WL354AP

User manual

Ver: 1.0

Content

Chapter 1 Introduction

The WL354AP, a Wireless Local Area Network (WLAN) Access Point supporting 802.11 b/g
and bringing high-speed wireless Internet connection to a home or office, can provide the

transmission of broadband data service. It is tailored to a wide range of both residential (in-home)
and commercial (offices, apartments, hotels, warehouses) network applications. It gives you a

blazingly fast connection to the internet, far fast and more convenient. This AP is a high-performance
wireless gateway and can support data rate up to 54Mbps.

It has a 100M wide area network (WAN) port connecting external Internet network. Using 802.11 b/g
wireless technology, Wi-Fi enabled computers and devices can wirelessly connect with this AP and

share a single incoming Internet connection. With four additional local Ethernet LAN ports, you can
connect four different PCs sharing the Internet connection.

It supports static IP, Dynamic IP, as well as PPPoE connections, and works with applications such
as online gaming and VPN transparent connections with no additional configuration.

It is easily upgradeable, making it future-proof for both end-users and service providers. Whether it's
for a home user who wants to share wireless high-speed Internet access or for a small office that

needs Internet access for conducting essential business activities, this AP is the ideal wireless
broadband solution.

Product Outline

Product topology
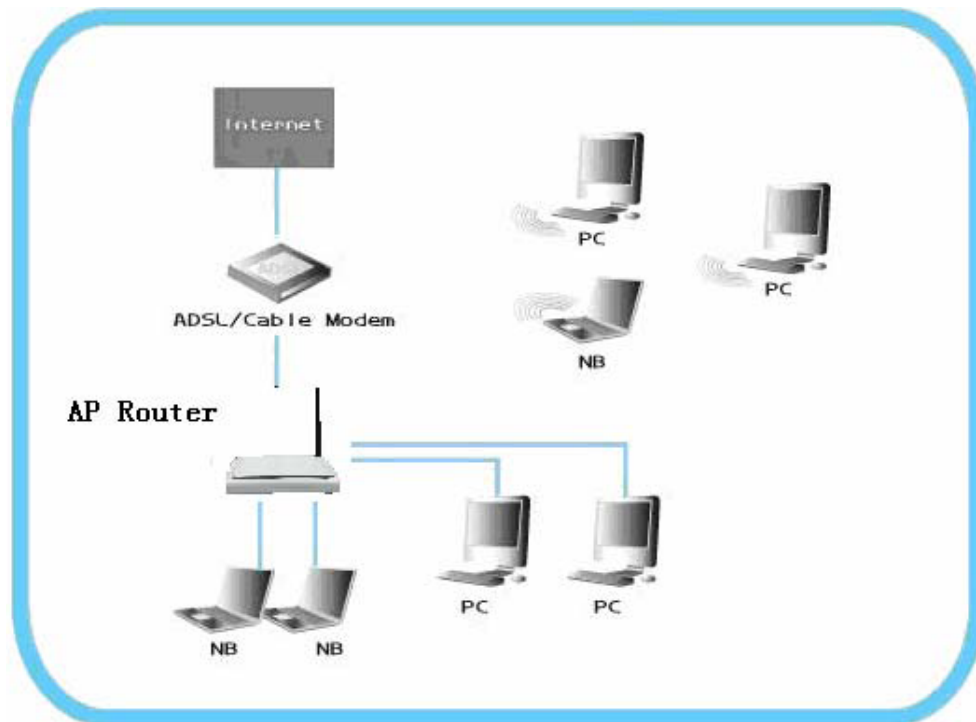
Applications

- ⌘ Home and   SOHO wireless gateway
- ⌘ The small enterprise Applications
- ⌘ TV over IP (IPTV)
- ⌘ Voice over IP (VoIP)
- ⌘ Higher data rate broadband sharing
- ⌘ Shared broadband internet access
- ⌘ Audio and video streaming and transfer
- ⌘ PC file and application sharing
- ⌘ Network and online gaming

Compliance Certificates:

- ⌘ Wi-Fi Certification
- ⌘ FCC Class B
- ⌘ CE Mark

External Connectors

- ⌘ 4   10/100M local Ethernet Ports (RJ-45)
- ⌘ 1 100M WAN port

Wireless Feature
- ⌘ Compatible with IEEE 802.11 b/g
- ⌘ Support 64/128-bit WEP, 802.1x, WPA, and WPA2 for wireless security
- ⌘ Support RTS/CTS, Fragmentation and Defragmentation function
- ⌘ Support WMM , WMM-PS

