.6.8 Schedule

Choose menu "Wireless → Schedule", time period allowed for the PC controlled to access the Internet.

his page allows you setup the wireless schedule rule. Please do not forget to configure ystem time before enable this feature.														
Ena	ble Wirele	ss Scł	redule	,										
nable	Day				Fr	om					1	ſo		
	Sun	-	00	-	(hour)	00	Ŧ	(min)	00	~	(hour)	00	~	(min)
	Sun	•	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	Ŧ	(min)
	Sun	•	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	Ŧ	(min)
	Sun	•	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	Ŧ	(min)
	Sun	•	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	-	(min)
	Sun	-	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	-	(min)
	Sun	•	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	-	(min)
	Sun	•	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	-	(min)
	Sun	-	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	-	(min)
	Sun	-	00	-	(hour)	00	Ŧ	(min)	00	-	(hour)	00	-	(min)

Figure 4-25 Schedule

4.7 Firewall



Figure 4-26 The Firewall menu

There are seven submenus under the Firewall menu (shown in Figure 4-26), **Port Filtering, IP Filtering, MAC Filtering, Port Forwarding, URL Filtering, DMZ, and VLAN.** Click any of them, and you will be able to configure the corresponding function.

4.7.1 Port Filtering

Choose menu "Firewall \rightarrow Port Filtering", you can control the wireless access by configuring the Port Filtering function as shown in Figure 4-27.

Port Filtering					
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.					
Enable Port Filtering					
Port Range: - Protocol: Both v					
Apply Changes Reset					
Current Filter Table:					
Port Range Protocol Comment Select					
Delete Selected Delete All Reset					

Figure 4-27 Port Filtering

- > Enable Port Filtering Check to Enable port filtering feature.
- Port Range / Protocol / Comment Specify the port range from start-port to end-port and put your comment to remind you why you have restriction on these ports. You can restricted TCP, UDP, or both protocol.

Be sure to click the Apply Changes button to save your settings on this page

4.7.2 IP Filtering

Choose menu "Firewall \rightarrow IP Filtering", you can control the wireless access by configuring the IP Filtering function as shown in Figure 4-28.

IP Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable IP Filtering
Loal IP Address: Protocol: Both 👻
Comment:
Apply Changes Reset
Current Filter Table:
Local IP Address Protocol Comment Select
Delete Selected Delete All Reset

Figure 4-28 IP Filtering

- > Enable IP Filtering Check to Enable IP filtering feature.
- Local IP Address / Protocol / Comment Specify the local IP address that you wish to put restriction and mark your comment to remind you why you have restriction on this IP address. You can restrict the traffic from TCP, UDP, or both protocol.

Be sure to click the Apply Changes button to save your settings on this page

4.7.3 MAC Filtering

Choose menu "Firewall \rightarrow MAC Filtering", you can control the wireless access by configuring the MAC Filtering function as shown in Figure 4-29.

Are Fatering	
Entries in this table are used to re from your local network to Intern such filters can be helpful in secu network.	estrict certain types of data packe 1et through the Gateway. Use of uring or restricting your local
Enable MAC Filtering	
MAC Address:	Comment:
Apply Changes Reset	
Current Filter Table:	
MAC Address	Comment Select

Figure 4-29 MAC Filtering

- > Enable MAC Filtering Check to Enable MAC filtering feature.
- > **MAC Address -** The wireless station's MAC address that you want to filter.

Be sure to click the **Apply Changes** button to save your settings on this page.

4.7.4 Port Forwarding

Choose menu "Firewall \rightarrow Port Forwarding", you can redirect the network traffic by configuring the Port Forwarding function as shown in Figure 4-30.

Port Forwarding					
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.					
Enable Port Forwarding					
IP Address: Protocol: Both Port Range:					
Comment:					
Apply Changes Reset					
Current Port Forwarding Table:					
Local IP Address Protocol Port Range Comment Select					
Delete Selected Delete All Reset					

Figure 4-30 Port Forwarding

- > Enable Port Forwarding Check to Enable port forwarding feature.
- > **IP Address –** Forward data packets to specific IP address in your local area network.
- > **Protocol -** The protocol used for forwarding data packets, either **TCP** or **UDP**, or **BOTH**
- Port Range The port range used by the remote system when it responds to the forwarding request. A response using one of these ports will be forwarded to the PC that triggered this rule.

Be sure to click the **Apply Changes** button to save your settings on this page.

