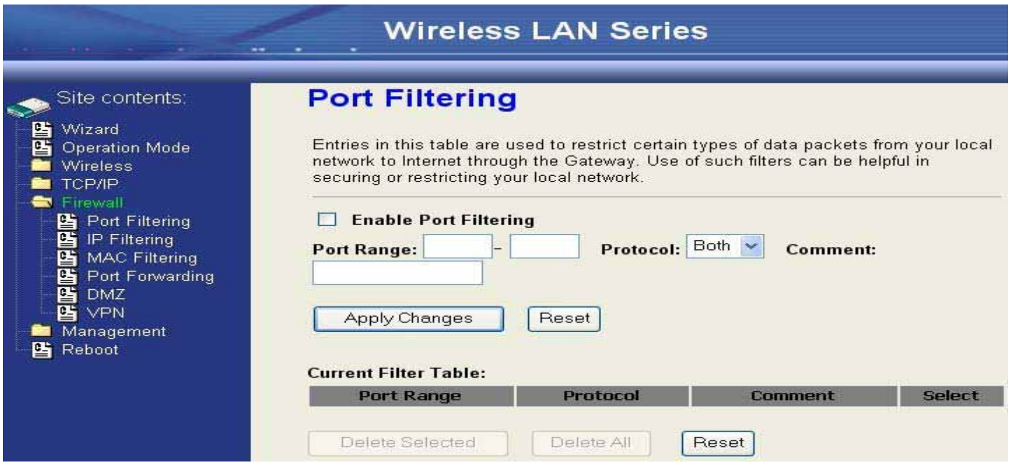
4 Advanced Configurations

Configuring LAN to WAN Firewall

Filtering function is used to block 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 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.

Port Filtering

When you enable the Port Filtering function, you can specify a single port or port ranges in current filter table. 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 from LAN to WAN.



Port Filtering

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

□ Enable Port Filtering

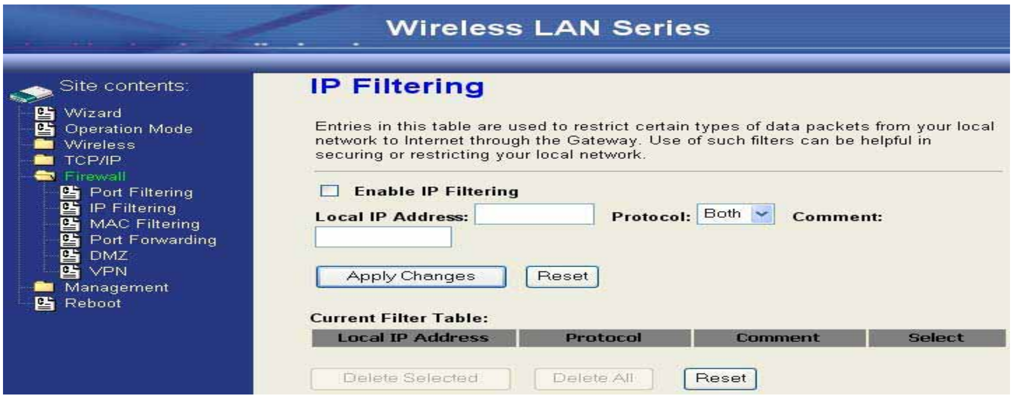
Port Range: ____ - ____ Protocol: Both Comment: ____

Current Filter Table:

Port Range	Protocol	Comment	Select

IP Filtering

When you enable the IP Filtering function, you can specify local IP Addresses in current filter table. Once the source IP address of outgoing packets match the IP Addresses in the table, the firewall will block this packet from LAN to WAN.



IP Filtering

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

□ Enable IP Filtering

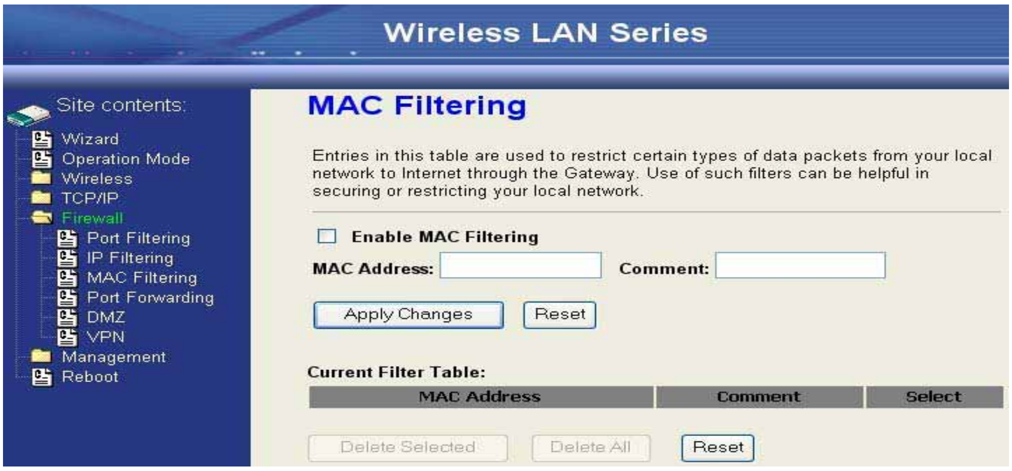
Local IP Address: ____ Protocol: Both Comment: ____

Current Filter Table:

Local IP Address	Protocol	Comment	Select

MAC Filtering

When you enable the MAC Filtering function, you can specify the MAC Addresses in current filter table. Once the source MAC Address of outgoing packets match the MAC Addresses in the table, the firewall will block this packet from LAN to WAN.