- ⌘ Support Multiple BSSID
- ⌘ Hardware WEP, TKIP, AES Engines
- ⌘ Support WDS
- ⌘ Hide SSID
- ⌘ Support MAC Access/Deny List
- ⌘ WMM support
- ⌘ WPA1/2 - PSK (WPA Home), WPA1/2 - 802.1x (WPA Enterprise)
- ⌘ EAP - TLS, TTLS, LEAP, PEAP
- ⌘ Roaming
- ⌘ Wireless Frequency Range, 2.4 ~ 2.4835GHz ISM Band.
- ⌘ Radio and Modulation Type. IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK ; IEEE 802.11 g: BPSK, QPSK, 16QAM, 64QAM ;
- ⌘ Transmission distance. 300 meters Outdoors, 100 meters Indoors coverage area(It's limited in an environment.)
- ⌘ Antenna 2dBi
- ⌘ Transmission power：802.11b: Typ.18dBm @Normal Temp Range; 802.11g:Typ.15dBm @ Normal Temp Range

Management Support

- ⌘ Device Configuration, Management and Update
- ⌘ Web based GUI
- ⌘ Localization support
- ⌘ Embedded web server
- ⌘ Download image via HTTP, TFTP client, TFTP server
- ⌘ Command Line Interface via serial port, telnet, or ssh
- ⌘ Menu-driven CLI via serial port or telnet
- ⌘ Universal Plug and Play (UPnP) Internet Gateway Device (IGDv1.0)
- ⌘ SNMP v1/v2c agent, SNMP MIBs;802.11 b/g MIBs;
- ⌘ PSI configuration file upload and download
- ⌘ Date/time update from SNTP Internet Time Server

Security Support

- ⌘ Three level login including local admin, local user and remote technical support access
- ⌘ Service access control based on incoming interface: WAN or LAN
- ⌘ Service access control based on source IP addresses
- ⌘ Protect DOS attacks from WAN/LAN: SYN flooding, IP surfing, ping of Death, fragile, - UDP ECHO (port 7), teardrop, land.
- ⌘ PAP (RFC1334), CHAP (RFC1994), MSCHAP for PPP session.
- ⌘ IP filter, Parental control.

OS Support

Linux kernel 2.4/2.6

Environment

- ⌘ Operating temperature: 0℃ to 40℃
- ⌘ Storage temperature: -20℃ to 70℃

⌘ Operating Humidity: 10%~95% no freezing
⌘ Storage humidity: 5%~95% no freezing

Chapter 2 Hardware Installation

This chapter contains the information you need to install and set up the Wireless RTL8186AP.   It covers the following topics:

- Decide where to place the AP
- Connecting the Access Point
- Checking the LED indicators
- Attaching an External Antenna

Decide where to place the AP

Place the AP in a dry, clean location near the hub, switch, computer or printer that will be connected to the AP. The location must have a power source and be within the following distance of a Wi-Fi compliant wireless LAN access point or wireless access point.

The key to maximizing the wireless range is to follow these basic guidelines:

- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise. The location should be away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators.
- Keep the number of walls and ceilings between the AP and other network devices to a minimum - each wall or ceiling can reduce your AP's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- Be a ware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- Building materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

Checking the LED Indicators

When the AP is connected to power, LEDs indicate activity as follows:

LED	Color	Activity
Power	Green	On: Power On
		Off: Power Off
WAN	Green	On: sending/receiving data from WAN Port
		Off: Transmitter is off
WLAN	Green	Blinking: sending/receiving data
		Off: Transmitter is off
LAN	Green	On: Good Link
		Blinking: sending/receiving data from LAN Port
		Off: No link

Attaching an External Antenna

This AP comes with an antenna. It is external removable monopole signal-band 2.4 GHz antenna. It can be rotated over 90 degrees and is omni-directional with a gain of less than 2dBi. You can change a 5dBi high gain antenna for creates a superior far-reaching wireless network

Chapter 3 Configuring the wireless AP

If the default AP configuration does not meet your network requirements, or if you want to customize the settings for your own network, you can directly connect to the device through it's Ethernet port or wireless to change the configuration. There are two typical applications:

1. Networks with a DHCP Server

If your network has a DHCP server, an IP address is automatic ally assigned to the AP. It takes between one and two minutes for the Access Point to determine if there is a DHCP server on the network. After you determine the AP's IP address, you can enter that IP address into a web browser on a computer on the same subnet to view the Access Point's system status or change its configuration

2. Networks without a DHCP Server

If your network does not have a DHCP server, the Access Point uses a factory assigned IP address (192.168.1.254). You can use that IP address to configure the Access Point, or you can assign a new IP address to the Access Point.