4.7.5 URL Filtering

Choose menu "Firewall \rightarrow URL Filtering", you can restrict user to access specific web page by configuring the URL Filtering function as shown in Figure 4-31.

URL Filtering					
URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.					
Enable URL Filtering					
URL Address:					
Apply Changes Reset					
Current Filter Table:					
URL Address	Select				
Delete Selected Delete All	Reset				

Figure 4-31 URL Filtering

- > Enable URL Filtering Check to Enable URL filtering feature.
- > URL Address The address that you want to restrict user to access.

Be sure to click the Apply Changes button to save your settings on this page.

4.7.6 DMZ

Choose menu "**Firewall** \rightarrow **DMZ**", you can view and configure DMZ host in the screen as shown in Figure 4-32. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

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

Figure 4-32 DMZ

To assign a computer or server to be a DMZ server:

- 1. Check the **Enable DMZ** checkbox.
- 2. Enter the IP Address of a local host in the **DMZ Host IP Address** field.
- 3. Click the Apply Changes button.

Prote: After you set the DMZ host, the firewall related to the host will not work.

4.7.7 VLAN

Choose menu "Firewall \rightarrow VLAN", if you want to configure the Guest and Internal networks on VLAN, the switch you are using must support VLAN. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard, and enable this field as shown in Figure 4-33.

traditionally provided by routers. VLANs address issues such as scalability, security, and network management. Enable VLAN								
Enable	Ethernet/Wireless	WAN/LAN	Forwarding Rule	Tag	VID (1~4090)	Priority	CFI	
	Ethemet Port1	LAN	NAT 🔽	Г	3022	0 -	Г	
	Wireless 1 Primary AP	LAN	NAT 🔽		1	0 🔻	Γ	
	Wireless 1 Virtual AP1	LAN	NAT 🔽		1	0 -	Γ	
	Wireless 1 Virtual AP2	LAN	NAT 🔽		1	0 -		
	Wireless 1 Virtual AP3	LAN	NAT 🔽		1	0 -	Γ	
	Wireless 1 Virtual AP4	LAN	NAT 💌		1	0 -		
	Ethemet Port2	WAN	NAT		1	0 -		
Apply	Apply Changes Reset							

Figure 4-33 VLAN

> Be sure to click the **Apply Changes** button to save your settings on this page.

4.8 QoS

QoS in AIP-W512 provides uploading/downloading bandwidth management feature to control the packet flow through the router in order to allocate a specific amount of bandwidth for a computer (IP) or a particular application (Port)

Note: Please refer to actual network scenario carefully before setting up the QoS parameters, improper bandwidth assignment may cause QoS to work in-effectively.

QoS	
Entries in this table improve your online gam other network traffic, such as FTP or Web.	ing experience by ensuring that your game traffic is prioritized over
Enable QoS	
Automatic Uplink Speed	
Manual Uplink Speed (Kbps): 512	
Automatic Downlink Speed	
Manual Downlink Speed (Kbps): 512	
QoS Rule Setting:	
Address Type:	◎ IP ◎ MAC
Local IP Address:	
MAC Address:	
Mode:	Guaranteed minimum bandwidth 👻
Uplink Bandwidth (Kbps):	
Downlink Bandwidth (Kbps):	
Comment:	
Apply Changes Reset	

Figure 4-34 The QoS menu

4.9 Route Setup

AIP-W512 supports static and dynamic routing protocol. routing table is often used in multi-segment network; for a single network segment or daily Internet access, it is not necessary to change routing parameters in this page.

Note: Routing features in AIP-W512 are dynamic routing (RIPv1, and RIPv2) and static routing.

Dynamic Route

If dynamic routing is enabled, router will cache and learn network routes via routing protocols, allowing automation of routing info exchanges. The router utilizes the RIP (Routing Information Protocol) protocol, to determine the network traffic route based on the fewest number of hops between the source and the destination. This is useful when there are physical changes in the network layout (in this scenario, all the routers in this network should have RIP support).

