Note: Under **AP、WDS and AP+WDS mode**, The Universal Repeater can take effective.

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

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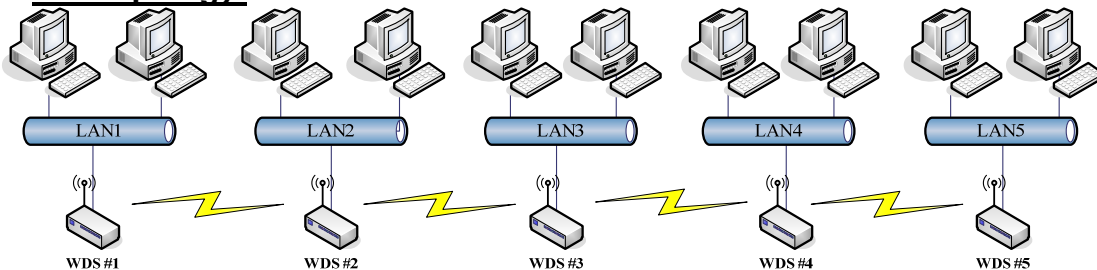
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Address of WDS2	No
WDS2	The MAC Addresses of WDS1 and WDS3	No
WDS3	The MAC Addresses of WDS2 and WDS4	No
WDS4	The MAC Addresses of WDS3 and WDS5	No
WDS5	The MAC Address of WDS4	No

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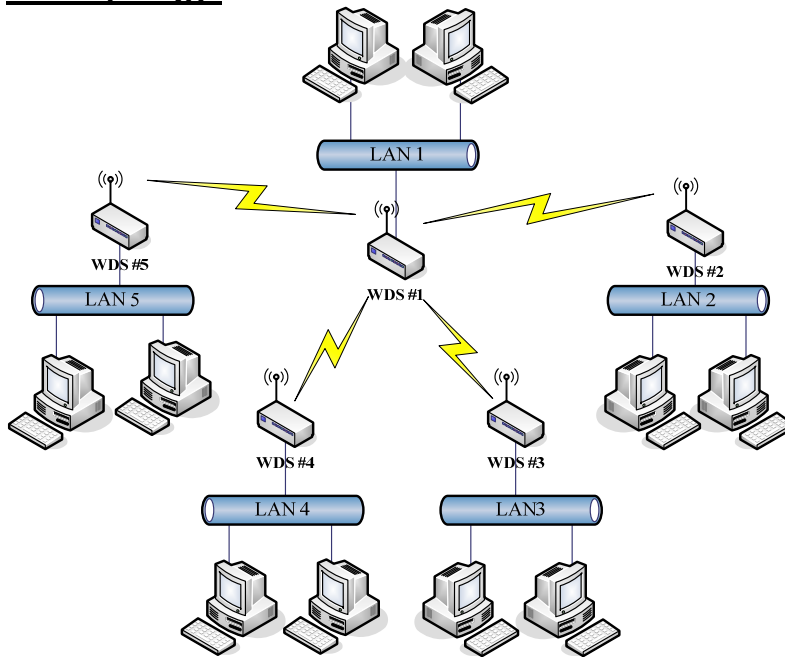
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	No
WDS2	The MAC Address of WDS1	No
WDS3	The MAC Address of WDS1	No
WDS4	The MAC Address of WDS1	No
WDS5	The MAC Address of WDS1	No