To verify that the Access Point is using the default IP address assigned at the factory: Connect a computer directly to the Access Point using the supplied standard Category 5 UTP Ethernet cable. Enter the Access Point's default IP address (192.168.1.254) into the computer's web browser. If the Configuration Management System starts, the Access Point is using the factory assigned IP address. You can configure the Access Point with the Web interface:

Username, type admin (case sensitive)
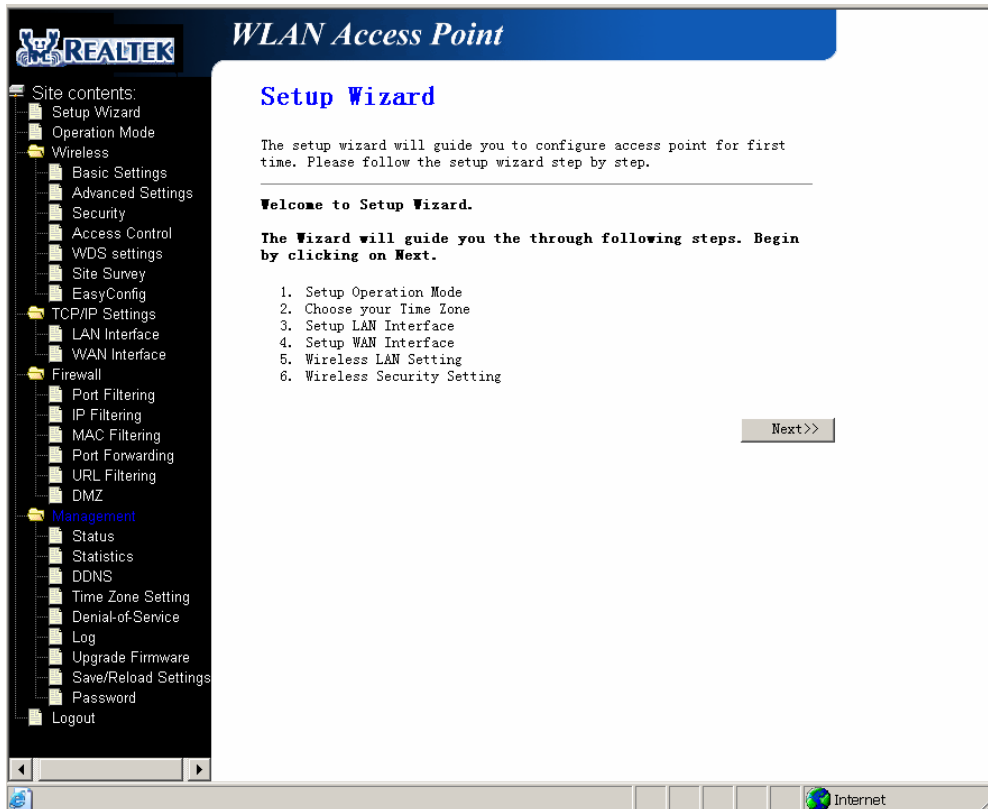
Password, type admin

