



Extend the Remote AP (BSS)

This device provides a software function to extend the AP-BSS (Basic Service Set) which is in the remote distance. When in AP, WDS, AP+WDS mode, this device can be set up to extend the remote AP BSS. This device plays two roles simultaneously, connecting to the remote AP-BSS as a WLAN client and serving as local AP-BSS and then forward packages from remote BSS to local BSS.

There are two ways below to enable this function.

1. Enable this option and then select a SSID in the Table that you want. Click Apply Changes button to take effective. **(Click Refresh button to make table renew)**

Site contents:

- Wizard
- Operation Mode
- Wireless**
- Basic Settings
- Advanced Settings
- Security
- Access Control
- WDS settings
- Site Survey
- Connecting Profile
- TCP/IP
- Firewall
- Management
- Reboot

well as wireless network parameters. Enable universal repeater mode can let radio act as AP and client simultaneously but remember the channel must be as same as the connected AP.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: AP-SSID

Channel Number: 11 Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

3 ☒ **Enable Universal Repeater Mode**

Extended SSID:

(once selected and applied, extended SSID and channel number will be updated)

SSID	BSSID	Channel	Type	Encrypt	RSSI	Quality	Select
WLAN_G_TEST	00:0d:14:00:80:18	1 (B+G)	AP	no	32 (-70 dbm)	81	5 <input checked="" type="radio"/>
RTL8186-default	00:00:00:aa:bb:01	1 (B+G)	AP	no	16 (-80 dbm)	76	<input type="radio"/>

4 Refresh

6 Apply Changes Reset

Note: It only applies under **AP**、**WDS** and **AP+WDS** mode

2. Enter specific SSID in the Extended SSID field and then click Apply Changes button to take effective.

Site contents:

- Wizard
- Operation Mode
- Wireless**
- Basic Settings
- Advanced Settings
- Security
- Access Control
- Site Survey
- Connecting Profile
- TCP/IP
- Firewall
- Management
- Reboot

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. Enable universal repeater mode can let radio act as AP and client simultaneously but remember the channel must be as same as the connected AP.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: AP-SSID

Channel Number: 11 Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

3 ☒ **Enable Universal Repeater Mode**

Extended SSID: WLAN_G_TEST

(once selected and applied, extended SSID and channel number will be updated)

SSID	BSSID	Channel	Type	Encrypt	RSSI	Quality
WLAN_G_TEST						

Refresh

4 Apply Changes Reset

Ch 3. Configuring WDS

Wireless Distribution System (WDS) uses wireless media to communicate with the other devices, like the Ethernet does. This function allows one or more remote LANs connect with the local LAN. To do this, you must set these devices in the same channel and set MAC address of other devices you want to communicate with in the WDS AP List and then enable the WDS.

When you decide to use the WDS to extend your WLAN, please refer the following instructions for configuration.

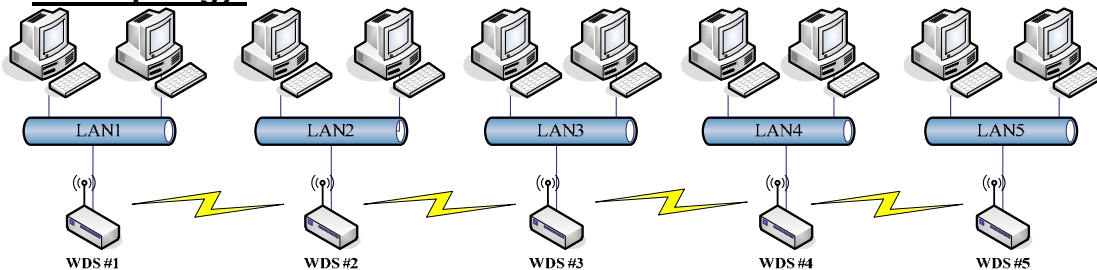
- The bridging devices by WDS must use the same radio channel.
- When the WDS function is enabled, all wireless stations can't connect the device.
- If your network topology has a loop, you need to enable the 802.1d Spanning Tree function.
- You don't need to add all MAC address of devices existed in your network to WDS AP List. WDS AP List only needs to specify the MAC address of devices you need to directly connect to.
- The bandwidth of device is limited, to add more bridging devices will split the more bandwidth to every bridging device.

WDS network topology

In this section, we will demonstrate the WDS network topologies and WDS AP List configuration. You can setup the four kinds of network topologies: bus, star, ring and mesh.

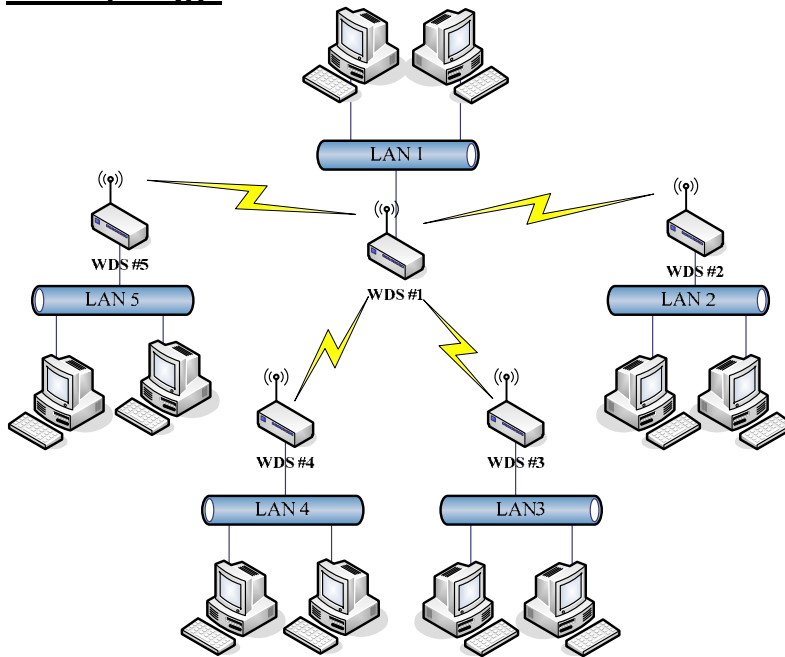
In this case, there are five devices with WDS enabled: WDS1, WDS2, WDS3, WDS4 and WDS5.

Bus topology:



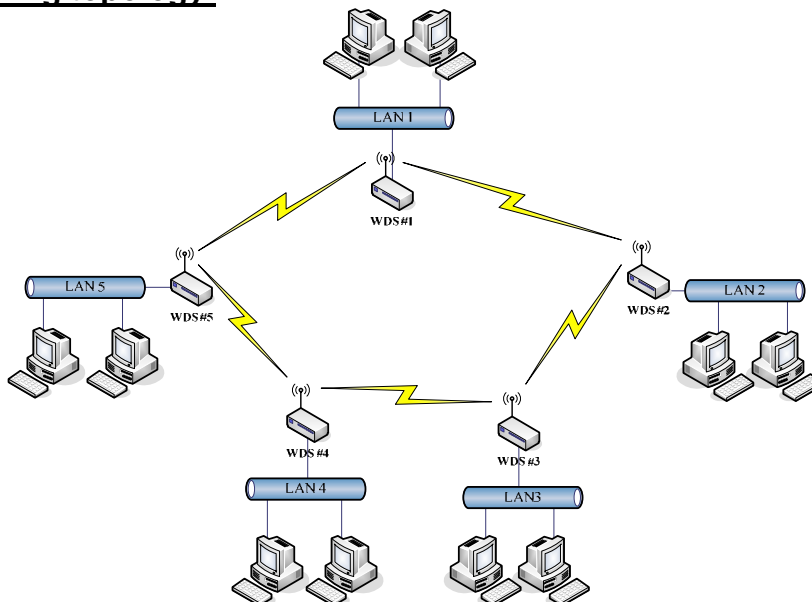
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Address of WDS2	No
WDS2	The MAC Addresses of WDS1 and WDS3	No
WDS3	The MAC Addresses of WDS2 and WDS4	No
WDS4	The MAC Addresses of WDS3 and WDS5	No
WDS5	The MAC Address of WDS4	No

Star topology:



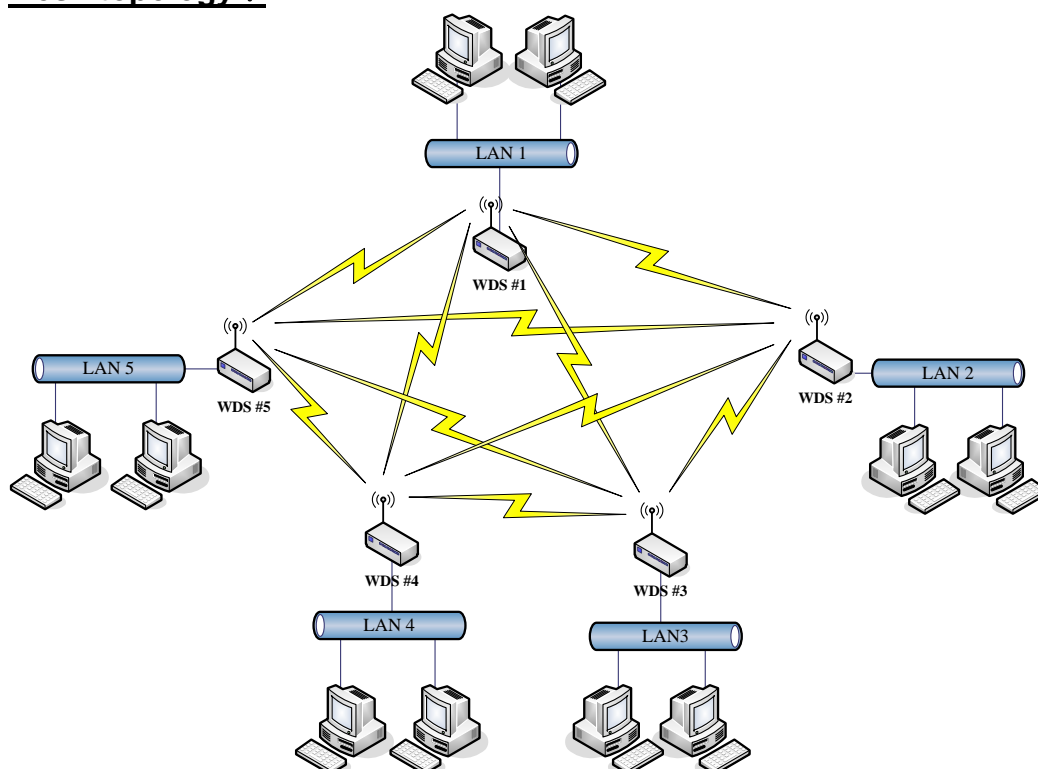
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	No
WDS2	The MAC Address of WDS1	No
WDS3	The MAC Address of WDS1	No
WDS4	The MAC Address of WDS1	No
WDS5	The MAC Address of WDS1	No