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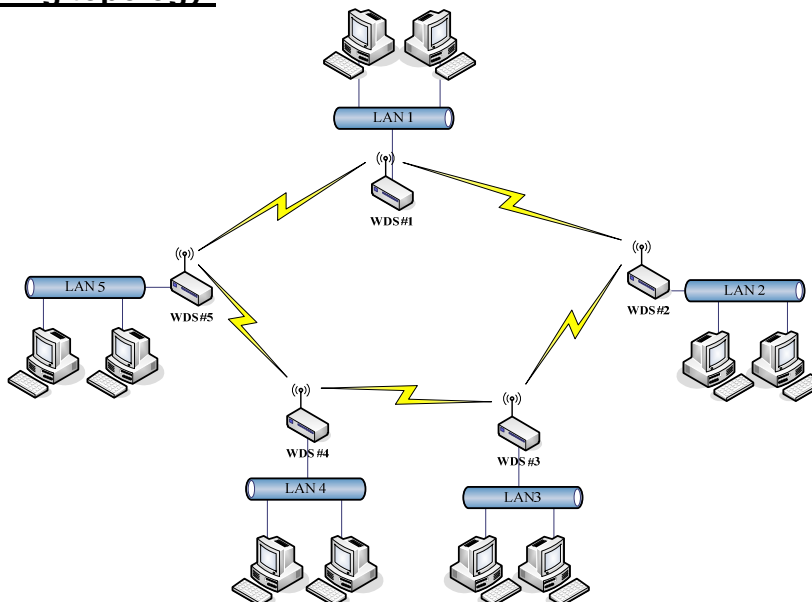
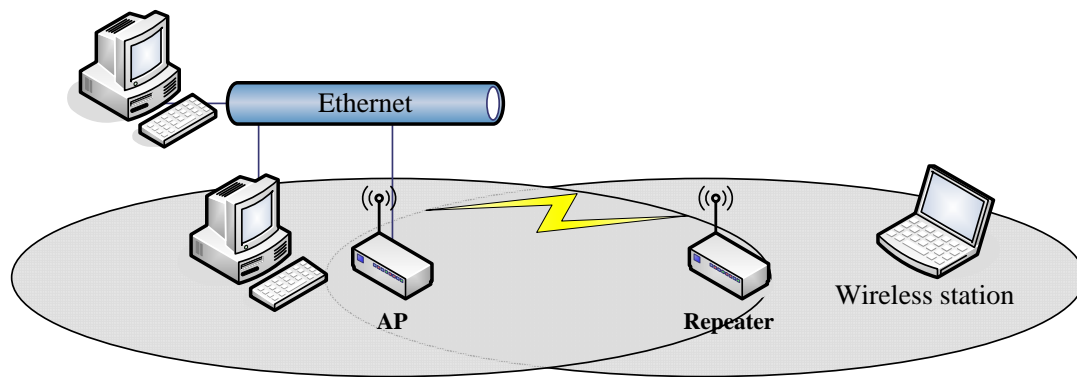| Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2 and WDS5	Yes
WDS2	The MAC Addresses of WDS1 and WDS3	Yes
WDS3	The MAC Addresses of WDS2 and WDS4	Yes
WDS4	The MAC Addresses of WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS4 and WDS1	Yes

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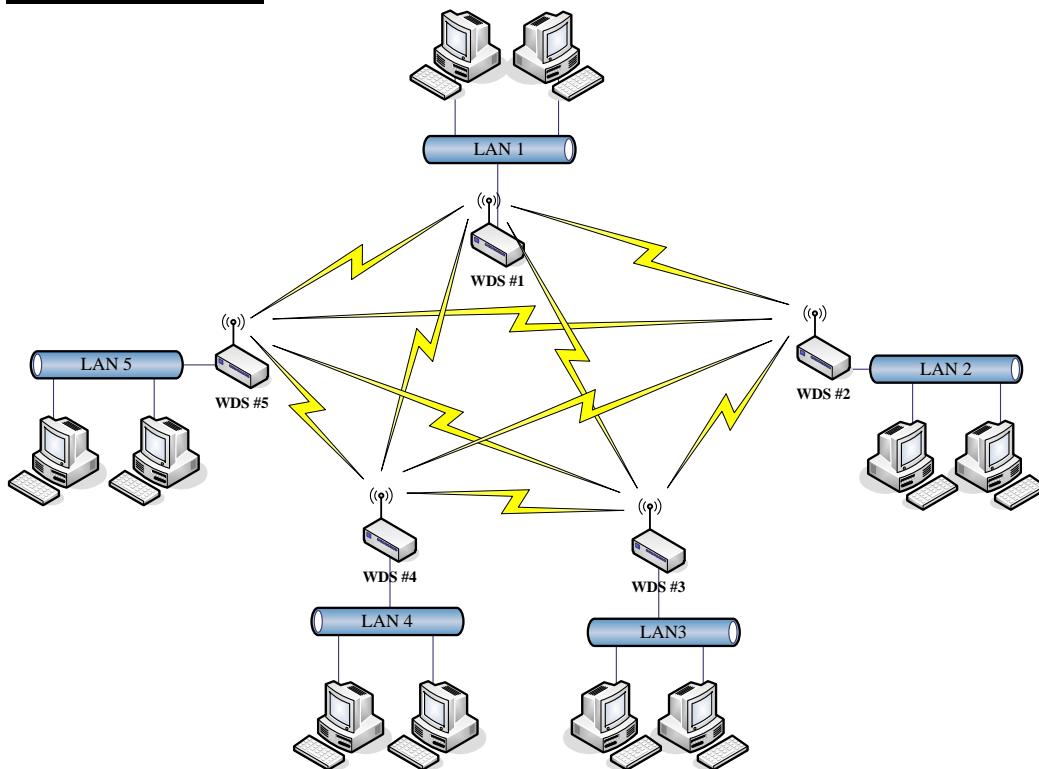
Device	Entries of WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	Yes
WDS2	The MAC Addresses of WDS1, WDS3, WDS4 and WDS5	Yes
WDS3	The MAC Addresses of WDS1, WDS2, WDS4 and WDS5	Yes
WDS4	The MAC Addresses of WDS1, WDS2, WDS3 and WDS5	Yes
WDS5	The MAC Addresses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