Click ok.
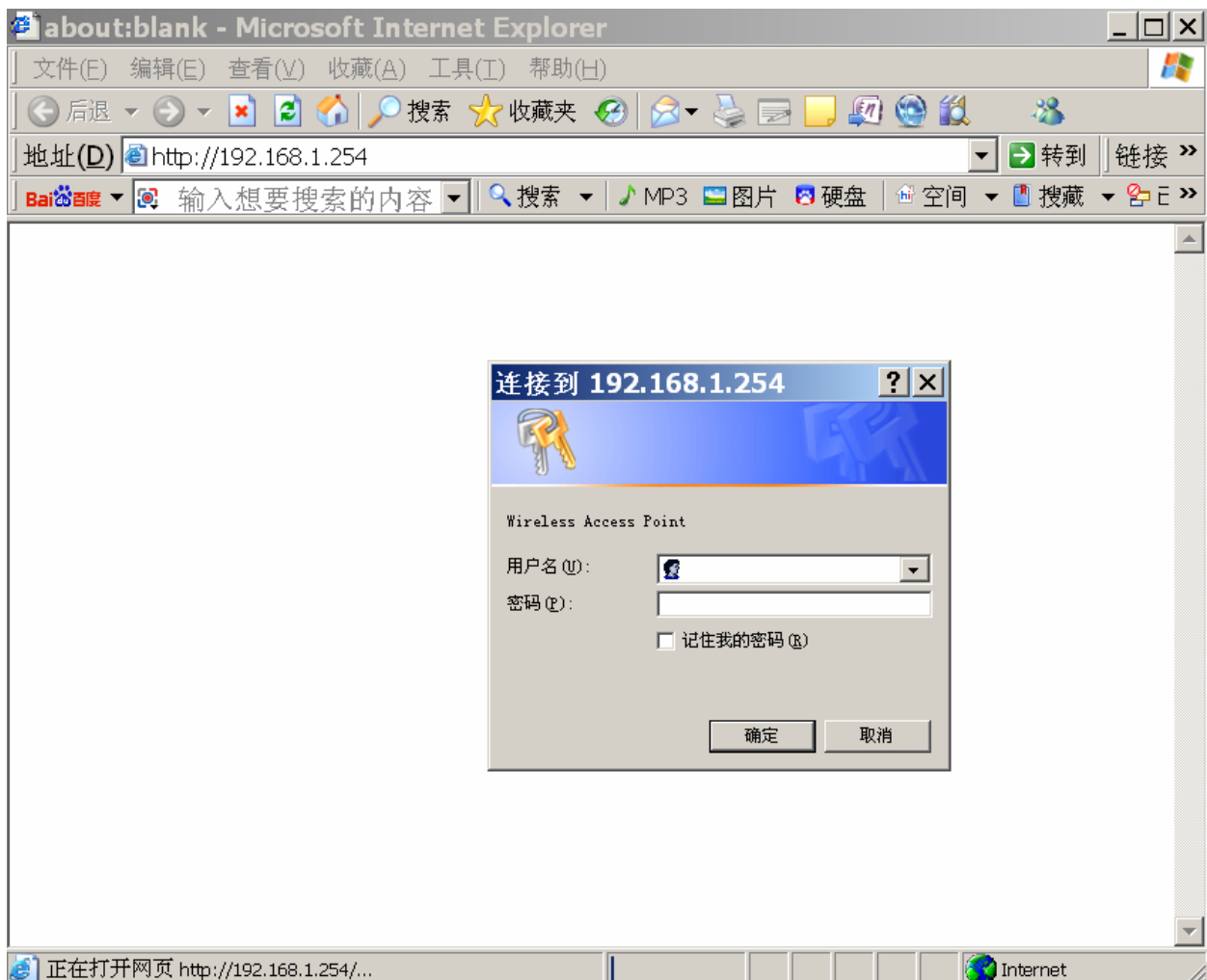
In the following, you will learn how to configure the basic functions of your wireless AP.

setup wizard

After login on the web UI，The setup wizard will guide you to configure access point for first time.

You can follow the setup wizard step by step or choose Status and Statistics to view information about the AP.

Operation Mode

You may configure the operation mode suitable for you environment. If you select Bridge mode, all Ethernet and wireless interfaces are bridged into a single bridge interface. If you select Gateway mode, the first Ethernet port is treated as WAN port. The other Ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

Click Cancel to close without saving, click Apply to save the settings.

Wireless Settings

⌘ Basic Wireless Settings

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

Band

The RTL8186AP supports 11b, 11g, and 11b/g mixed mode. You can configure the suitable network mode.

Mode

The RTL8186AP supports AP, Client，WDS,AP+WDS mode, you can select one from the list.

SSID

Service Set Identifier. This is the assigned name for a wireless Wi-Fi network. Stations must use this unique identifier to communicate with an Access Point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

Channel / Frequency

Select the channel for your wireless LAN in Channel/Frequency block. The default setting is Smart Select it selects the channel which provides the best transmission quality. The frequencies available vary depending which wireless mode you select.

⌘ **Advanced Wireless Settings**

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Authentication Type

Select between open system, shared key and auto.

Fragment threshold

The maximum packet size is used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.

RTS Threshold

Request to send threshold. The packet size that is used to determine if it should use the CSMA/CA mechanism or the CSMA/CD mechanism, the default is 2347.

Beacon Interval

The interval time between 20ms and 1024ms for each beacon transmission. The default is 100ms.

Basic Data Rate

Choose between the following data rates 1, 2, 5.5, 11, 6, 9 , 12, 18, 24, 36, 48,54 and auto. Default is auto.