Static Route

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. (For example: Destination Network IP: 192.168.12.1, Subnet Mask: 255.255.255.0, Gateway IP: 192.168.11.1)

Routing Setup					
This page is used to setup dynamic routing protocol or edit static route entry.					
Enable Dynamic Route					
NAT:	🖷 Enabled 🖉 Disabled				
Transmit:	🖲 Disabled 🛛 🖱 RIP 1 💭 RIP 2				
Receive:	🖲 Disabled 🔎 RIP 1 🔎 RIP 2				
Apply Changes	Reset				
Enable Static Route					
IP Address:					
Subnet Mask:					
Gateway:					
Metric:					
Interface:	LAN 💌				
Apply Changes	Reset Show Route Table				
Static Route Table:					
Destination IP Address	Netmask Gateway Metric Interface Select				
Delete Selected	Delete All Reset				

4.10 Management



Figure 4-35 The Management menu

There are nine submenus under the Management menu as shown in Figure 4-35: Status, Statists, DDNS, Time Zone Setting, Denial-of-Service, Log, Upgrade Firmware, Save/Reload Setting, and Password. Click any of them, and you will be able to configure the corresponding function.

4.10.1 Status

Choose menu "Management \rightarrow Status", display the current status of AIP-W512 as shown in Figure 4-39.

System	
Uptime	Oday:2h:Om:49s
Firmware Version	v3.2.2.2.2
Build Time	Mon Jun 10 04:32:25 EDT 2013
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID (III 2)	AIP-W512
Channel Number	11
Encryption	Disabled
BSSID	00:c0:ca:6f:9c:48
Associated Clients	2
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.11.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.11.1
DHCP Server	Enabled
MAC Address	00:c0:ca:6f:9c:46
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:c0:ca:6f:9c:47

Figure 4-35 Status

4.10.2 Statistics

Choose menu "Management \rightarrow Statistics", you can view the network traffic on the router as shown in Figure 4-36.

his page shows the par etworks.	cket counters for transmissio	n and reception reg	arding to wireless and Ethern
Wireless LAN	Sent Packets	128374	
	Received Packets	48342	
Ed a at I ANI	Sent Packets	824	
Ethernet LAN	Received Packets	5884	
Ethernet WAN	Sent Packets	0	
	Received Packets	0	

Figure 4-36 Network activity statistics

4.10.3 DDNS

Choose menu "Management -> DDNS", you can configure the Dynamic DNS function.

The router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as <u>www.dyndns.org</u>, or <u>TZO</u>. The Dynamic DNS client service provider will give you a password or key.

If the dynamic DNS **Service Provider** your select is <u>www.dyndns.org</u>, the page will appear as shown in Figure 4-41.

-	
Dynamic D	NS Setting
Dynamic DNS is a servi to go with that (possibly	ce, that provides you with a valid, unchanging, internet domain name (an URL) everchanging) IP-address.
Enable DDNS	
Service Provider :	DynDNS -
Domain Name :	host.dyndns.org
User Name/Email:	
Password/Key:	
Note: For TZO, you can have For DynDNS, you can t	a 30 days free trial <u>here</u> or manage your TZO account in <u>control panel</u> create your DynDNS account <u>here</u>
Apply Change	Reset

Figure 4-41 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

- 1. Type the **User Name** for your DDNS account.
- 2. Type the **Password** for your DDNS account.
- 3. Type the **Domain Name** you received from dynamic DNS service provider here.
- 4. Click the **Apply Change** button to log in to the DDNS service.

4.10.4 Time Zone Setting

Choose menu "Management \rightarrow Time Zone Settings", you can configure the time on the following screen.

	em time by synchronizing with a public time server over the internet.
Current Time :	Yr 2011 Mon 6 Day 8 Hr 18 Mn 11 Sec 14
	Copy Computer Time
Time Zone Select :	(GMT+08:00)Taipei
 Enable NTP clie Automatically A 	nt update Adjust Daylight Saving
NTP server :	192.5.41.41 - North America

Figure 4-42 Time zone settings

- Current Time Type in the current time into the blanks or click "Copy Computer Time" to get the current time from computer.
- > **Time Zone Select –** select the time zone.
- > Enable NTP client update click to enable the NTP client update.

P Note:

- This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the AIP-W512 successfully, otherwise, these functions will not take effect.
- 2. The time will be lost if the AIP-W512 is turned off.
- 3. The AIP-W512 will obtain GMT automatically from Internet if it has already connected to Internet.

4.10.5 Denial-of-Service (DoS)

DoS Protection will take effect only when the **Enable DoS Preventation** in "**Management** \rightarrow **DoS**" is enabled as shown in Figure 4-43.