Ring topology:



Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2 and WDS5	Yes
WDS2	The MAC Addresses of WDS1 and WDS3	Yes
WDS3	The MAC Addresses of WDS2 and WDS4	Yes
WDS4	The MAC Addresses of WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS4 and WDS1	Yes

Mesh topology :



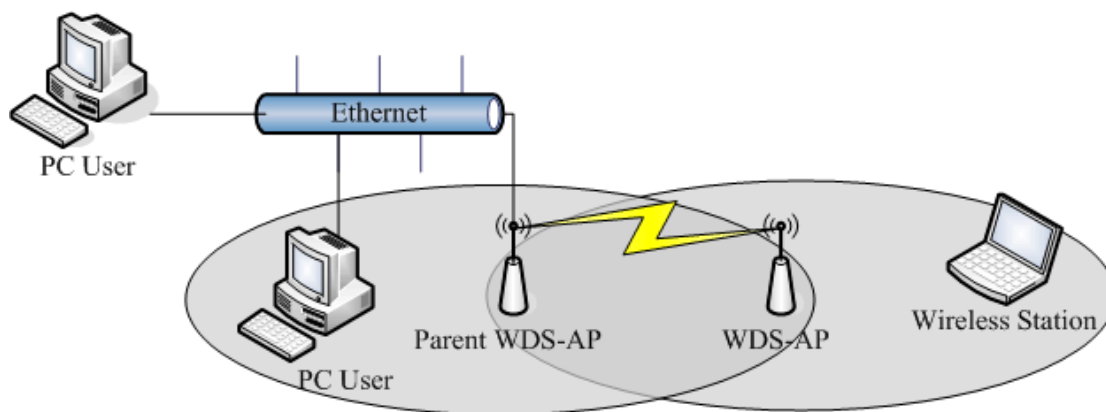
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	Yes
WDS2	The MAC Addresses of WDS1, WDS3, WDS4 and WDS5	Yes
WDS3	The MAC Addresses of WDS1, WDS2, WDS4 and WDS5	Yes
WDS4	The MAC Addresses of WDS1, WDS2, WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS1, WDS2, WDS3 and WDS4	Yes

WDS Application

Peer to Peer connection

WDS-AP can be used to increase the coverage area of another device (Parent WDS-AP). Between the Parent WDS-AP and the WDS-AP, Wireless Stations can move among the coverage areas of both devices. When you decide to use the WDS function to connect another WDS-AP, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel and SSID.
- Choose “WDS+AP” mode.
- Using the bus or star network topology.



Description	Entries of WDS AP List	Spanning Tree Protocol Required
Parent WDS-AP	The MAC Address of WDS-AP	Yes
WDS-AP	The MAC Address of Parent WDS-AP	Yes

Wireless Bridge

Wireless Bridge can establish a wireless connection between two or more Wired LANs. When you decide to use the WDS as a Wireless Bridge, please refer the following instructions for configuration.

- In AP mode, enable the WDS function.
- You must set these connected devices with the same radio channel, but you may use different SSID.
- Choose “WDS” mode for only wireless backbone extension purpose.
- You can use any network topology, please refer the WDS topology section.

Ch 4. Advanced Configurations

Configuring LAN to WAN Firewall

Filtering function is used to block or permit packets from LAN to WAN. The device supports three kinds of filter Port Filtering, IP Filtering and MAC Filtering. All the entries in current filter table are used to restrict or allow certain types of packets from your local network to through the device. Use of such filters can be helpful in securing or restricting your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page. The IP forwarding default policy is “ACCEPT”.

If you want block some application from LAN to WAN, you can go to Route page to select “ACCEPT” for IP Forwarding Default Policy.



If you want permit some application from LAN to WAN, you can go to Route page to select “DROP” for IP Forwarding Default Policy.



Port Filtering

When you enable the Port Filtering function, you can specify a single port or port ranges in current filter table. If you select ACCEPT for the IP forwarding default policy, once the source port of outgoing packets match the port definition or within the port ranges in the table, the firewall will block those packets form LAN to WAN.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
 - Port Filtering**
 - IP Filtering
 - MAC Filtering
 - Port Forwarding
 - DMZ
 - VPN
- Management
- Reboot

Port Filtering

Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.

☒ **Enable Port Filtering (denied list)**

Port Range: -
Protocol: **Both**
Comment:

Current Filter Table:

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

If you select DROP for the IP forwarding default policy, once the source port of outgoing packets match the port definition or within the port ranges in the table, the firewall will allow those packets form LAN to WAN.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
 - Port Filtering**
 - IP Filtering
 - MAC Filtering
 - Port Forwarding
 - DMZ
 - VPN
- Management
- Reboot

Port Filtering

Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.

☒ **Enable Port Filtering (allowed list)**

Port Range: -
Protocol: **Both**
Comment:

Current Filter Table:

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

IP Filtering

When you enable the IP Filtering function, you can specify local IP Addresses in current filter table. If you select ACCEPT for the IP forwarding default policy, once the source IP address of outgoing packets match the IP address definition in the table, the firewall will block those packets form LAN to WAN.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
 - Port Filtering
 - IP Filtering**
 - MAC Filtering
 - Port Forwarding
 - DMZ
 - VPN
- Management
- Reboot

IP Filtering

Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.

☒ **Enable IP Filtering (denied list)**

Local IP Address: Protocol: Both Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
192.168.2.11	TCP	Client 11	<input type="checkbox"/>
192.168.2.23	TCP+UDP	Client 23	<input type="checkbox"/>
192.168.2.35	UDP	Client 35	<input type="checkbox"/>

If you select DROP for the IP forwarding default policy, once the source IP address of outgoing packets match the IP address definition in the table, the firewall will allow those packets form LAN to WAN.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
 - Port Filtering
 - IP Filtering**
 - MAC Filtering
 - Port Forwarding
 - DMZ
 - VPN
- Management
- Reboot

IP Filtering

Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.

☒ **Enable IP Filtering (allowed list)**

Local IP Address: Protocol: Both Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
192.168.2.11	TCP	Client 11	<input type="checkbox"/>
192.168.2.23	TCP+UDP	Client 23	<input type="checkbox"/>
192.168.2.35	UDP	Client 35	<input type="checkbox"/>

MAC Filtering

When you enable the MAC Filtering function, you can specify the MAC Addresses in current filter table. If you select ACCEPT for the IP forwarding default policy, once the source MAC Address of outgoing packets match the MAC Address definition in the table, the firewall will block those packets form LAN to WAN.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
 - Port Filtering
 - IP Filtering
 - MAC Filtering**
 - Port Forwarding
 - DMZ
 - VPN
- Management
- Reboot

MAC Filtering

Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.

☒ **Enable MAC Filtering (denied list)**

MAC Address: Comment:

Current Filter Table:

MAC Address	Comment	Select
00:00:03:12:01:02	Client 1	<input type="checkbox"/>
00:00:00:06:06:10	Client 5	<input type="checkbox"/>
00:00:00:10:10:22	Client 13	<input type="checkbox"/>

If you select DROP for the IP forwarding default policy, once the source MAC Address of outgoing packets match the MAC Address definition in the table, the firewall will allow those packets form LAN to WAN.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
 - Port Filtering
 - IP Filtering
 - MAC Filtering**
 - Port Forwarding
 - DMZ
 - VPN
- Management
- Reboot

MAC Filtering

Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.

☒ **Enable MAC Filtering (allowed list)**

MAC Address: Comment:

Current Filter Table:

MAC Address	Comment	Select
00:00:03:12:01:02	Client 1	<input type="checkbox"/>
00:00:00:06:06:10	Client 5	<input type="checkbox"/>
00:00:00:10:10:22	Client 13	<input type="checkbox"/>

NAT (Network Address Translation)

NAT is the translation between public IP address and private IP address. While NAT is enabling, you can use port forwarding or DMZ to redirect your common network services. If you want to disable NAT, you can go to Management-Route page to disable it and the functions of DMZ, Port Forwarding will be disabled.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP**
 - LAN Interface
 - WAN Interface
 - Route**
- Firewall
- Management

Routing Setup

This page is used to setup dynamic routing protocol or edit static route entry. Disable the NAT will turn off IP masquerade and the functions of DMZ,Port Forwarding.