WDS Application

Wireless Repeater

Wireless Repeater can be used to increase the coverage area of another device (Parent AP). Between the Parent AP and the Wireless Repeater, wireless stations can move among the coverage areas of both devices. When you decide to use the WDS as a Repeater, 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
Access Point	The MAC Address of Repeater	Yes
Repeater	The MAC Address of Access Point	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.
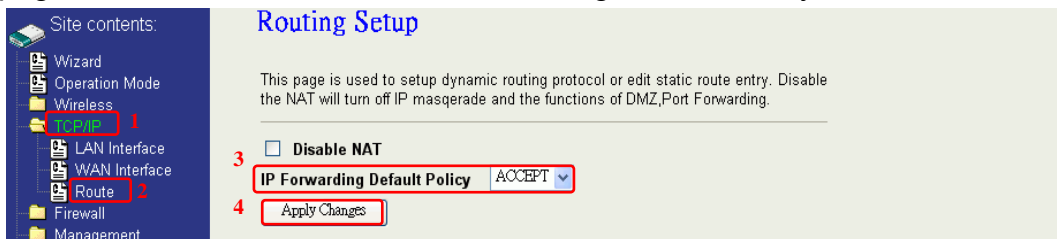
If you want permit some application from LAN to WAN, you can go to Route page to select "DROP" for IP Forwarding Default Policy.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Web Server
IP Address:192.168.2.1
Port:80

AP Client #1

AP Client #2

FTP Server
IP Address:192.168.2.2
Port:21

AP

Internet

User

Device with Router Mode enabled
WLAN IP Address:192.168.2.254
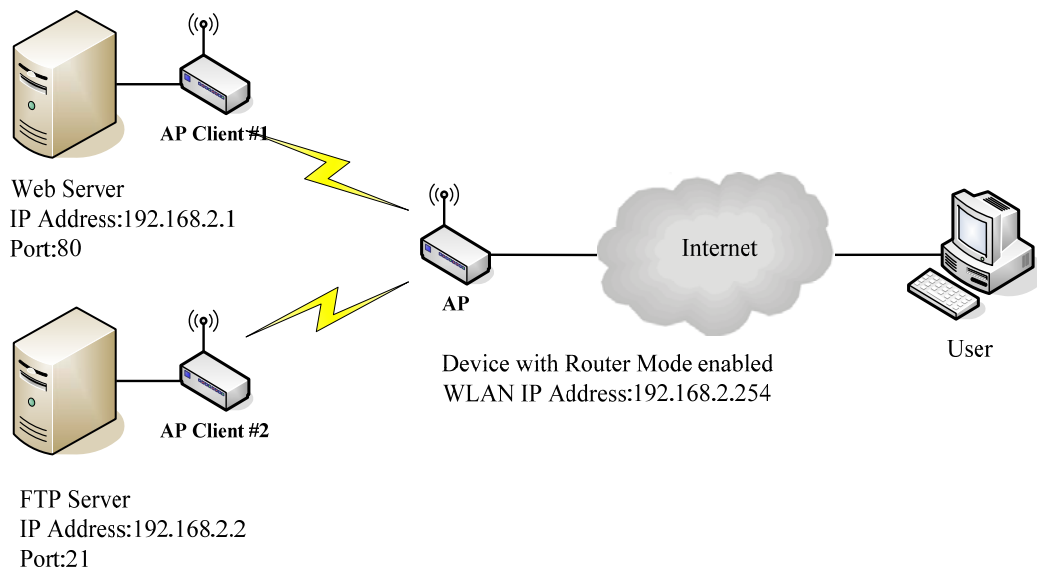
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.2.1	TCP+UDP	80	Web Server	☐
192.168.2.2	TCP+UDP	21	FTP Server	☐

[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.

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.

DNS Host AP Client Internet Device with Router Mode enabled
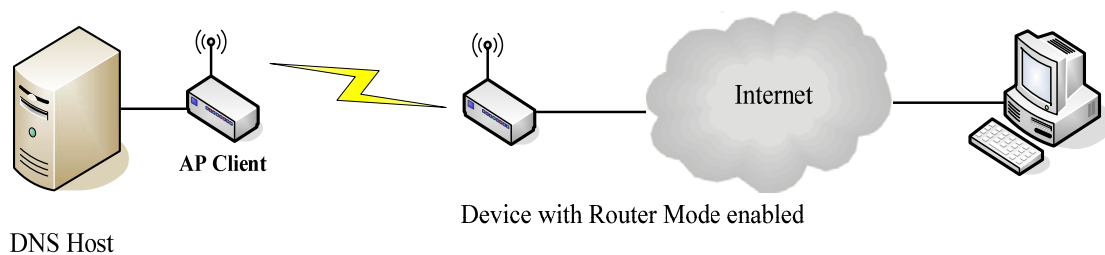
Configuring WAN Interface

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".

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.

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]

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.

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: 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

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.

64

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.

65

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

2. Clone MAC address for DHCP Client WAN access type

3. Clone MAC address for PPPoE WAN access type

4. Clone MAC address for PPTP WAN access type

5. Physical LAN interface MAC address clone

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.