MAC Filtering

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

□ Enable MAC Filtering

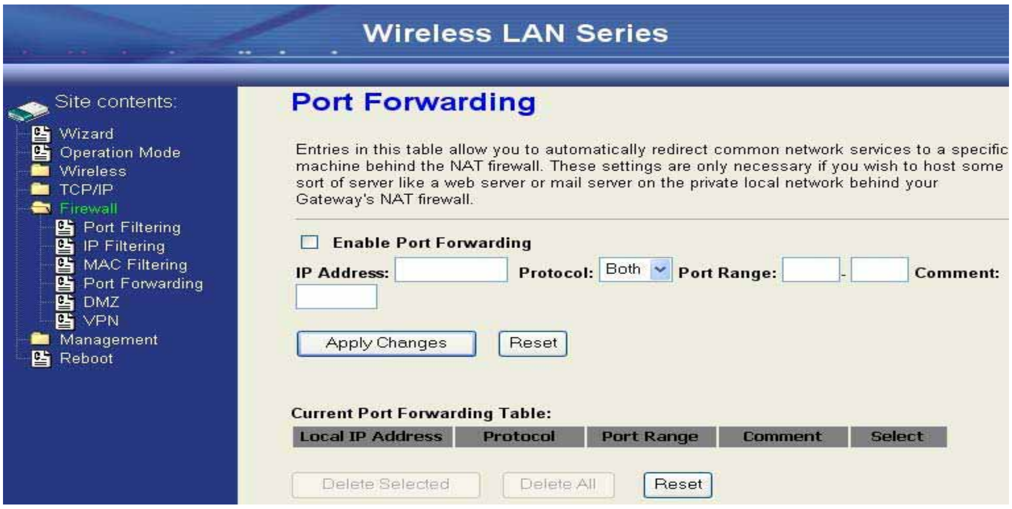
MAC Address: Comment:

Current Filter Table:

MAC Address	Comment	Select

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

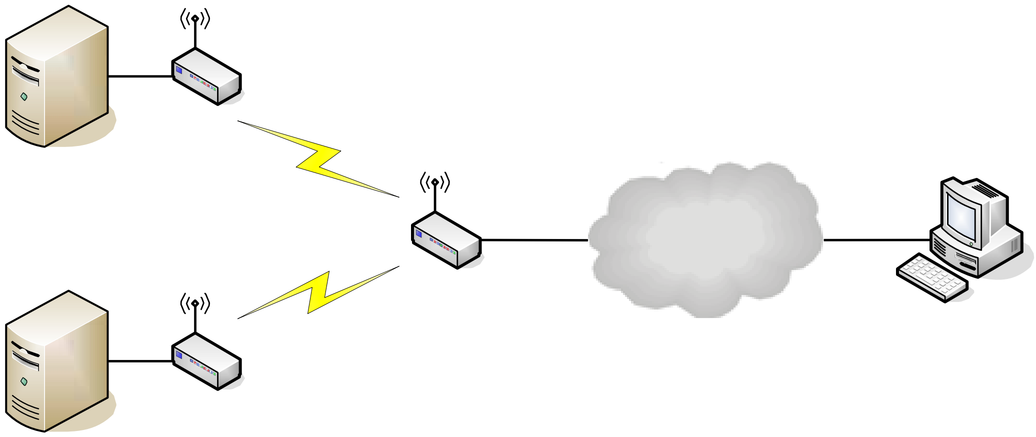
IP Address: Protocol: Both Port Range: - Comment:

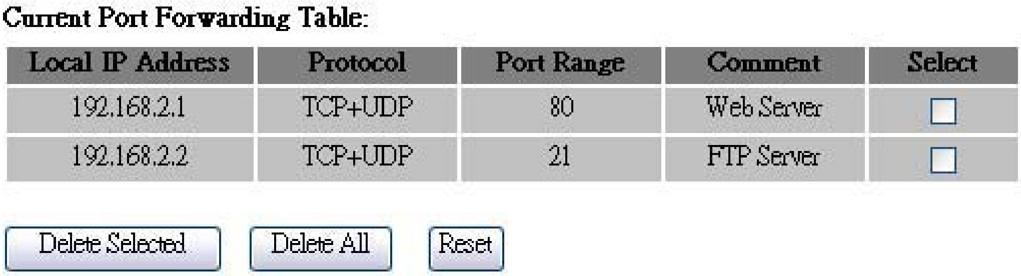
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Multiple Servers behind NAT Example:

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



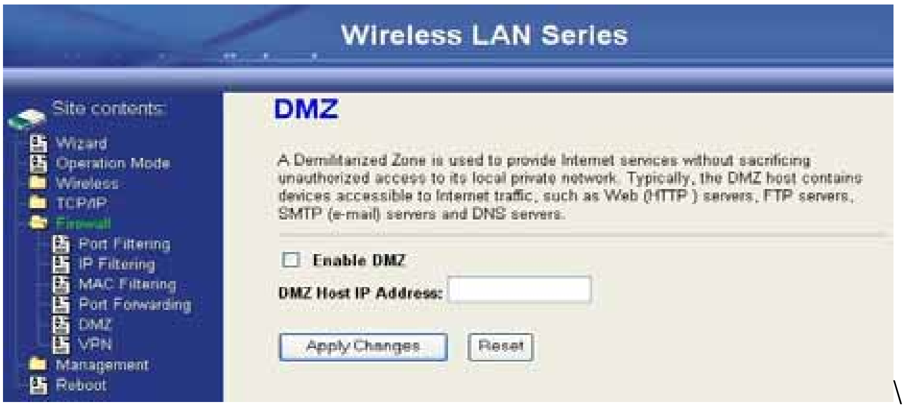


Current Port Forwarding Table:

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

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.



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

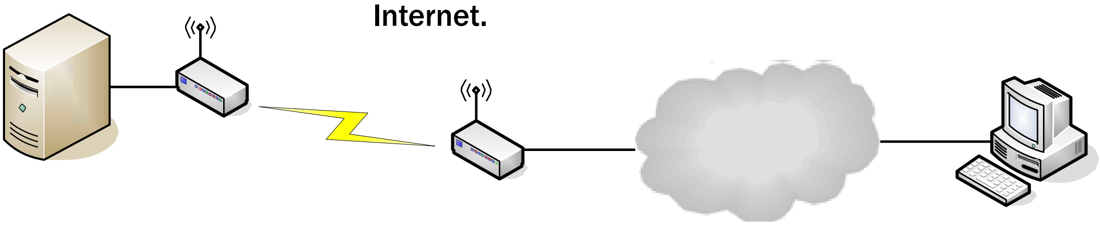
DMZ Host IP Address:

\

Enable DMZ: Enable the “Enable DMZ”, and then click “Apply Changes” button to save the changes.

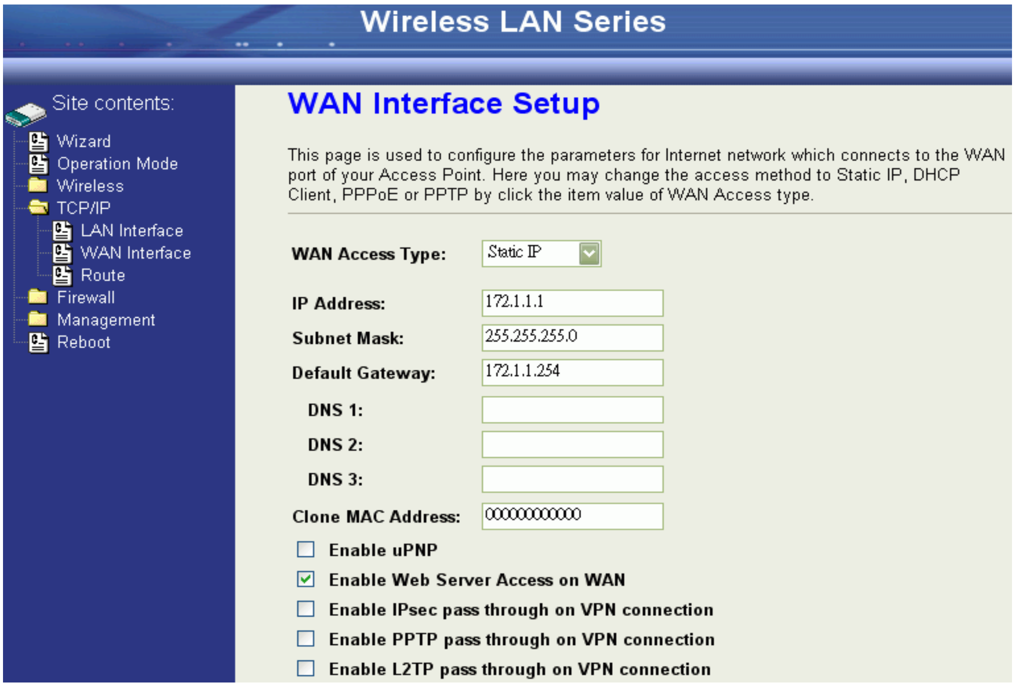
DMZ Host IP Address: Input the IP Address of the computer that you want to expose to

Internet.