3 ☒ **Disable NAT**

IP Forwarding Default Policy:

4

Configuring Port Forwarding (Virtual Server)

This function allows 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 the device's NAT firewall.

Port Forwarding

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

☐ Enable Port Forwarding

IP Address: Protocol: Port Range: - Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
------------------	----------	------------	---------	--------

The most often used port numbers are shown in the following table.

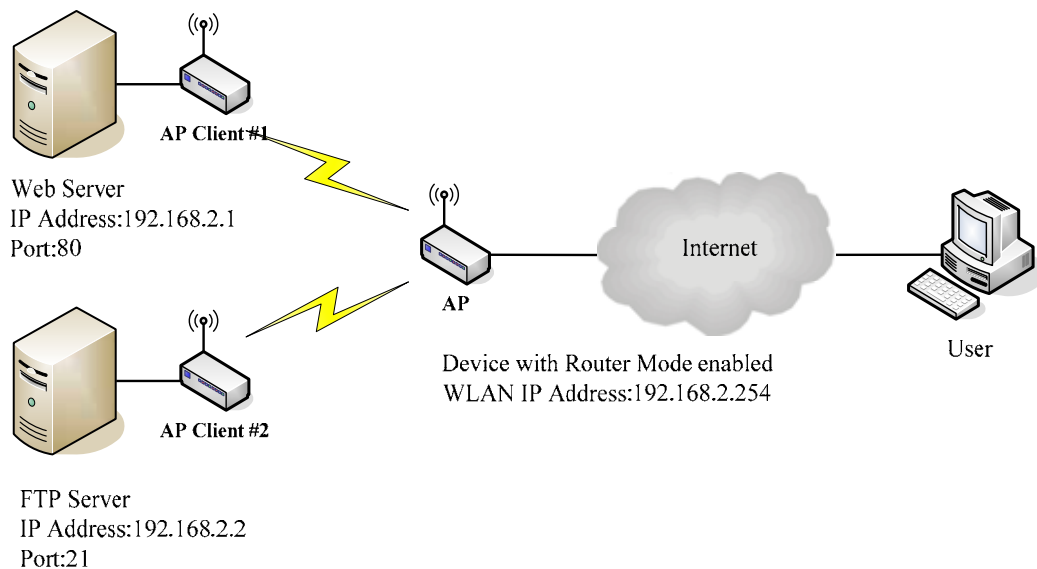
Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer Protocol)	80
POP3 (Post Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
SIP (Session Initiation Protocol)	5060
PPTP (Point-to-Point Tunneling Protocol)	1723

About the other well-known ports, please search in

<http://www.iana.org/assignments/port-numbers>.

Multiple Servers behind NAT Example:

In this case, there are two PCs in the local network accessible for outside users.



Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.2.1	TCP+UDP	80	Web Server	<input type="checkbox"/>
192.168.2.2	TCP+UDP	21	FTP Server	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Configuring 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. So that all inbound packets will be redirected to the computer you set. It also is useful while you run some applications (ex. Internet game) that use uncertain incoming ports.

Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Port Filtering
IP Filtering
MAC Filtering
Port Forwarding
DMZ
VPN
Management
Reboot

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:

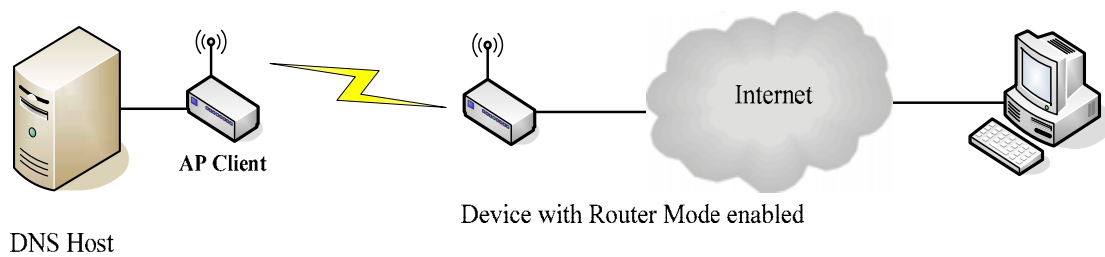
Apply Changes Reset

Enable DMZ:

Enable the "Enable DMZ", and then click "Apply Changes" button to save the changes.

DMZ Host IP Address:

Input the IP Address of the computer that you want to expose to Internet.



Configuring VPN

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
- Port Filtering
- IP Filtering
- MAC Filtering
- Port Forwarding
- DMZ
- VPN**
- Management
- Reboot

VPN Setup

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

☒ **Enable IPSEC VPN**
☒ **Enable NAT Traversal**

Current VPN Connection Table: WAN IP:172.1.1.1

#	Name	Active	Local Address	Remote Address	Remote Gateway	Status
1	-	-	-	-	-	-
2	-	-	-	-	-	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-	-	-	-
10	-	-	-	-	-	-

Enable IPSEC VPN:

Select this check box to enable IPsec VPN.

Enable NAT Traversal:

Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPsec routers. The remote IPsec router must also have NAT traversal enabled.

Generate RSA Key:

Click on this button to generate RSA key.

Show RSA Public Key:

Click on this button to show the RSA public key.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall**
- Port Filtering
- IP Filtering
- MAC Filtering
- Port Forwarding
- DMZ
- VPN**
- Management
- Reboot

VPN Setup

☒ **Enable Tunnel 1**

Connection Name: VPN_1

Auth Type: PSK

Local Site: Subnet Address

Local IP Address/Network: 192.168.2.0

Local Subnet Mask: 255.255.255.0

Remote Site: Subnet Address

Remote Secure Gateway: 172.1.1.2

Remote IP Address/Network: 192.168.1.0

Remote Subnet Mask: 255.255.255.0

Local/Peer ID:

Local ID Type: IP

Local ID:

Remote ID Type: IP

Remote ID:

Key Management: ☒ IKE ☐ Manual

Connection Type: Responder

ESP: 3DES (Encryption Algorithm)

MD5 (Authentication Algorithm)

PreShared Key: 12345

Remote RSA Key:

Status: Disconnected

Enable Tunnel

Select this check box to enable this tunnel.

Connection Name

You can type a name for this connection in this field.

Auth Type

You can select PSK/RSA from drop-down list for this device's Auth Type.

Local Site

You can select Single Address/Subnet Address from drop-down list for this device.

Remote Site

You can select Single Address/Subnet Address/Any Address/NAT-T Any Address from the drop-down list for remote site.

Local ID Type

You can select IP/DNS/Email from the drop-down list to identify this device.

Remote ID Type

You can select IP/DNS/Email from the drop-down list to identify remote site.

Key Management

You can select IKE or Manual for the Key Management. IKE is selected by default.

Connection Type

Select Initiator/Responder from the drop-down list for this device's Connection Type.

ESP

Encapsulating Security Payload Protocol.

Encryption Algorithm

Select 3DES/AES128/NULL from the drop-down list for the

Authentication

Algorithm

device's encryption algorithm.

Select MD5 or SHA1 from the drop-down list for this devices' authentication algorithm.

Configuring WAN Interface

The device supports four kinds of IP configuration for WAN interface, including Static IP, DHCP Client, PPPoE and PPTP. You can select one of the WAN Access Types depend on your ISP required. The default WAN Access Type is "Static IP".

Site contents:

- Wizard
- Operation Mode
- Wireless
- LAN Interface
- WAN Interface**
- Route
- Firewall
- Management
- Reboot

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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

☐ Enable uPnP

☒ 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

Static IP

You can get the IP configuration data of Static-IP from your ISP. And you will need to fill the fields of IP address, subnet mask, gateway address, and one of the DNS addresses.

Site contents:

- Wizard
- Operation Mode
- Wireless
- LAN Interface
- WAN Interface**
- Route
- Firewall
- Management
- Reboot

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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

☐ Enable uPnP
☒ 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

IP Address:	The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.
Subnet Mask:	The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
Default Gateway:	The IP address of Default Gateway provided by your ISP or MIS. Default Gateway is the intermediate network device that has knowledge of the network IDs of the other networks in the Wide Area Network, so it can forward the packets to other gateways until they are delivered to the one connected to the specified destination.
DNS 1~3:	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address:	Clone device MAC address to the specify MAC address required by your ISP
Enable uPnP:	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

DHCP Client (Dynamic IP)

All IP configuration data besides DNS will obtain from the DHCP server when DHCP-Client WAN Access Type is selected.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP**
 - LAN Interface
 - WAN Interface**
 - Route
- Firewall
- Management
- Reboot

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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

☐ Attain DNS Automatically
☒ Set DNS Manually

DNS 1:
 DNS 2:
 DNS 3:

Clone MAC Address:

☐ Enable uPnP
☒ 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

DNS1~3:

The IP addresses of DNS provided by your ISP.

DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

Clone MAC Address:

Clone device MAC address to the specify MAC address required by your ISP

Enable uPnP:

Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

PPPoE

When the PPPoE (Point to Point Protocol over Ethernet) WAN Access Type is selected, you must fill the fields of User Name, Password provided by your ISP. The IP configuration will be done when the device successfully authenticates with your ISP.