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.

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％.

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%)

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 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 higher than Medium priority's ratio and Medium priority's ratio should 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: [▼]

[Apply Changes] [Reset]

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 Match	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 Adr	Dst Adr	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	☐
anywhere	anywhere	-	-	80-80	-	TCP/UDP	MED	0	Normal	☐
192.168.2.13/24	anywhere	-	-	50000-50050	-	TCP/UDP	LOW	2	Normal	☐
anywhere	192.168.2.12/24	-	-	-	-	TCP/UDP	MED	1	Normal	☐
192.168.2.15/24	anywhere	00:05:9e:80:aa:cc	-	-	-	TCP/UDP	HIGH	0	Normal	☐

[Delete Selected] [Delete All] [Reset]

An example for usage
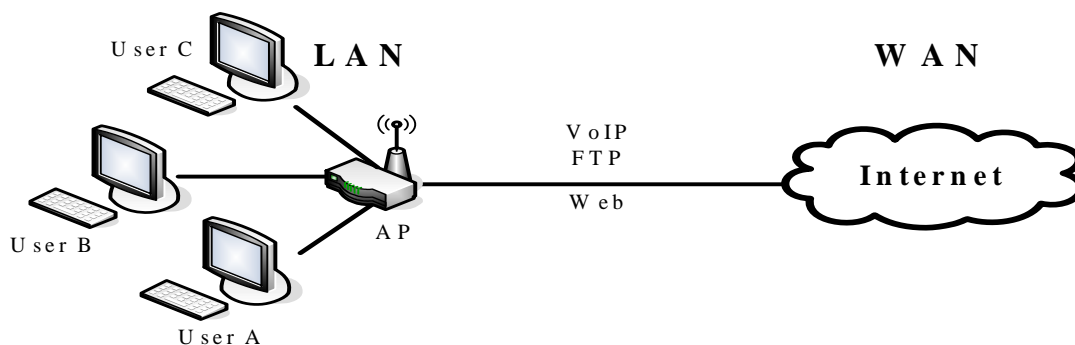
For example, there are three users in your network.

- 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 Adr	Dst Adr	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	☐
192.168.2.12/24	anywhere	-	-	21-21	-	TCP	LOW	0	Normal	☐
192.168.2.13/24	anywhere	-	-	80-80	-	TCP	MED	0	Normal	☐

[Delete Selected] [Delete All] [Reset]

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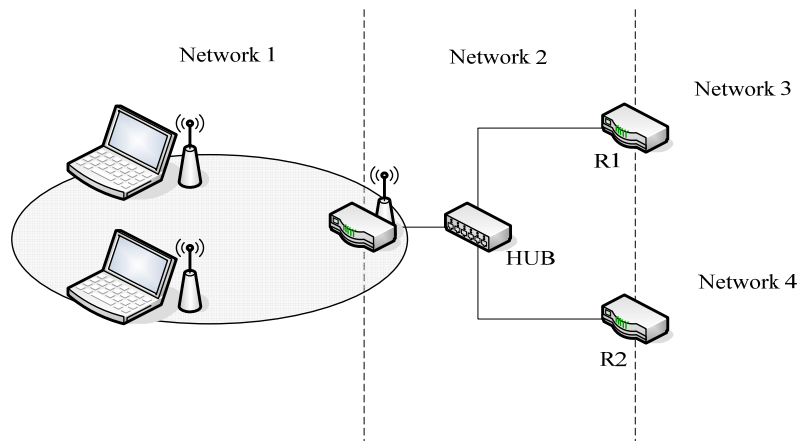
For example, if user wants to link the Network 3 and Network 4 separately from Network 1 that Routing Table configuration as below:

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.

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

3. In Static Route Table there have two routings for Network 3 and Network 4
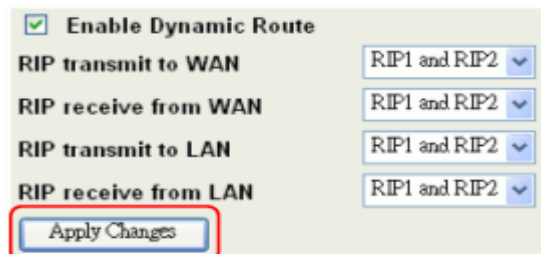
Destination IP Address	Netmask	Gateway	Select
192.168.3.0	255.255.255.0	192.168.2.1	☐
192.168.4.0	255.255.255.0	192.168.2.2	☐

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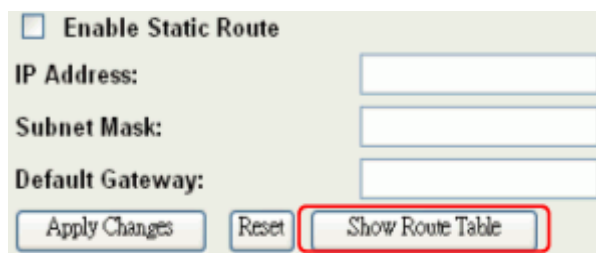
The Dynamic Route utilizes RIP1/2 to transmit and receive the route information with other Routers.