Configuring 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”.



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

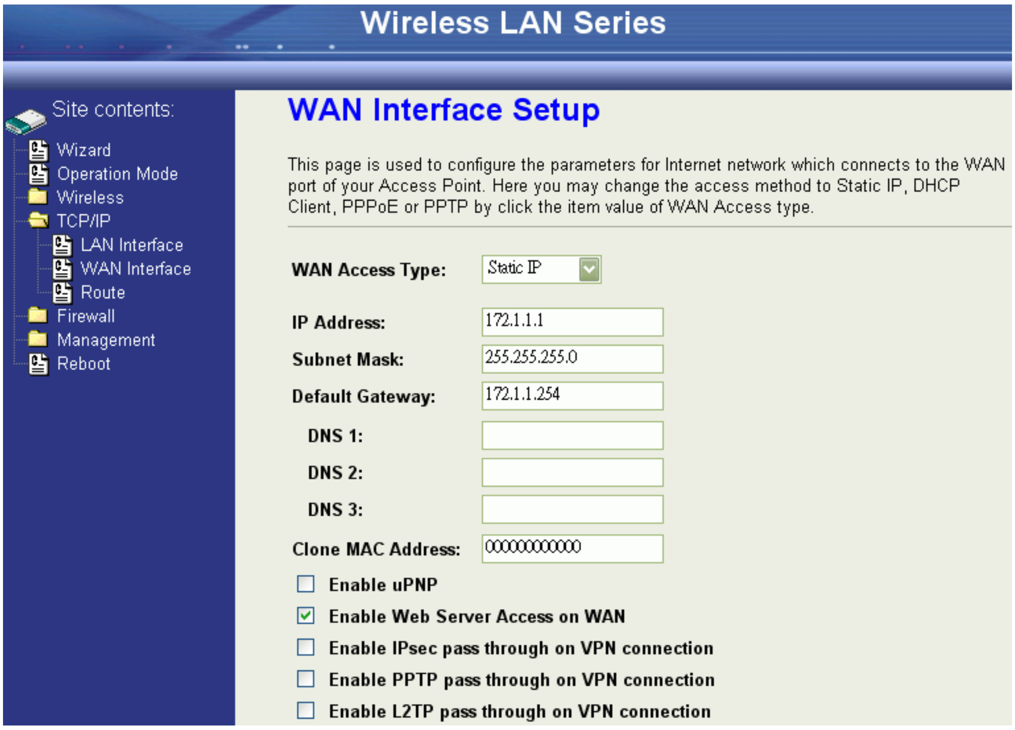
☐ Enable IPsec pass through on VPN connection

☐ Enable PPTP pass through on VPN connection

☐ Enable L2TP pass through on VPN connection

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

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.

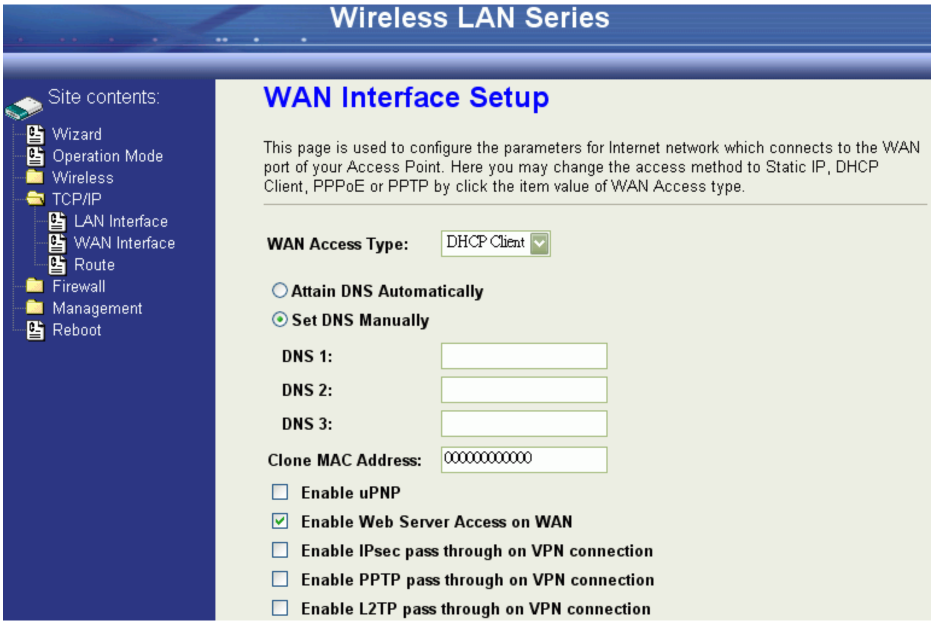
DNS 1~3: The IP addresses of DNS provided by your ISP.DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