The screenshot displays the WAN configuration page. On the left, a sidebar lists site contents including Wizard, Operation Mode, Wireless, LAN Interface, WAN Interface (selected), Route, Firewall, Management, and Reboot. The main configuration area includes:

- WAN Access Type:** A dropdown menu set to 'PPPoE'.
- User Name:** and **Password:** text input fields.
- Connection Type:** A dropdown menu set to 'Continuous', with 'Connect' and 'Disconnect' buttons.
- Idle Time:** A text input field set to '5', with a note '(1-1000 minutes)'.
- MTU Size:** A text input field set to '1412', with a note '(1400-1492 bytes)'.
- DNS Settings:** Radio buttons for 'Attain DNS Automatically' and 'Set DNS Manually' (selected). Below are three text input fields for DNS 1, DNS 2, and DNS 3.
- Clone MAC Address:** A text input field containing '000000000000'.
- Checkboxes:** 'Enable uPnP', 'Enable Web Server Access on WAN' (checked), 'Enable IPsec pass through on VPN connection', 'Enable PPTP pass through on VPN connection', and 'Enable L2TP pass through on VPN connection'.
- Buttons:** 'Apply Changes' and 'Reset' at the bottom.

- User Name:** The account provided by your ISP
- Password:** The password for your account.
- Connect Type:** “Continuous “ : connect to ISP permanently.
 “Manual” : Manual connect/disconnect to ISP.
 “On-Demand”: Automatically connect to ISP when user needs to access the Internet.
- Idle Time:** The number of inactivity minutes to disconnect from ISP. This setting is only available when “Connect on Demand” connection type is selected.
- MTU Size:** Maximum Transmission Unit, 1412 is the default setting; you may need to change the MTU for optimal performance with your specific ISP.
- DNS1~3:** The IP addresses of DNS provided by your ISP.
 DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
- Clone MAC Address:** Clone device MAC address to the specify MAC address required by your ISP.
- Enable UPnP:** Enable UPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.

IP Address:	The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.
Subnet Mask:	The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
Server IP Address: (Default Gateway)	The IP address of PPTP server
User Name:	The account provided by your ISP
Password:	The password of your account
MTU Size:	Maximum Transmission Unit, 1412 is the default setting, you may need to change the MTU for optimal performance with your specific ISP.
DNS1~3:	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address:	Clone device MAC address to the specify MAC address required by your ISP.
Enable uPnP:	Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

Configuring Clone MAC Address

The device provides MAC address clone feature to fit the requirement of some ISP need to specify the client MAC address.

Physical WAN interface MAC Address clone

1. Clone MAC address for Static IP WAN access type

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface**
 - Route
- Firewall
- Management
- Reboot

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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 001122334455

☐ Enable uPnP

☒ 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

2. Clone MAC address for DHCP Client WAN access type

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface**
 - Route
- Firewall
- Management
- Reboot

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 Client, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

☐ Attain DNS Automatically

☒ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 001122334455

☐ Enable uPnP

☒ 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

3. Clone MAC address for PPPoE WAN access type

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
- Route
- Firewall
- Management
- Reboot

WAN Access Type: PPPoE

User Name: 87043609@hinet.net

Password:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1412 (1400-1492 bytes)

☐ Attain DNS Automatically

☒ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 001122334455

☐ Enable uPnP

☒ 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

4. Clone MAC address for PPTP WAN access type

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
- Route
- Firewall
- Management
- Reboot

WAN Access Type: PPTP

IP Address: 172.1.1.2

Subnet Mask: 255.255.255.0

Server IP Address: 172.1.1.1

User Name:

Password:

MTU Size: 1412 (1400-1492 bytes)

MPPE: ☒ Enabled ☐ Disabled

☐ Attain DNS Automatically

☒ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 001122334455

☐ Enable uPnP

☒ 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

5. Physical LAN interface MAC address clone

The screenshot shows the 'LAN Interface Setup' page in a web interface. On the left is a 'Site contents' tree with 'LAN Interface' selected and highlighted with a red box. The main area has a title 'LAN Interface Setup' and a description: 'This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..'. The configuration fields are: IP Address (192.168.2.254), Subnet Mask (255.255.255.0), Default Gateway (0.0.0.0), DHCP (Server dropdown), DHCP Client Range (192.168.2.100 - 192.168.2.200 with a 'Show Client' button), 802.1d Spanning Tree (Disabled dropdown), Clone MAC Address (001122334455, highlighted with a red box), and MTU Size (1500). At the bottom are 'Apply Changes' and 'Reset' buttons.

Configuring DHCP Server

1. To use the DHCP server inside the device, please make sure there is no other DHCP server existed in the same network as the device.
2. Enable the DHCP Server option and assign the client range of IP addresses as following page.

This screenshot shows the same 'LAN Interface Setup' page, but with the 'DHCP' dropdown menu highlighted by a red box. The 'DHCP' dropdown is now set to 'Server'. The 'Clone MAC Address' field now contains '000000000000'. All other fields and the interface layout remain the same as in the previous screenshot.

3. When the DHCP server is enabled and also the device router mode is enabled then the default gateway for all the DHCP client hosts will set to the IP address of device.

Bandwidth Control

This functionality can control Bandwidth of Up/Downstream

1. Enable Bandwidth Control and then enter Data Rate、 Latency and Burst Packet in the specific field.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management (1)
- Status
- QoS
- Bandwidth Control (2)
- SNMP
- Statistics
- DDNS
- Time Zone
- Log
- Miscellaneous
- Upgrade Firmware
- Save/Reload Setting
- Password
- Reboot

Bandwidth Control Settings

This page is used to configure the networking bandwidth. You can set the upstream and downstream data rate when the device is set to client mode.

3 ☒ Bandwidth Control

Upstream Data Rate: 24000 (16-24000 kbps)

Upstream Latency: 50 (20-1024 ms)

Upstream Burst Packet: 25600 (1600-40000 Bytes)

Downstream Data Rate: 24000 (16-24000 kbps)

Downstream Latency: 50 (20-1024 ms)

Downstream Burst Packet: 25600 (1600-40000 Bytes)

4

Note: Only device on **Client** mode or **WISP** mode this functionality can take effective.

2. Parameter Definition

Label	Description
Upstream Data Rate	Speed of transmit data that from Ethernet interface to Wireless interface.
Upstream Latency	Similar a waiting time the data queuing- time.
Upstream Burst Packet	Similar a buffer the data will into the buffer while the data is transmit or receive.
Downstream Data Rate	Speed of transmit data that from Wireless interface to Ethernet interface.
Downstream Latency	Similar a waiting time the data queuing- time.
Downstream Burst Packet	Similar a buffer the data will into the buffer while the data is transmit or receive.

QoS (Quality of Service)

Filter Priority and IP-ToS have not finished yet and also fine tuning.

QoS allows you to specify some rules, to ensure the quality of service in your network. Such as use Bandwidth Priority concept to allocate bandwidth. This function can be helpful in shaping and queuing traffic from LAN (WLAN) to WAN or LAN to WLAN, but not WLAN to WLAN.

Enable the QoS and then fill in Bandwidth Ratio (H/M/L) the device has three Bandwidth Priorities High, Medium and Low user can allocation Bandwidth to these and default is High:50%, Medium:30% and Low:20%.

QoS setting

Entries in this table are used to restrict certain quality of service for your network. Use of such setting can be helpful in traffic control or queuing discipline of your network. The traffic control among WLAN stations is futile, it works between LAN(WLAN)/WAN or LAN/WLAN. The default queue is Med and once the bandwidth borrowed is enabled, the higher bandwidth priority will get the remaining bandwidth first.

☒ **QoS Enabled**

☒ **Bandwidth Borrowed**

Max Throughput : (kbps)

Bandwidth Ratio (H/M/L): : : (%)

The following table describes the priorities that you can apply to bandwidth.

Priority Level	Description
High	Typically used for voice or video applications that is especially sensitive to the variations in delay.
Medium	Typically used for important traffic that can tolerate some delay.
Low	Typically used for non-critical traffic such as a large number of transfers but that should not affect other application.

Click the **QoS** link under **Management** to open the QoS Setting page. This page is divided into three parts: basic settings, QoS rule settings, and current QoS setting table.

1. Enable QoS and enter Max Throughput (default 20Mbps) 、Bandwidth Ratio (default H:50%, M:30%, L:20%)

☒ **QoS Enabled**

☒ **Bandwidth Borrowed**

Max Throughput : (kbps)





Bandwidth Ratio (H/M/L): : : (%)

The following table describes the labels in this part.

Label	Description
QoS Enabled	Select this check box to enable quality of service.
Bandwidth Borrowed	Select this check box to allow a rule to borrow unused bandwidth. Bandwidth borrowing is decided by priority of the rules. Higher priority will get the remaining bandwidth first.
Max Throughput	Enter the value of max throughput in kbps that you

	want to allocate for one rule. The value should be between 1200 kbps and 24000 kbps.
Bandwidth Ratio (H/M/L)	You can specify the ratio of priority in these fields. The range from 1 to 99. The High priority's ratio should be higher than Medium priority's ratio and Medium priority's ratio should be higher than Low priority's ratio.
Apply Changes	Click this button to save and apply your settings.

2. QoS Rule settings

Source IP Address :
Source Netmask :
Destination IP Address :
Destination Netmask :
Source MAC Address :
Destination MAC Address :
Source Port / range: to
Destination Port / range: to
Protocol: 
Bandwidth Priority: 
Filter Priority:  (Lower number, Higher Priority)
IP TOS Set: 

The following table describes the labels in this part.

Label	Description
IP Address	Enter source/destination IP Address in dotted decimal notation.
Netmask	Once the source/destination IP Address is entered, the subnet mask address must be filled in this field.
MAC Address	Enter source/destination MAC Address.
Port / range	You can enter specific port number or port range of the source/destination
Protocol	Select a protocol from the drop down list box. Choose TCP/UDP , TCP or UDP .
Bandwidth Priority	Select a bandwidth priority from the drop down list box. Choose Low , Medium or High .
Filter Priority	Select a filter priority number from the drop down list box. Lower number gets higher priority while

	two rules have the same bandwidth priority.
IP TOS Set	Select an IP type-of-service value from the drop down list box. Choose Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, or Minimize Delay.
Apply Changes	Click this button to save and apply your settings.
Reset	Click this button to begin re-input the parameters.