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

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

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.

VPN Connection

LAN   WAN

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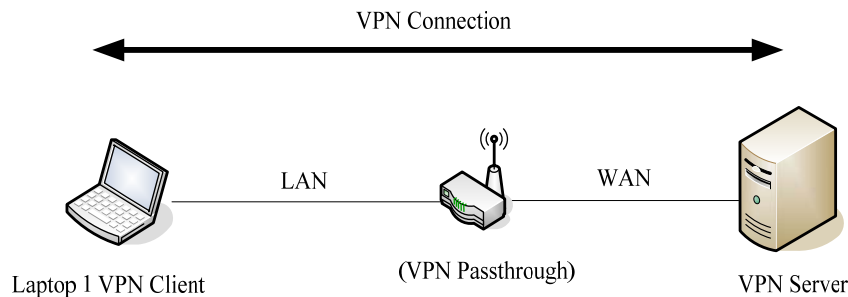
1. Check the VPN Pass-through in WAN Interface of TCP/IP Page that you want and then click Apply Changes button.

☑ Enable Web Server Access on WAN
1 ☑ Enable IPsec pass through on VPN connection
  ☑ Enable PPTP pass through on VPN connection
  ☑ Enable L2TP pass through on VPN connection
2 [Apply Changes] [Reset]
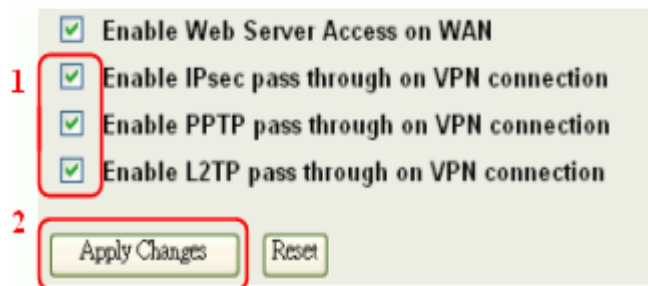
Using CLI Menu

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 "qwert", 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

Operation Mode
1: Router
2: Bridge
0: Cancel

Wireless Setting
  A. Basic Settings
  B. Advanced Settings
  C. Security Settings
  D. Access Control Settings
  E. WDS Settings
  0. Exit

TCP/IP-LAN Setting
  A. IP Address
  B. Subnet Mask
  C. Default Gateway
  D. DHCP
  E. DHCP Client Range
  F. 802.1d Spanning Tree
  G. Clone MAC Address
  H. MTU Size
  I. DHCP Client Table
  0. Exit

TCP/IP WAN Settings
  A. WAN Type
  B. IP Address
  C. Subnet Mask
  D. Default Gateway
  E. DNS1
  F. DNS2
  G. DNS3
  U. Clone MAC Address
  V. uPNP
  W. Web Server Access on WAN
  X. IPSec passthrough on VPN connection
  Y. PPTP passthrough on VPN connection
  Z. L2TP passthrough on VPN connection
  0. Exit

Route Settings
-[NAT]------------------------------
  A. NAT
  B. IP Forwarding Default Policy
-[Dynamic Route]------------------
  C. Dynamic Route
  D. RIP transmit to WAN
  E. RIP receive from WAN
  F. RIP transmit to LAN
  G. RIP receive from LAN
-[Static Route]----------------------
  H. Static Route
   I. Add Static Route Setting
  J. Delete Static Route Setting
 K. Delete all Static Route Setting
  L. Current Static Route Setting List
-[Route Table]------------------------
  M. Show Route Table List
  0. Exit

Firewall Settings
  A. Port Filtering
  B. IP Filtering
  C. MAC Filtering
  D. Port Forwarding
  E. DMZ
  F. VPN
  0. Exit

Wireless Basic Settings
  A. Access Point Status
  B. QoS Settings
  C. Bandwidth Control
  D. SNMP Settings
  E. Miscellaneous Settings
  F. Password
  0. Exit