Wireless Advanced Settings

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

Authentication Type:	○ Open System ○ Shared Key ⦿ Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto ▼
Preamble Type:	⦿ Long Preamble ○ Short Preamble
Broadcast SSID:	⦿ Enabled ○ Disabled
IAPP:	⦿ Enabled ○ Disabled
802.11g Protection:	⦿ Enabled ○ Disabled
RF Output Power:	⦿ 100% ○ 50% ○ 25% ○ 10% ○ 5%
Turbo Mode:	⦿ Auto ○ Always ○ Off
	Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

[Apply Changes]   [Reset]

Click Cancel to close without saving, click Apply to save the settings.

⌘ **Security**

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.

For example, when you select Security mode, you should config the Radius Sever information.

Click Cancel to close without saving, click Apply to save the settings.

⌘ **Access Control**

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

Wireless Access Control

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

Wireless Access Control Mode: [Disable ▼]
                                 Disable
                                 Allow Listed

MAC Address: [   ]   Comm[Deny Listed]

[Apply Changes]   [Reset]

Current Access Control List:

MAC Address	Comment	Select

[Delete Selected]   [Delete All]   [Reset]

⌘ WDS Link Settings

WDS (Wireless Distribution System) allows access points to communicate with one another

wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required.   Basically the access points will act as a client and an access point at the same time.

WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bi-

directional, so the AP must know the MAC address of the other AP, and the other AP must have a WDS link back to the AP.

Dynamically assigned and rotated encryption key are not supported in a WDS connection. This

means that WPA and other dynamic key assignment technologies may not be used. Only Static WEP keys may be used in a WDS connection, including any STAs that are associated with a WDS repeating AP.

Enter the MAC address of the other APs you want to link to and click enable.

Supports up to 8 point to multipoint WDS links, check Enable WDS and then enable on the MAC

addresses.

Example of a WDS topology:

AP1 <-- WDS --> Master AP (our AP) <-- WDS --> AP3<-- WDS --> AP4

WDS Settings

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

☑ **Enable WDS**

Add WDS AP: **MAC Address** [   ]   **Comment**
[   ]

[Apply Changes]   [Reset]   [Set Security]
[Show Statistics]

Current WDS AP List:

MAC Address	Comment	Select

[Delete Selected]   [Delete All]   [Reset]

⌘ **Wireless Site Survey**

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

Wireless Site Survey

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

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
802.11g-SSID	00:e0:4c:81:86:d1	11 (B+G)	AP	no	15	●
RT2880_AP	00:0c:43:28:60:68	6 (B+G)	AP	no	6	○
TWB9	00:19:5b:db:59:6e	1 (B+G)	AP	WPA-PSK	1	○

[Refresh]   [Connect]

⌘ **Wireless EasyConfig**

This page allows you change the setting for EasyConfig. Use this feature could let your wireless client automatically synchronizes its setting and connect to the Access Point in a minute without any hassle.

Wireless EasyConfig

This page allow you change the setting for EasyConfig. Use this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ **Enable EasyConfig**

Configure Method: [Button ▼]   [Apply Changes]

☐ **First Time Configuration**

Question 1:

Pick up one question: [Your lucky number (no more than 4 digits) ? ▼]

Answer: [_____]

Question 2:

Pick up one question: [Your favorite person ? ▼]

Answer: [_____]

[Do EasyConfig (Button)]   [Do EasyConfig (Q&A)]

TCP/IP Settings

WAN

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

WAN Interface Setup

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

WAN Access Type: [DHCP Client ▼]

- Static IP
- DHCP Client
- PPPoE
- PPTP

Host Name: [_____]

MTU Size: [_____] (00-1492 bytes)

⦿ **Attain DNS Automatically**

○ **Set DNS Manually**

  DNS 1: [_____]

  DNS 2: [_____]

  DNS 3: [_____]

Clone MAC Address: [000000000000]

☐ **Enable uPNP**

☐ **Enable Ping Access on WAN**

☐ **Enable Web Server Access on WAN**

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

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

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

[Apply Changes]   [Reset]

14

Click Cancel to close without saving, click Apply to save the settings.

LAN

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

LAN Interface Setup

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

IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.1.100 – 192.168.1.200 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Apply Changes   Reset

Click Cancel to close without saving, click Apply to save the settings.

Firewall

This section mainly introduces some ways to protect you through the following configuration.