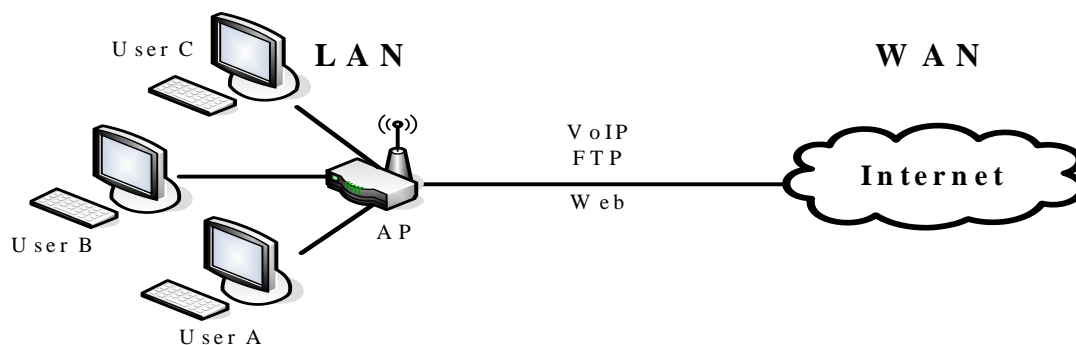
Current QoS setting table

In this part, you can see how many rules have been specified. And you can see the detail about the rules and manage the rules. This table can input 50 rules at most.

Current QoS Setting:
(Mask 255.255.255.255 means single host)

Src Addr	Dst Addr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	140.113.27.181/24	00:05:9e:80:aa:ee	-	21-21	21-21	TCP	LOW	0	Normal	<input type="checkbox"/>
anywhere	anywhere	-	-	80-80	-	TCP/UDP	MED	0	Normal	<input type="checkbox"/>
192.168.2.13/24	anywhere	-	-	50000-50050	-	TCP/UDP	LOW	2	Normal	<input type="checkbox"/>
anywhere	192.168.2.12/24	-	-	-	-	TCP/UDP	MED	1	Normal	<input type="checkbox"/>
192.168.2.15/24	anywhere	00:05:9e:80:aa:cc	-	-	-	TCP/UDP	HIGH	0	Normal	<input type="checkbox"/>

An example for usage



For example, there are three users in your network.

- User A wants to **browse the websites** to retrieve information.
- User B wants to use **FTP** connection to download a large file.
- User C wants to use **software phone** to connect with customer.

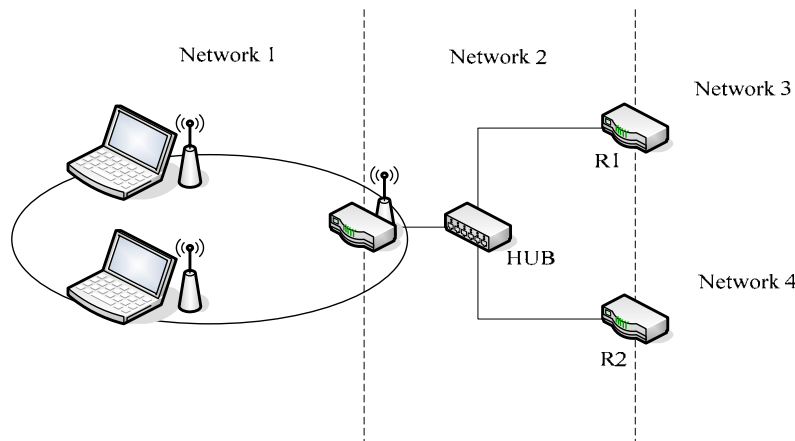
The voice is sensitive to the variations in delay; you can set **High** priority for **User C**. The FTP transmission may take a long time; you can set **Low** priority for **User B**.

Current QoS Setting:
(Mask 255.255.255.255 means single host)

Src Addr	Dst Addr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	anywhere	-	-	5060-5061	-	TCP/UDP	HIGH	0	Normal	<input type="checkbox"/>
192.168.2.12/24	anywhere	-	-	21-21	-	TCP	LOW	0	Normal	<input type="checkbox"/>
192.168.2.13/24	anywhere	-	-	80-80	-	TCP	MED	0	Normal	<input type="checkbox"/>

Static Route Setup

User can set the routing information let the Router knows what routing is correct also it can not learn automatically through other means.



For example, if user wants to link the Network 3 and Network 4 separately from Network 1 that Routing Table configuration as below:

1. Enable Static Route in Route Setup of TCP/IP page and then enter IP Address of Network 3, Subnet Mask and IP Address of Router (R1) in Default Gateway field final click Apply Change button.

☒ Enable Static Route

IP Address:

Subnet Mask:

Default Gateway:

2. Enter IP Address of Network 4, Subnet Mask and IP Address of Router (R2) in Default Gateway field final click Apply Change button.

☒ Enable Static Route

IP Address:

Subnet Mask:

Default Gateway:

3. In Static Route Table there have two routings for Network 3 and Network 4

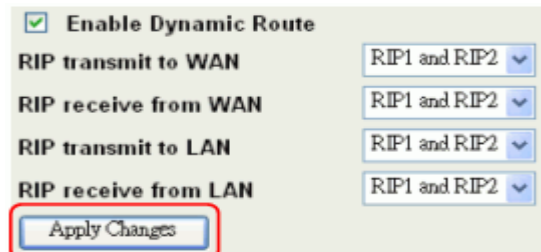
Static Route Table:

Destination IP Address	Netmask	Gateway	Select
192.168.3.0	255.255.255.0	192.168.2.1	<input type="checkbox"/>
192.168.4.0	255.255.255.0	192.168.2.2	<input type="checkbox"/>

Dynamic Route Setup

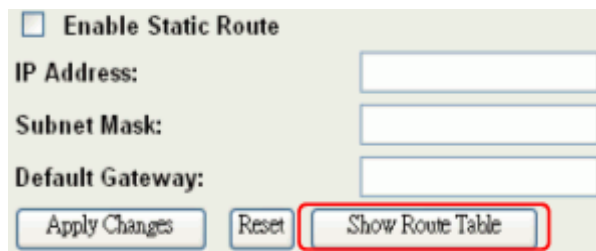
The Dynamic Route utilizes RIP1/2 to transmit and receive the route information with other Routers.

1. Enable Dynamic Route and then select RIP 1、RIP2 or Both to transmit/receive packets final click Apply Change button.



The image shows a configuration window for Dynamic Route. It has a checkbox labeled 'Enable Dynamic Route' which is checked. Below it are four dropdown menus: 'RIP transmit to WAN', 'RIP receive from WAN', 'RIP transmit to LAN', and 'RIP receive from LAN'. All four dropdown menus are set to 'RIP1 and RIP2'. At the bottom, there is a button labeled 'Apply Changes' which is highlighted with a red rectangle.

2. Click Show Route Table button to show Dynamic Route Table.



The image shows a configuration window for Static Route. It has a checkbox labeled 'Enable Static Route' which is unchecked. Below it are three input fields: 'IP Address:', 'Subnet Mask:', and 'Default Gateway:'. At the bottom, there are three buttons: 'Apply Changes', 'Reset', and 'Show Route Table'. The 'Show Route Table' button is highlighted with a red rectangle.

3. In Dynamic Routing Table there have two routings for Network 3 and Network 4

Routing Table

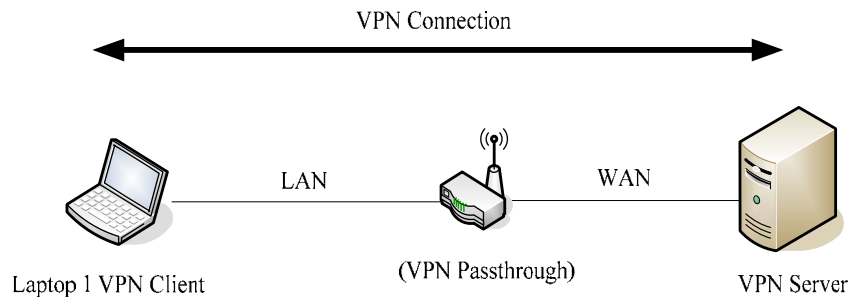
This table shows the all routing entry .

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
255.255.255.255	0.0.0.0	255.255.255.255	UH	0	0	0	br0
192.168.4.0	192.168.2.2	255.255.255.0	UG	2	0	0	br0
192.168.3.0	192.168.2.1	255.255.255.0	UG	2	0	0	br0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
172.1.1.0	0.0.0.0	255.255.255.0	U	0	0	0	wlan0
0.0.0.0	172.1.1.254	0.0.0.0	UG	0	0	0	wlan0

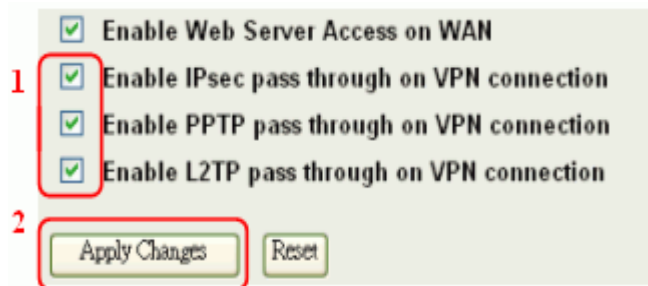
Refresh Close

VPN Pass-through

This functionality let the device can Pass-through the VPN packets including PPTP/ L2TP/IPsec VPN Connection.