A. Operation Mode

B. Wireless Setting

C. TCP/IP-LAN Setting

D. TCP/IP-WAN Setting

E. Route Setting

F. Firewall Setting

G. Management

H. Apply Changes to Flash

I. Reboot to take effect

0. Exit

The System Management

Password Protection

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

To disable the Web-Browser password protection just leave the "User Name" field to blank then click "Apply Changes" button.
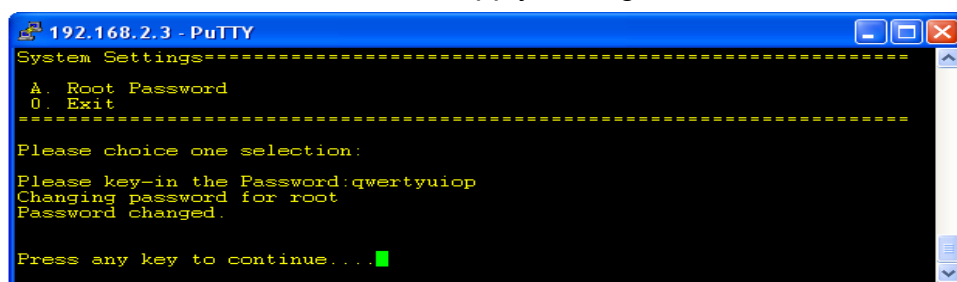
To change the password of user "root" for SSH session, please use the CLI menu item G. Management→F. Password

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.

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
Cold Start(0)	The trap from device after reboot the device
Link Down(2)	The trap is sent when any of the links are down. See the following table.
Link up(3)	The trap is sent when any of the links are UP. See the following table.
Authentication Failure(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

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: | 65500 | (1-65535) |
| RSSI Interval: | 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.
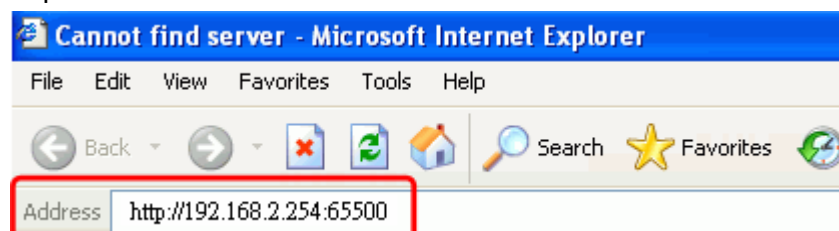
RSSI Interval

| HTTP Port: | 80 | (1-65535) |
| RSSI Interval: | 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.

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 and LED, so the installer can adjust the antenna of this device and visually check RSSI by LED.

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.

After clicking the "Aiming" button, RSSI will be displayed on the web page. It's also displayed by the LED. The flashing frequency of each LED shows the RSSI; the more frequency the LED flashing, the more RSSI it detected. From 20% to100% on the following picture, the more LED on means the more RSSI detected. For example, if the 20% LED and 40% LED are both on and flash quickly, that means the RSSI of the specific SSID is approaching 40%.
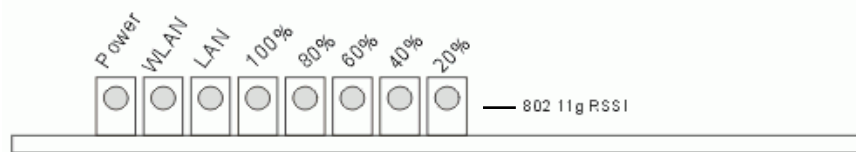
To stop the Aiming tool, the user just click "Stop Aiming" button.

Connecting Profile

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	☑
Device AP 1	00:00:00:00:00:00	☐

[Delete Selected] [Delete All] [Reset]

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.

Firmware Upgrade

Firmware Types

The firmware for this device is divided into 2 parts, one is web pages firmware the other is application firmware, and the naming usually are **zwa-2000webpages_adv.bin** and **zwa-2000linux_adv_led1.bin**. To upgrade firmware, we suggest user first upgrade the application firmware then web pages firmware.

Upgrading Firmware

The Web-Browser upgrading interface is the simplest and safest way for user, it will check the firmware checksum and signature, and the wrong firmware won't be accepted. After upgrading, the device will reboot and please note that depends on the version of firmware, the upgrading may cause the device configuration to be restored to the factory default setting, and the original configuration data will be lost!

To upgrade firmware, just assign the file name with full path then click "Upload" button as the following page.