Denial of Service	
A "denial-of-service" (DoS) attack is characterized by an er from using that service.	splicit attempt by hackers to prevent legitimate users of a service
Enable DoS Provention	
Whole System Flood: SYN	Packats/Second
Whole System Flood: FIN	Packats/Second
Whole System Flood: IIDP	Packats/Second
Whole System Flood: ICMP	Packate/Second
Par Source ID Flood, SVN	Packets/Second
	Packets/Second
Per-Source IP Plood: PIN	Packets/Second
Per-Source IP Plood: UDP	Packets/Second
Per-Source IP Flood: ICMP	Packets/Second
TCP/UDP PortScan	Low Sonsitivity
ICMP Smurf	
IP Land	
IP Spoof	
IP TearDrop	
PingOfDeath	
TCP Scan	
TCP SynWithData	
UDP Bomb	
UDP EchoChargon	
Select ALL Clear ALL	
Enable Source IP Blocking	D Block time (sec)
Apply Changes	

Figure 4-43 DoS

Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

4.10.6 Log

Enable Log			
system all	wireless	DoS	
Enable Remote Log	Log Server IP Address:		
Annly Changes			
r Blob on Bro			

Choose menu "Management \rightarrow Log", you can view the logs of the AIP-W512.

Figure 4-44 System Log

- > System all Display all the log file on the router .
- > Wireless Display just the wireless log on the router.
- **DoS –** Display just Denial-of-Service log on the router.
- > Enable Remote Log Click to enable remote log service.
- Log Server IP Address Please enter the IP address to store your log file when Enable Remote Log is enabled.

4.10.7 Upgrade Firmware

Choose menu "Management \rightarrow Upgrade Firmware", you can update the latest version of firmware for the router on the following screen.

Upgrade Firmware		
This page allows you upgrade the . power off the device during the up	Access Point firmware to new version. Please note, do not load because it may crash the system.	
Firmware Version:	v3.2.1-1	
Select File:	Browse	
Upload Reset		



Firmware Version - This displays the current firmware version.

To upgrade the router's firmware, follow these instructions below:

- 1. Download a more recent firmware upgrade file from our website.
- 2. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.
- 3. Click the Upgrade button.

P Note:

- New firmware versions are posted at our website and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the router rather than the configuration, you can try to upgrade the firmware.
- 2. When you upgrade the router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
- 3. Do not turn off the router or press the Reset button while the firmware is being upgraded, otherwise, the router may be damaged.
- 4. The router will reboot after the upgrading has been finished.

4.10.8 Save/Reload Setting

Choose menu "Management \rightarrow Save/Reload Setting", you can save the current configuration of the router as a backup file and restore the configuration via a backup file as shown in Figure 4-46.

Save/Reload Se	ettings
This page allows you save co	urrent settings to a file or reload the settings from the file which
was saved previously. Besid	es, you could reset the current configuration to factory default.
Save Settings to File:	Save
Load Settings from File:	Browse Upload
Reset Settings to Default:	Reset

Figure 4-46 Backup & Restore Configuration

- > Click the **Save** button to save all configuration settings as a backup file in your local computer.
- > To upgrade the router's configuration, follow these instructions.
 - Click the **Browse...** button to locate the update file for the router, or enter the exact path to the Setting file in the text box.
 - Click the **Upload** button.
- Click the **Reset** button restore the configurations of the router to factory defaults.

4.10.9 Password

Choose menu "Management \rightarrow Password", you can change the factory default user name and password of the router in the next screen as shown in Figure 4-47.

Password Setup	
This page is used to set the accoun password will disable the protectio	to access the web server of Access Point. Empty user name and n.
User Name:	
New Password:	
Confirmed Password:	
Apply Changes Reset	

Figure 4-47 Password

It is strongly recommended that you should change the factory default user name and password of the router, because all users who try to access the router's Web-based utility or Quick Setup will be prompted for the router's default user name and password.

Click the **Apply Change** button when finished.

Click the **Reset** button to clear all.

Appendix A: FAQ

1. How do I configure the router to access the Internet by ADSL users?

- 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Log in to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, finish by clicking Connect.

WAN	
WAN Connection Type:	PPPoE/Russia PPPoE 💙 🛛 Detect
PPPoE Connection:	
User Name:	username
Password:	•••••

Figure A-1 PPPoE Connection Type

2. How do I configure the router to access the Internet by Ethernet users?

 Log in to the router, click the "TCP/CP Settings" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "DHCP Client" for "WAN Connection Type", finish by clicking Save.