1. Check the VPN Pass-through in WAN Interface of TCP/IP Page that you want and then click Apply Changes button.



Using CLI Menu

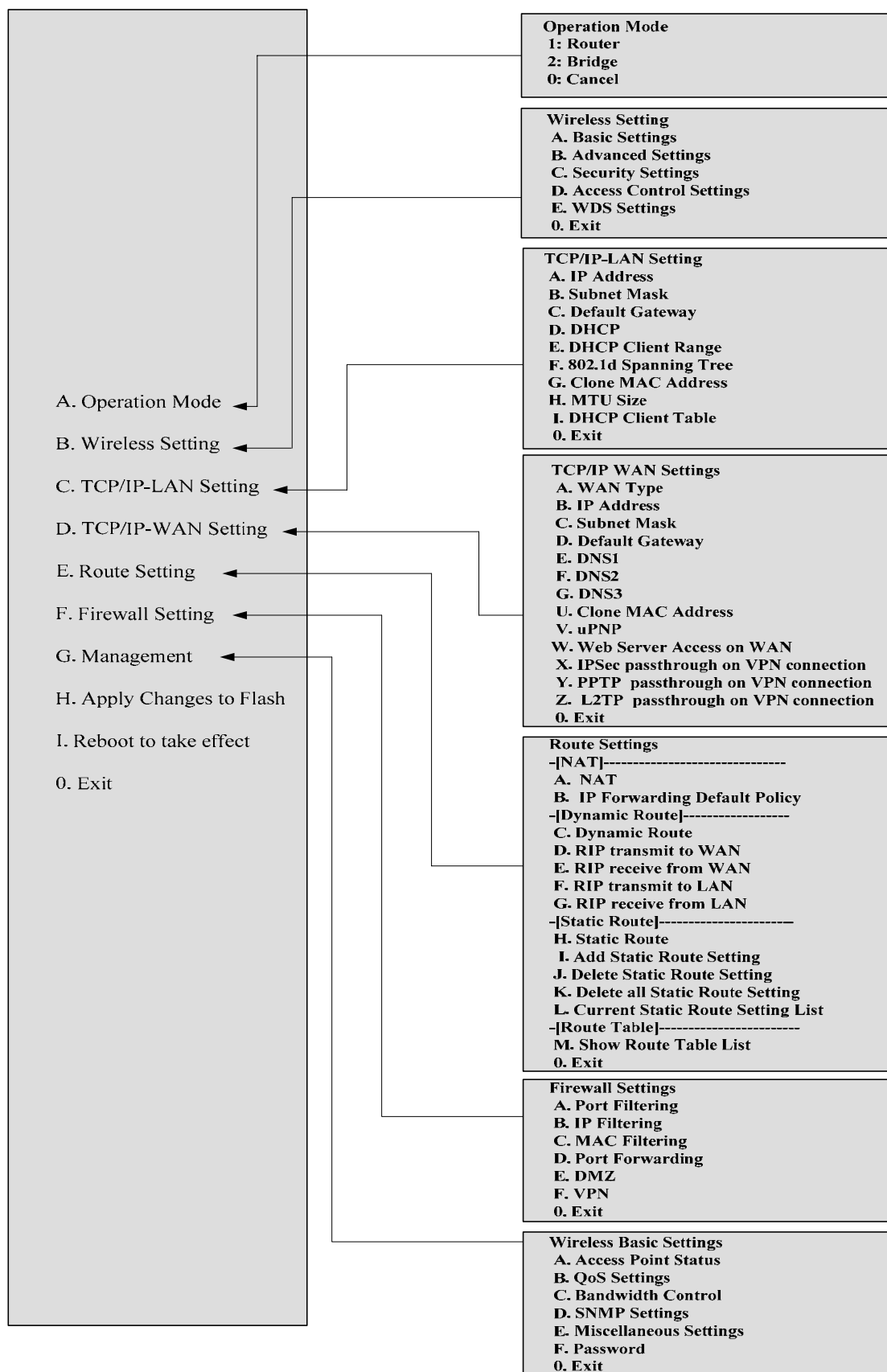
Start a SSH(Secure Shell) client session to login the device

The SSH server daemon inside device uses well-known TCP port 22. User must use SSH client utility such like Putty to login the device. The default password for user “root” is “qwerty”, once user login the device then can change the password by CLI command.

Execute CLI program

This program won't execute automatically when user login the device. User must manually execute it by typing the case-sensitive command “cli”. Please note that any modified settings won't save permanently until user “Apply Changes to Flash” or reboot it. The new settings modified by CLI will take effect after rebooting the device.

Menu Tree List



The System Management

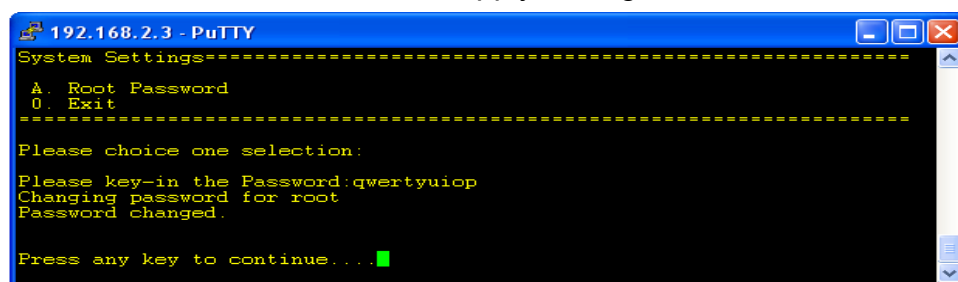
Password Protection

Both Web-Browser and SSH configuration interfaces have password protection.



The screenshot shows a web browser interface for 'Password Setup'. On the left is a navigation menu with items like Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management (highlighted), Status, QoS, Bandwidth Control, SNMP, Statistics, DDNS, Time Zone, Log, Miscellaneous, Upgrade Firmware, Save/Reload Setting, Password, and Reboot. The main content area is titled 'Password Setup' and contains a text box explaining its purpose: '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.' Below this are three input fields: 'User Name:', 'New Password:', and 'Confirmed Password:'. At the bottom are two buttons: 'Apply Changes' and 'Reset'.

To disable the Web-Browser password protection just leave the “User Name” field to blank then click “Apply Changes” button.



To change the password of user “root” for SSH session, please use the CLI menu item G. Management→F. Password

SNMP Agent

This device is compatible with SNMP v1/v2c and provides standard MIB II. Currently only the “public” community string is available and the modified settings by SNMP SET request will be lost after rebooting the device.

1. Enable SNMP and then enter IP Address of SNMP Manager in Trap Receiver IP Address field and Community String in System Community String field. Final click Apply Changes button.

SNMP Settings

This page is used to configure the SNMP settings. You can get some of the system information via setting the SNMP network protocol.

3 ☒ **SNMP Enabled**

System Community String: public

System Name: last

System Location: 1F

System Contact: MIKE

4 Trap Receiver IP Address1: 192.168.2.11

Address1 Community String: MIKE

Trap Receiver IP Address2:

Address2 Community String:

Trap Receiver IP Address3:

Address3 Community String:

5

2. Following Table describes the SNMP configuration parameter

Label	Description
System Community String	This is password sent with each trap to the SNMP Manager.
System Name	Type the Name which is name of device.
System Location	Type the Location which is location of device
System Contact	Type the Name which is person or group when the device has problem can find they.
Trap Receiver IP Address	Type the IP Address which is address of SNMP Manager.
Trap Receiver Community String	This is password receive with trap from the device (SNMP Agent).

3. SNMP Traps

Traps	Description
coldStart(0)	The trap from device after reboot the device
linkDown(2)	The trap is sent when any of the links are down. See the following table.
linkup(3)	The trap is sent when any of the links are UP. See the following table.
authenticationFailure(4)	The trap is sent when the device receiving gets or sets requirement with wrong community.

4. Private MIBs

OID	Description
-----	-------------

1.3.6.1.4.1.99.1	Mode, Operation Mode in device.
1.3.6.1.4.1.99.2	SSID, SSID of the device
1.3.6.1.4.1.99.3	Channel, Channel of the device in WLAN
1.3.6.1.4.1.99.4	Band, 802.11g / 802.11b only
1.3.6.1.4.1.99.5	RSSI, Receive Signal Strength Index (Support AP and Client RSSI)
1.3.6.1.4.1.99.6	Active_Clients, The number of associate clients
1.3.6.1.4.1.99.7	Active_Clients_List, Client's Information (MAC Address, Data Rate, RSSI...etc)
1.3.6.1.4.1.99.8	Encryption, Encryption type of device in Wireless Network

1.3.6.1.4.1.99.1 - Mode

.1.3.6.1.4.1.99.1.2.1	MODE
.1.3.6.1.4.1.99.1.3.1	/bin/flash snmpget MODE
.1.3.6.1.4.1.99.1.100.1	0
.1.3.6.1.4.1.99.1.101.1	AP - Bridge

1.3.6.1.4.1.99.2 - SSID

.1.3.6.1.4.1.99.2.2.1	SSID
.1.3.6.1.4.1.99.2.3.1	/bin/flash snmpget SSID
.1.3.6.1.4.1.99.2.100.1	0
.1.3.6.1.4.1.99.2.101.1	hank