⌘ **Port Filtering**

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

Port Filtering

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

☑ **Enable Port Filtering**

Port Range: [ ] – [ ]   Protocol: Both ▼   Comment:

Both
TCP
UDP

Apply Changes   Reset

Current Filter Table:

Port Range	Protocol	Comment	Select

Delete Selected   Delete All   Reset

⌘ **IP Filtering**

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

IP Filtering

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

☑ **Enable IP Filtering**

Loal IP Address: [   ]   Protocol: [Both ▾]   Comment:
[   ]
                                          | Both |
                                          | TCP |
                                          | UDP |

[Apply Changes]   [Reset]

Current Filter Table:

Local IP Address	Protocol	Comment	Select

[Delete Selected]   [Delete All]   [Reset]

⌘ **MAC Filtering**

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

MAC Filtering

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

☑ **Enable MAC Filtering**

MAC Address: [   ]   Comment: [   ]

[Apply Changes]   [Reset]

Current Filter Table:

MAC Address	Comment	Select

[Delete Selected]   [Delete All]   [Reset]

⌘ **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.

⌘   **URL Filtering**

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

⌘   **DMZ**

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

DMZ

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

☑ **Enable DMZ**

DMZ Host IP Address: [   ]

[Apply Changes]   [Reset]

Management

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

⌘ **Status**

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

Access Point Status

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

System	
Uptime	0day:2h:6m:15s
Firmware Version	v1.4
Wireless Configuration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G)
SSID	802.11g-SSID
Channel Number	4
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:00:00:00:00:00
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	11:11:11:11:11:11

goahead WEBSERVER

⌘ **Statistics**

The Statistics page shows all the statistics information about your AP.

Statistics

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

Wireless LAN	Sent Packets	0
	Received Packets	32
Ethernet LAN	Sent Packets	0
	Received Packets	0
Ethernet WAN	Sent Packets	21
	Received Packets	16

Refresh

⌘ **Dynamic DNS Setting**

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

Dynamic DNS Setting

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

☑ **Enable DDNS**

Service Provider :	DynDNS ▾
	DynDNS
Domain Name :	TZO
User Name/Email:	
Password/Key:	

Note:
For TZO, you can have a 30 days free trial here *or manage your TZO account in*
control panel
For DynDNS, you can create your DynDNS account here

[Apply Change] [Reset]

⌘ **Time Zone Setting**

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

Time Zone Setting

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

Current Time : Yr [2000] Mon [1] Day [1] Hr [0] Mn [13] Sec [9]

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana ▾

☐ **Enable NTP client update**

NTP server : ⦿ 192.5.41.41 - North America ▾

○ [   ] (Manual IP Setting)

[Apply Change] [Reset] [Refresh]

⌘ Denial of Service

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

☑ **Enable DoS Prevention**

☐ Whole System Flood: SYN `0` Packets/Second

☐ Whole System Flood: FIN `0` Packets/Second

☐ Whole System Flood: UDP `0` Packets/Second

☐ Whole System Flood: ICMP `0` Packets/Second

☐ Per-Source IP Flood: SYN `0` Packets/Second

☐ Per-Source IP Flood: FIN `0` Packets/Second

☐ Per-Source IP Flood: UDP `0` Packets/Second

☐ Per-Source IP Flood: ICMP `0` Packets/Second

☐ TCP/UDP PortScan `Low ▼` Sensitivity

☐ ICMP Smurf

☐ IP Land

☐ IP Spoof

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

☐ UDP Bomb

☐ UDP EchoChargen

[Select ALL]   [Clear ALL]

☐ Enable Source IP Blocking `0` Block time (sec)

[Apply Changes]

⌘ System Log

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

System Log

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

☑ **Enable Log**
    ☐ system all   ☐ wireless   ☐ DoS
                     Log Server IP
    ☐ Enable Remote Log Address: [ ]

[Apply Changes]

[Refresh]   [Clear]

⌘ **Upgrade Firmware**

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

Upgrade Firmware

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

Select File: [ ] [浏览...]

[Upload]   [Reset]

Click Reset to clear the firmware, click Apply to upgrade the firmware.

⌘ **Save/Reload Settings**

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

Save/Reload Settings

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

Save Settings to File:	Save...
Load Settings from File:	[_____] 浏览... Upload
Reset Settings to Default:	Reset

⌘ **Password Setup**

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

Password Setup

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

User Name:	[_____]
New Password:	[_____]
Confirmed Password:	[_____]

Apply Changes   Reset