3. The wireless stations cannot connect to the router.

- 1) Make sure the "Enable Wireless router Radio" is checked.
- 2) Make sure that the wireless stations' SSID accord with the router's SSID.
- Make sure the wireless stations have right KEY for encryption when the router is encrypted.
- If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if necessary.

1. Configure TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.
- Click the Network and Internet Connections icon, and then click on the Network Connections tab in the appearing window.
- 3) Right click the icon that showed below, select Properties on the prompt page.



Figure B-1

4) In the prompt page that showed below, double click on the Internet Protocol (TCP/IP).

🚣 Local Area Connection Properties 🔗 🏼 💽
General Authentication Advanced
Connect using:
Bealtek RTL8139 Family PCI Fast Et
This connection uses the following items:
✓ Oos Packet Scheduler ✓ T AEGIS Protocol (IEEE 802.1x) v3.4.3.0 ✓ T Internet Protocol (TCP/IP)
Install Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected ✓ Notify me when this connection has limited or no connectivity
OK Cancel

Figure B-2

5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

Now you have two ways to configure the **TCP/IP** protocol below:

> Setting IP address automatically

Select **Obtain an IP address automatically**, Choose **Obtain DNS server automatically**, as shown in the Figure below:

Internet Protocol (TCP/IP) Propertie	25	<u>?</u> ×
General Alternate Configuration		
You can get IP settings assigned autor this capability. Otherwise, you need to the appropriate IP settings.	natically if your network supports ask your network administrator fo	n
Obtain an IP address automatical	ly	
C Use the following IP address:		— II
[P address:		
S <u>u</u> bnet mask:		
Default gateway:		
Obtain DNS server address autor	natically	
O	dresses:	_
Preferred DNS server:		
Alternate DNS server:		
	Ad <u>v</u> anced.	
	OK Car	icel



Prote: For Windows 98 OS or before, the PC and router may need to be restarted.

Setting IP address manually

- 1 Select **Use the following IP address** radio button. And the following items available.
- 2 If the router's LAN IP address is 192.168.11.1, specify the **IP address** as 192.168.2.x (x is from 2 to 254), and the **Subnet mask** as 255.255.255.0.
- 3 Type the router's LAN IP address (the default IP is 192.168.11.1) into the **Default gateway** field.
- 4 Select **Use the following DNS server addresses**. In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.

ou can get IP settings assigned (is capability. Otherwise, you nee e appropriate IP settings.	automatically if your network supports d to ask your network administrator for
C <u>O</u> btain an IP address autom	atically
Use the following IP address	¢
IP address:	192 . 168 . 2 . 241
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	192.168.2.1
C Obtain DNS server address C Use the following DNS serve	automatically addresses:
Preferred DNS server:	202 . 96 . 134 . 133
<u>A</u> lternate DNS server:	X X 0
	Ad <u>v</u> anced

Figure B-4

Now, click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b, 802.11g, 802.11n
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, one 10/100M Auto-Negotiation LAN RJ45 port supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LEDs	PWR x1, WLAN x1, LAN x1, WAN x1
Safety & Emissions	FCC, CE
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	 11n: up to 150Mbps (Automatic) 11g: 54/48/36/24/18/12/9/6M (Automatic) 11b: 11/5.5/2/1M (Automatic)
Channels	1~13
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Antenna Gain	2dBi
Environmental and Physical	
Temperature.	Operating : 0°C ~50°C
	Storage: -20°C ~70°C
Humidity	Operating: 10% - 90% RH, Non-condensing
	Storage: 5% - 90% RH, Non-condensing

Appendix D: Glossary

- 802.11b The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- 802.11g specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- DDNS (Dynamic Domain Name System) The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- DHCP (Dynamic Host Configuration Protocol) A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- DMZ (Demilitarized Zone) A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- DNS (Domain Name System) An Internet Service that translates the names of websites into IP addresses.
- > Domain Name A descriptive name for an address or group of addresses on the Internet.
- DSL (Digital Subscriber Line) A technology that allows data to be sent or received over existing traditional phone lines.
- > **ISP** (Internet Service Provider) A company that provides access to the Internet.
- MTU (Maximum Transmission Unit) The size in bytes of the largest packet that can be transmitted.
- NAT (Network Address Translation) NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- PPPoE (Point to Point Protocol over Ethernet) PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- SSID A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

- WEP (Wired Equivalent Privacy) A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- Wi-Fi A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- WLAN (Wireless Local Area Network) A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.