1.3.6.1.4.1.99.3 - Channel

.1.3.6.1.4.1.99.3.1.1	1
.1.3.6.1.4.1.99.3.2.1	CHANNEL
.1.3.6.1.4.1.99.3.3.1	/bin/flash snmpget CHANNEL
.1.3.6.1.4.1.99.3.100.1	0
.1.3.6.1.4.1.99.3.101.1	11

1.3.6.1.4.1.99.4 - Band

.1.3.6.1.4.1.99.4.2.1	BAND
.1.3.6.1.4.1.99.4.3.1	/bin/flash snmpget BAND
.1.3.6.1.4.1.99.4.100.1	0
.1.3.6.1.4.1.99.4.101.1	802.11bg

1.3.6.1.4.1.99.5 - RSSI

.1.3.6.1.4.1.99.5.2.1	RSSI
.1.3.6.1.4.1.99.5.3.1	/bin/flash snmpget RSSI
.1.3.6.1.4.1.99.5.100.1	0
.1.3.6.1.4.1.99.5.101.1	100

1.3.6.1.4.1.99.6 - Active_Clients

.1.3.6.1.4.1.99.6.2.1	ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.3.1	/bin/flash snmpget ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.100.1	0
.1.3.6.1.4.1.99.6.101.1	1

1.3.6.1.4.1.99.7 - Active_Clients_List

.1.3.6.1.4.1.99.7.2.1	ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.3.1	/bin/flash snmpget ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.100.1	0 MAC Data Rate RSSI
.1.3.6.1.4.1.99.7.101.1	00:13:02:03:51:5e 102,125 54 no,300 57(-55 dbm)

1.3.6.1.4.1.99.8 - Encryption

.1.3.6.1.4.1.99.8.2.1	ENCRYPTION
.1.3.6.1.4.1.99.8.3.1	/bin/flash snmpget ENCRYPTION
.1.3.6.1.4.1.99.8.100.1	0 AP-WEP
.1.3.6.1.4.1.99.8.101.1	WEP(AP),Disabled(WDS)

Miscellaneous Settings

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management**
 - Status
 - QoS
 - Bandwidth Control
 - SNMP
 - Statistics
 - DDNS
 - Time Zone
 - Log
 - Miscellaneous**
 - Upgrade Firmware
 - Save/Reload Setting
 - Password
 - Reboot

Miscellaneous Settings

This page is used to configure the miscellaneous settings.

HTTP Port: (1-65535)

RSSI Interval: (30-86400 seconds)

☐ Ping WatchDog Enabled

Target Host IP Address:

Ping Interval: (15-86400 seconds)

Ping Threshold: (1-100 times)

Ping Rebooting Delay: (10-600 seconds)

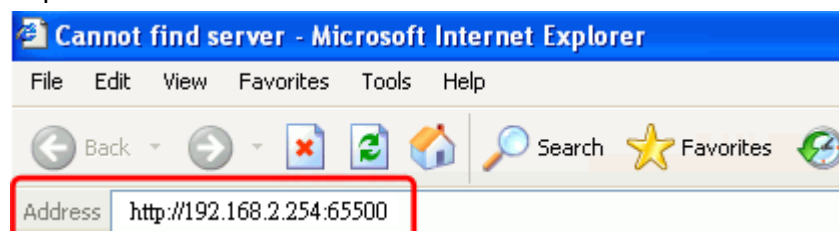
HTTP Port

The default http port is 80. For security concern, you can change the device's http port, to protect this web server from intrusion and attack.

1. Entering the port number you want to change in HTTP PORT field, then click Apply Changes button.

HTTP Port:	<input type="text" value="65500"/>	(1-65535)
RSSI Interval:	<input type="text" value="100"/>	(30-86400 seconds)

2. After apply change, you should re-login the web server. Type `http://192.168.2.254:65500/` in URL field.



RSSI Interval

HTTP Port:	<input type="text" value="80"/>	(1-65535)
RSSI Interval:	<input type="text" value="100"/>	(30-86400 seconds)

Input your RSSI Interval to specify the refresh time of RSSI information. The RSSI information can be found on the page of Wireless Basic Setting, Active Client Table, Wireless Site Survey and Status. Because it has to wait to receive the radio signal, the throughput of this device will be impacted if the interval is too short. The default interval is 100 seconds.

Ping WatchDog

Ping WatchDog Enabled:

Click to enable this function. This device can check its own status by ping another host. When user enable this option, the device perform ping to a specific network host. Once the ping is timeout, it may be caused by its network function crashes, and the device will reboot to fix it.

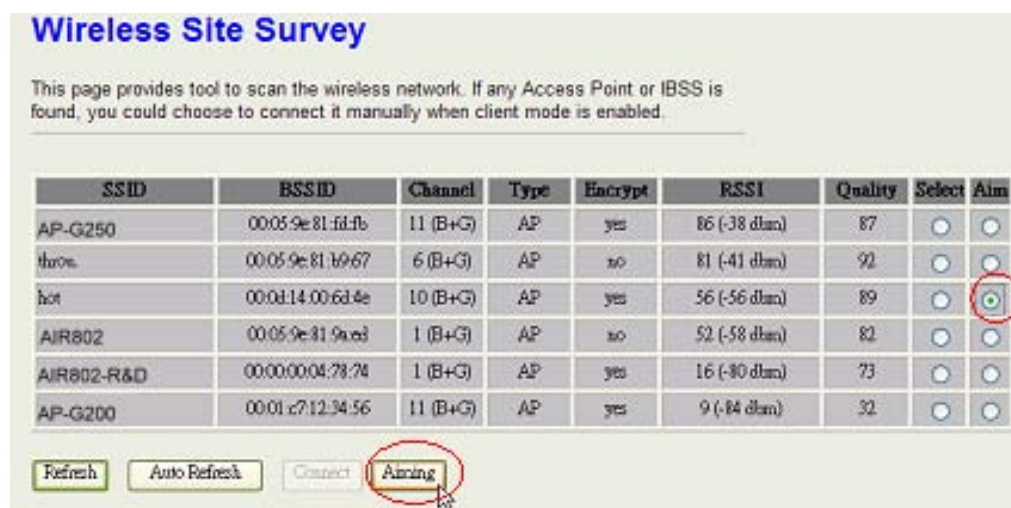
<input checked="" type="checkbox"/> Ping WatchDog Enabled	
Target Host IP Address:	<input type="text" value="192.168.2.254"/>
Ping Interval:	<input type="text" value="100"/> (15-86400 seconds)
Ping Threshold:	<input type="text" value="5"/> (1-100 times)
Ping Rebooting Delay:	<input type="text" value="60"/> (10-600 seconds)
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

Following Table describes the Ping WatchDog configuration parameter

Label	Description
Target Host IP Address	Specify the IP Address of the Network host to ping.
Ping Interval	Specify the waiting time for the next ping. If this time is too short, it will impact the through of this AP. The default value is 100.
Ping Threshold	Specify the Ping-fail times of criteria. If this device ping fails several times continuously, and the fail times meet this criterion, it will perform reboot. The default value is 5.
Ping Rebooting Delay	The time before it starting rebooting. When it meets the Ping Threshold, it will wait for this time and then reboot. The default value is 60.

Aiming Tool

The “Aiming tool” can help the installer of the device to find the best direction targeting the specific Access Point or IBSS. It displays the RSSI of the specify SSID on the Wireless Site Survey page on the web, so the installer can adjust the antenna of this device to find the best position and angle.



When this device is in AP Client mode, the user can click the “Aim” option of one SSID on the list in the Wireless Site Survey page and then click the “Aiming” button.

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	RSSI	Quality
hot	00:0d:14:00:6d:4e	10 (B+G)	AP	yes	58 (-55 dbm)	89

Refresh Stop Aiming

58%

After clicking the “Aiming” button, RSSI will be displayed on the web page. The RSSI information will be refreshed by second. You can adjust the position and the angle of the antenna while the device is aiming.

The RSSI value will change depending on your adjustment, so it is very easy to get a high RSSI by aiming.

To stop the Aiming tool, the user just click “Stop Aiming” button.

*: If you can't get high RSSI through aiming, consider changing a high gain antenna to improvement the RF receives.

Connecting Profile

Connecting Profile Settings

Enable the connecting profile in client mode, the system will check the preferred SSID and BSSID in a fixed period, if preferred APs are found, the radio will try to connect with them one by one and regardless of the signal quality and strength. Please note that check the preferred APs will impact the throughput a lot! Unless the signal strength is good enough, otherwise don't set the interval too short. And currently, all the profiles share the same security setting.

☒ Enable connecting profile

SSID: BSSID:

Apply Changes Reset

Checking Interval: (5-1440 minutes)

Current preferred AP list:

SSID	BSSID	Select
Test AP 1	00:00:00:00:00:00	<input type="checkbox"/>

Delete Selected Delete All Reset

To enable this function, this device must be in the client mode. User clicks to enable this function and input the SSID of preferred AP and then click “Apply Changes”. The BSSID field is an option in case of two preferred APs having the same SSID. In this case, this device will check both SSID and BSSID and connect to the matching AP. We can leave it empty in the normal case.

After enabling the connecting profile, the system will check the preferred SSID in a fixed period, if preferred APs are found; the radio will try to connect with them one by one from top to down of the list and regardless of the signal quality and strength. The users can put their most favorite AP on the top so it will be connected first. Please note that check the preferred APs will impact the throughput a lot! Unless the signal strength is good enough, otherwise don't set the interval too short. The default value is 10 minutes. And currently, all the profiles share the same security setting.