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

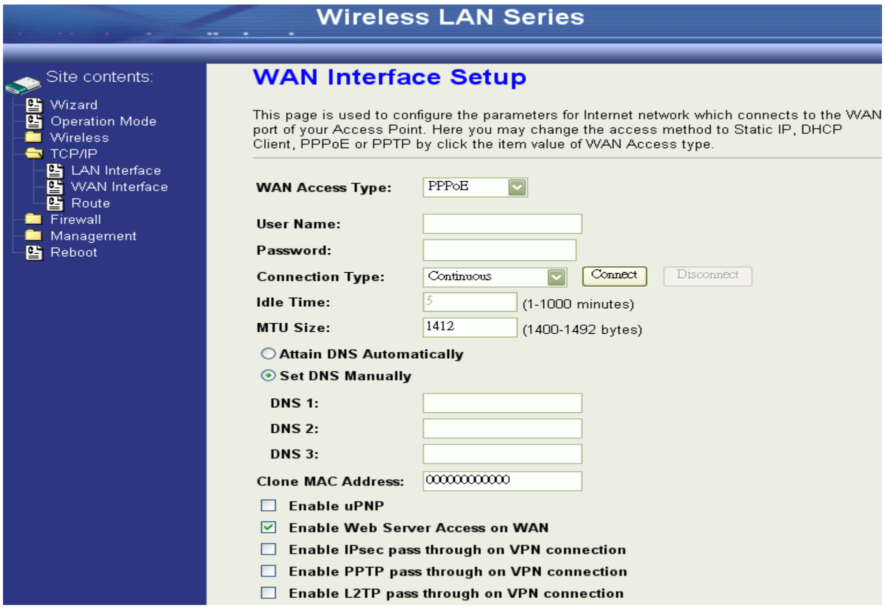
DNS1~3: The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

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.



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: PPPoE

User Name:

Password:

Connection Type: Continuous [Connect] [Disconnect]

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: 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

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 need 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.

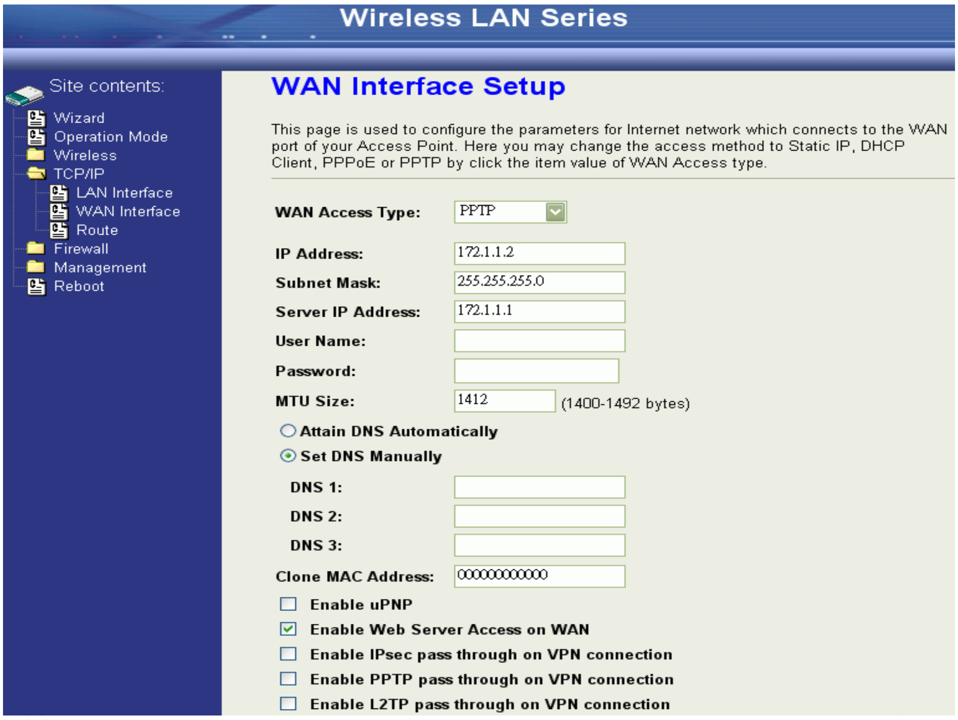
DNS1~3: The IP addresses of DNS provided by your ISP.DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

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



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: 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)

○ 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

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: The IP address of PPTP server (Default Gateway)

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.