Memory Limitation

To make sure the device have enough memory to upload firmware, the system will check the capacity of free memory, if the device lack of memory to upload firmware, please temporarily turn-off some functions then reboot the device to get enough memory for firmware uploading.
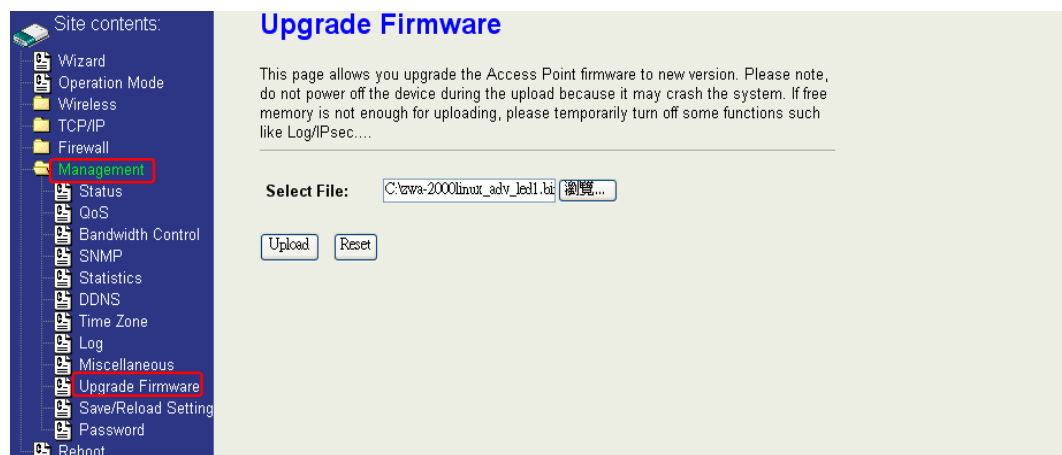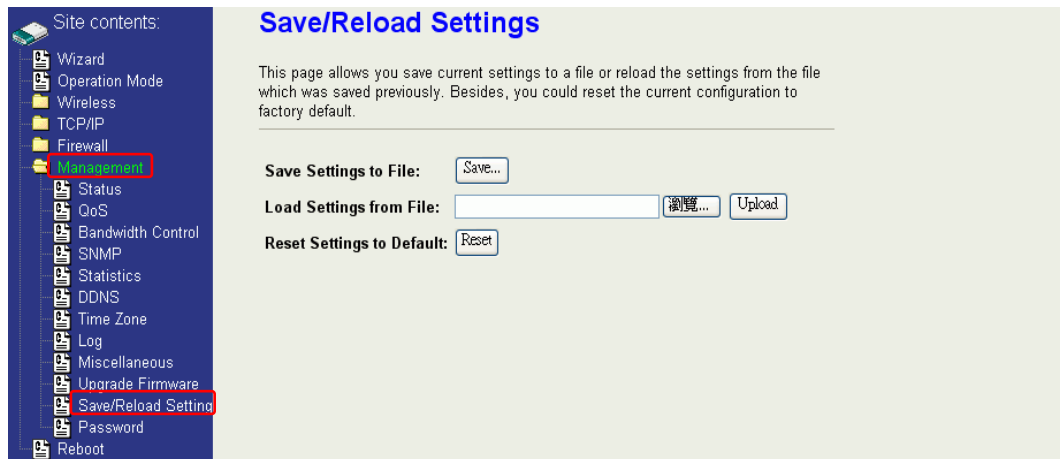

Configuration Data Backup & Restore

Rest 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.
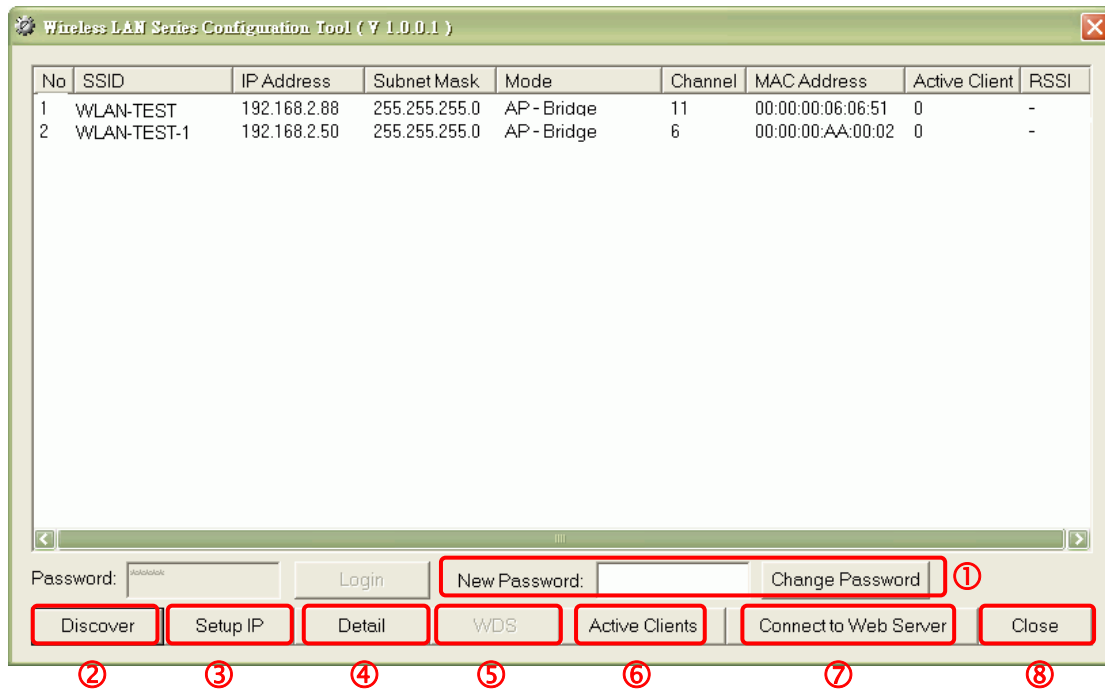
Login:

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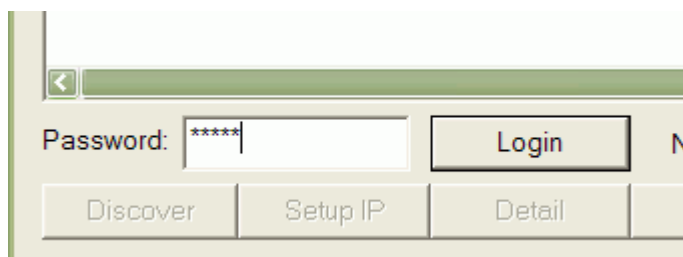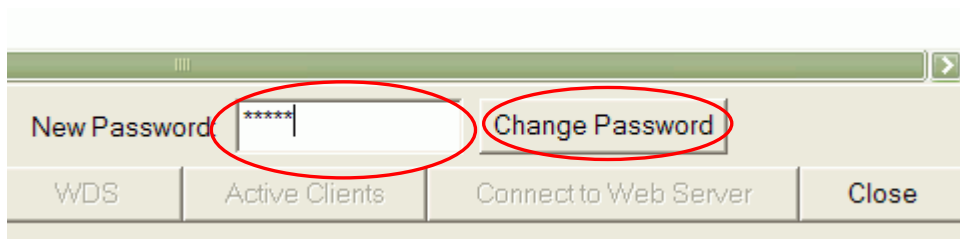

If the user doesn't input the password or input a wrong password, he can't login the tool and see the alert window.
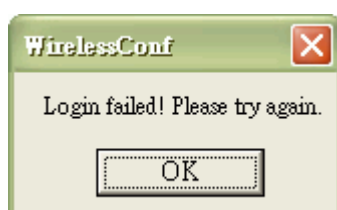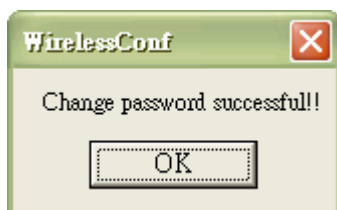
1. Change Password

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.
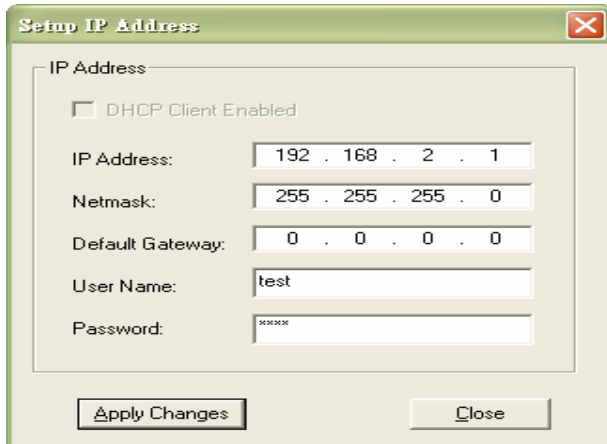

2. Discover

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 Received 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.

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.
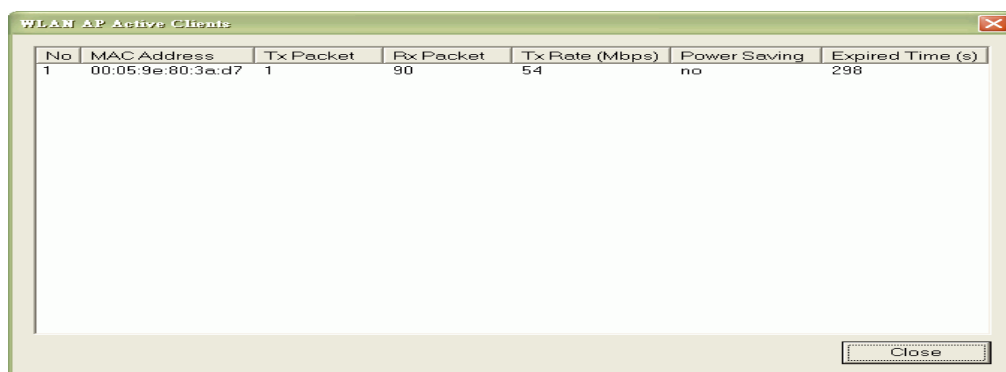

6. Active Clients

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

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 "qwert" to login the tool.
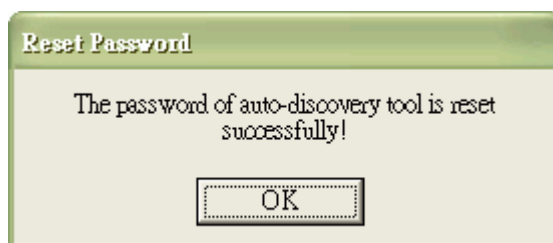
REMARK: This device must be installed by professional.