Current preferred AP list:

SSID	BSSID	Select
Test AP 1	00:00:00:00:00:00	<input checked="" type="checkbox"/>
Device AP 1	00:00:00:00:00:00	<input type="checkbox"/>

To delete one SSID in the list, users click the square to select it and click “Delete Selected” and then click “OK” in the pop-up window to confirm it. The user can delete the whole list once for all! Just click “Delete All” and then click “OK” in the pop-up window to confirm it.

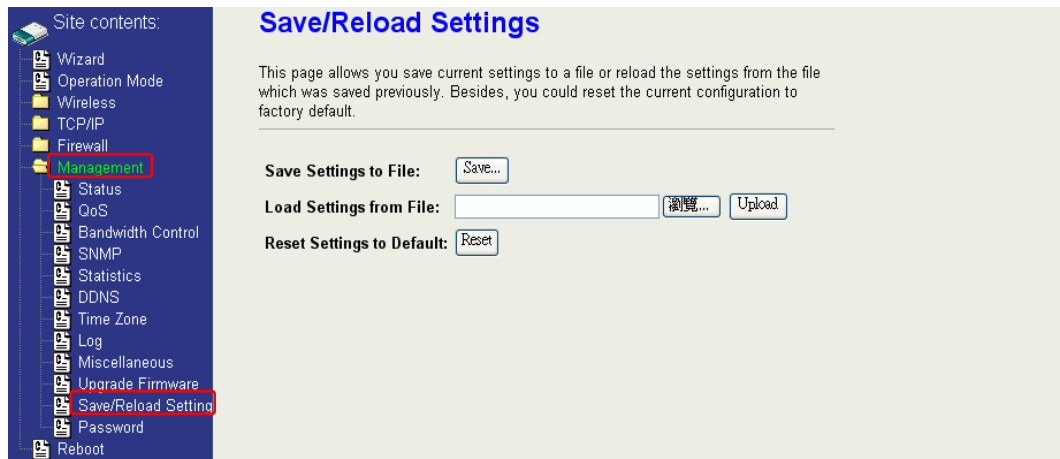
To simply disable this function, the user just clicks to disable “Enable connecting profile”. The preferred AP list will be preserved for the next use.

Configuration Data Backup & Restore

Reset Setting to Factory Default Value

Since the device is designed for outdoor used, there is no interface outside the housing to reset the configuration value to the factory default value. The device provides the Web-Browser interface to rest the configuration data. After resetting it, the current configuration data will be lost and restored to factory default value.

Saving & Restoring Configuration Data



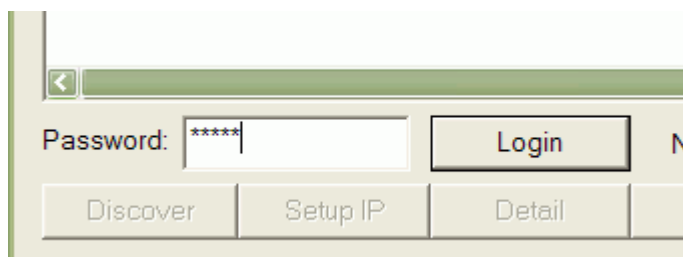
To save & restore configuration data of device, just assign the target filename with full path at your local host, then you can backup configuration data to local host or restore configuration data to the device.

Auto Discovery Tool

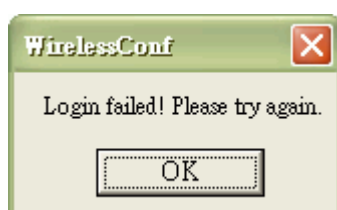
User can use this tool to find out how many devices in your local area network. The name of tool is WirelessConf.exe it in the packing CD.

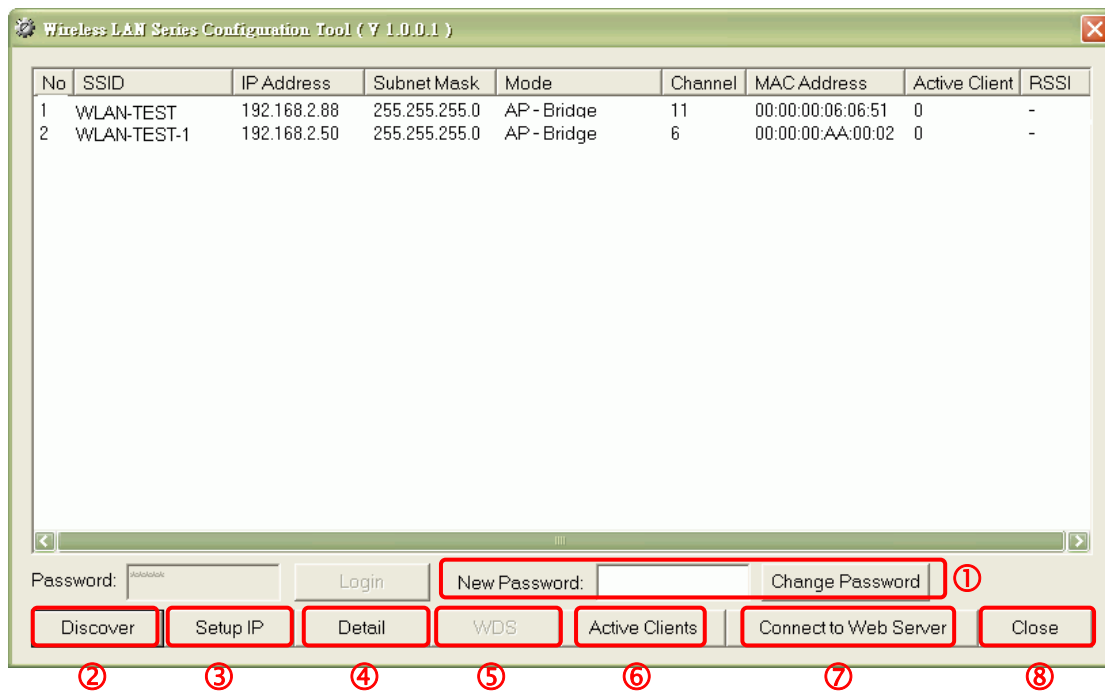
Login:

When the user opens this Auto Discovery tool, the login password must be inputted. The default password is “qwerty”. After inputting the password, click “Login” button to open the tool.



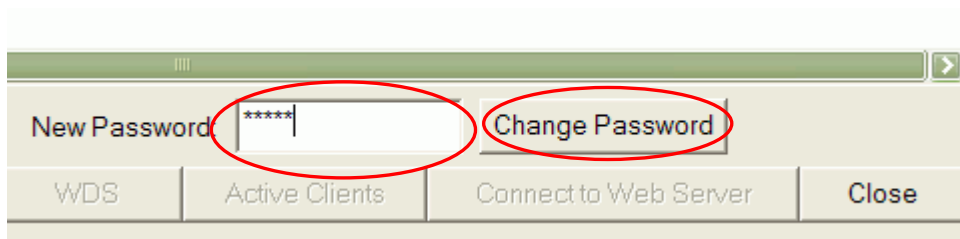
If the user doesn't input the password or input a wrong password, he can't login the tool and see the alert window.



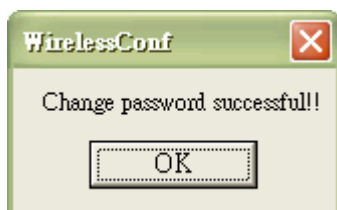


1. Change Password

The user can change the default login password. Just enter new password after login this tool and click “Change Password” button.



The pop-up window shows that the password has been successfully changed.



2. Discover

After press this button, you could see there are how many devices in your network. And you would see the basic information about these devices, such as:

- **SSID**
- **IP Address**
- **Subnet Mask**
- **Operation Mode**
- **Channel number**

- **MAC Address**
- **Active Client:** this field shows how many clients associated with the device
- **RSSI:** this field shows Recieved Signal Strength Indication while device is on AP-Client mode

3. Setup IP

After you press the **Setup IP** button, you would see **Setup IP Address** window. You could change device's IP Address, Netmask, and Default Gateway in this window. But if the device's web server needs User Name and Password to login, you should fill in these two fields and then apply changes.

4. Detail

If you want to see more detailed information, you could press the **Detail** button, and then you would see the **Detail Information** window.

Detail

System Name:	MIKE
System Location:	1F
System Contact:	MIKE
Firmware Version:	
Mode:	AP - Bridge
Band:	802.11bg
TXPowerLevel:	OFDM 100mW / CCK 250mW
Upstream Data Rate:	24000 kbps
Upstream Latency:	50 ms
Upstream Burst Packet:	25600 Bytes
Downstream Data Rate:	24000 kbps
Downstream Latency:	50 ms
Downstream Burst Packet:	25600 Bytes
Encryption:	Disabled(AP), Disabled(WDS)

Close

5. WDS

If the device you selected is on WDS mode or AP+WDS mode, you could press **WDS** button, and then you would see the **WDS List** window.

WDS List

No	MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
1	00:05:9e:80:aa:11	41	37	0	1
2	00:05:9e:80:aa:22	41	39	0	1
3	00:e0:4c:81:86:21	20	3	633	11

Close

6. Active Clients

After press **Active Clients** button, you would see WLAN AP Active Clients window. In this window, you could see client's information, such as:

WLAN AP Active Clients

No	MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
1	00:05:9e:80:3a:d7	1	90	54	no	298

Close

7. Connect to Web Server

If you want connect to device's web server, you could press this button, or double-click on the device.

8. Close

You could press this button to leave this tool.

9. Reset the password to default password

If the user had changed the login password and forgot it, he can execute "ResetPassword.exe" to reset to the default password. When the password has been reset by this program, the following message window will be prompt on screen. Then the user can use the default password "qwerty" to login the tool.