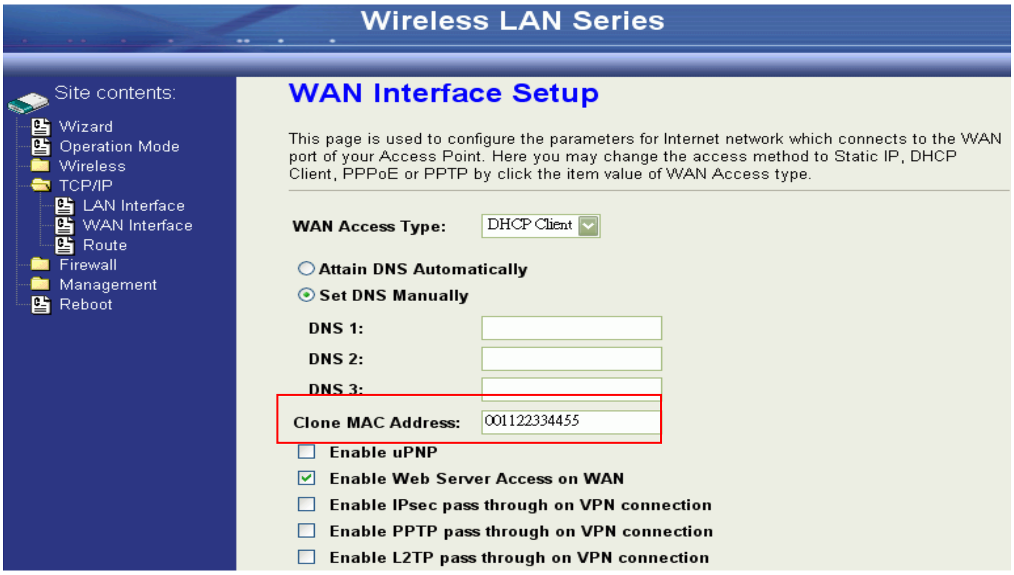
Enable uPnP: Enable uPnP, this function allows the device to be found and configured automatically by the system. (Ex. Window XP)

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 DHCP Client WAN access type



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP 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

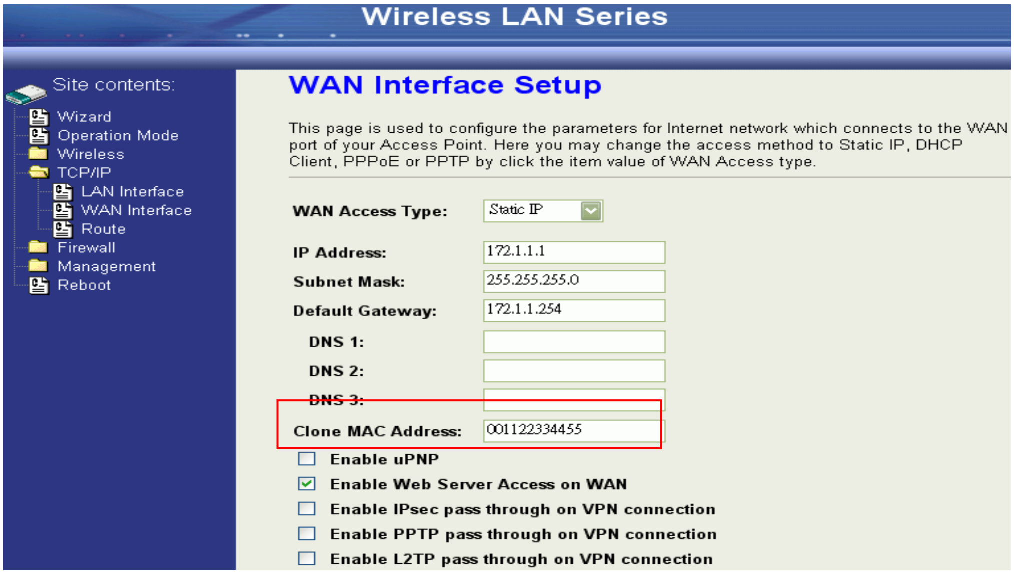
☑ Enable Web Server Access on WAN

□ Enable IPsec pass through on VPN connection

□ Enable PPTP pass through on VPN connection

□ Enable L2TP pass through on VPN connection

2. Clone MAC address for Static IP WAN access type



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP 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

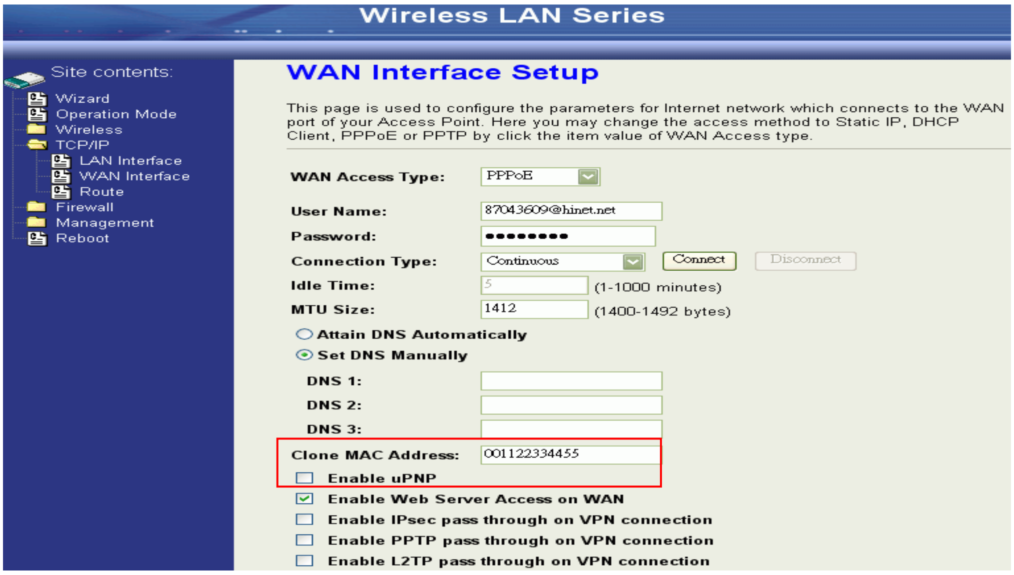
☑ Enable Web Server Access on WAN

□ Enable IPsec pass through on VPN connection

□ Enable PPTP pass through on VPN connection

□ Enable L2TP pass through on VPN connection

3. Clone MAC address for PPPoE WAN access type



WAN Interface Setup

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

WAN Access Type: PPPoE

User Name: 87043609@hinet.net

Password: •••••••••

Connection Type: Continuous Connect Disconnect

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

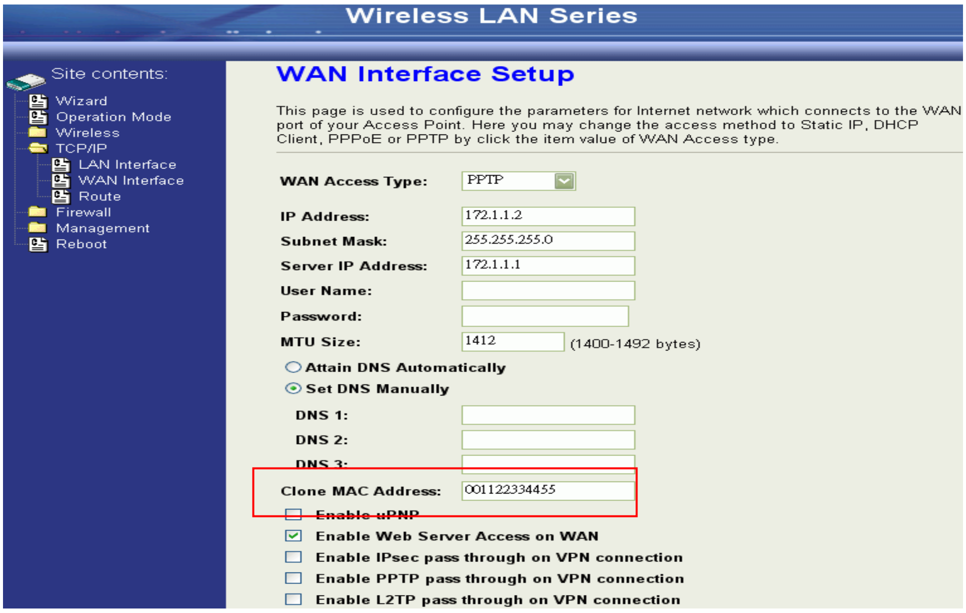
☑ Enable Web Server Access on WAN

□ 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



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: 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)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 001122334455

□ Enable uPNP

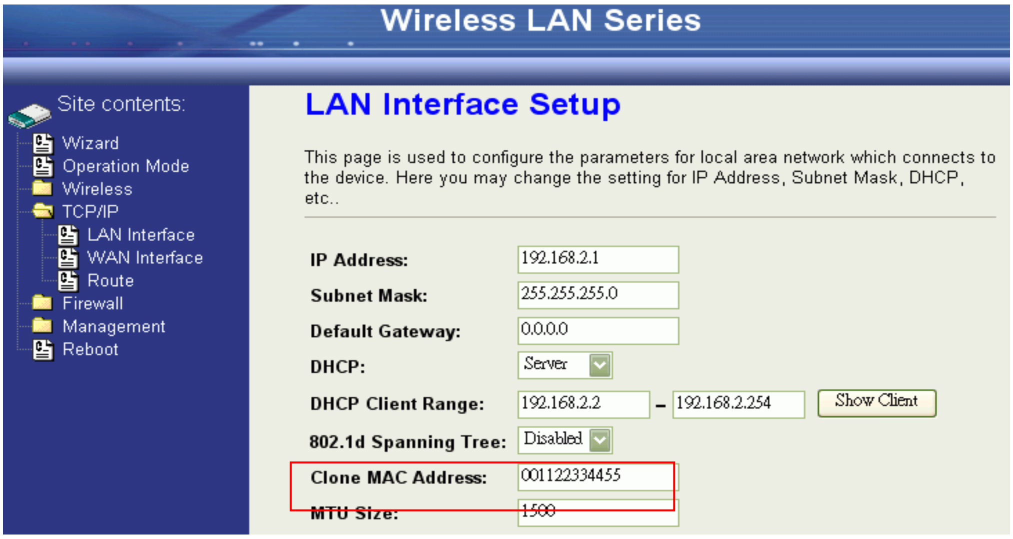
☑ Enable Web Server Access on WAN

□ 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



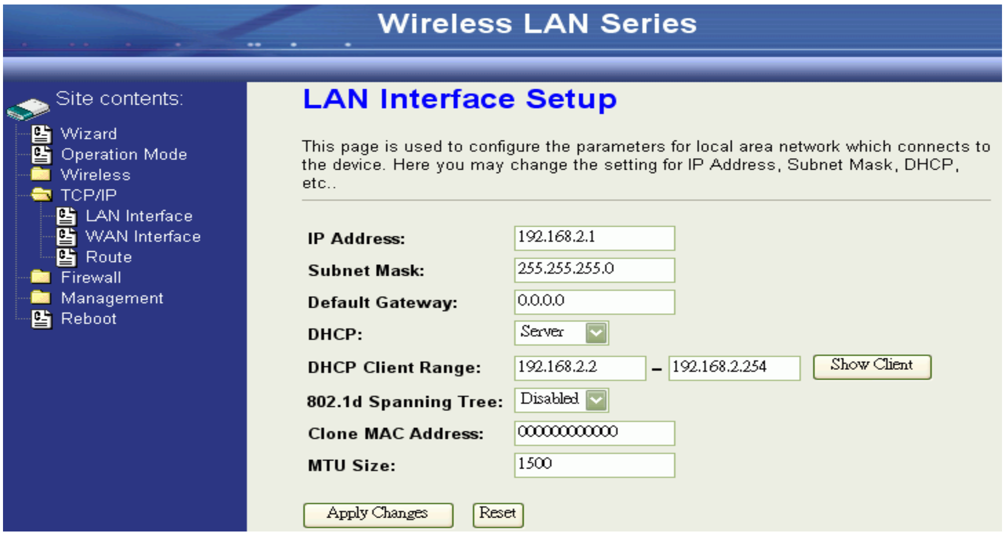
LAN Interface Setup

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..

IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.2.2 – 192.168.2.254 Show Client
802.1d Spanning Tree:	Disabled
Clone MAC Address:	001122334455
MTU Size:	1500

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.



LAN Interface Setup

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..

IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.2.2 – 192.168.2.254 Show Client
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000
MTU Size:	1500

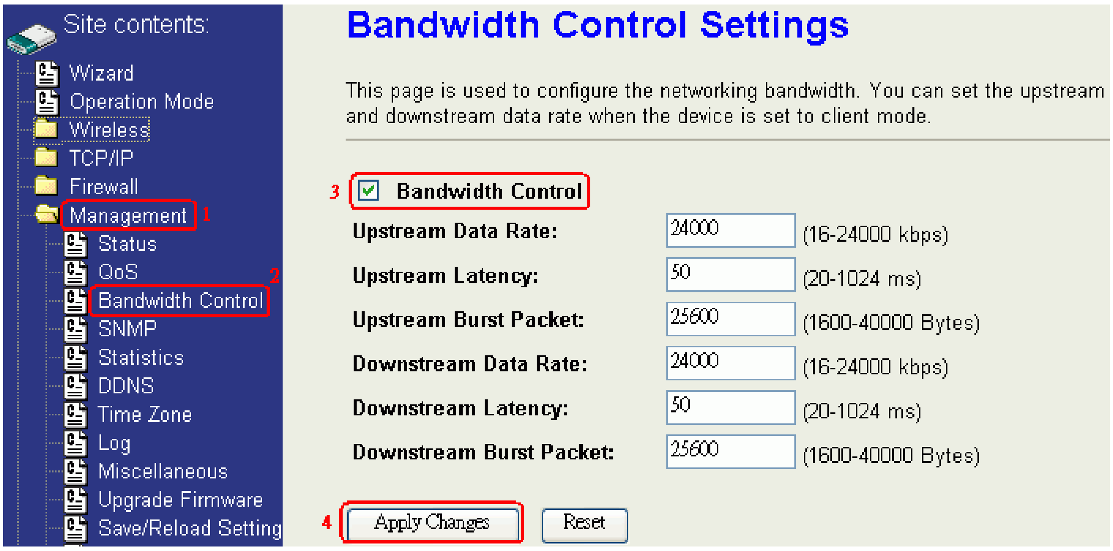
3. When the DHCP server is enabled and also the device router mode is enabled then the default gateway for all the DHCP client hosts will set to the IP address of device.

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.



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.

☑ 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)

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.

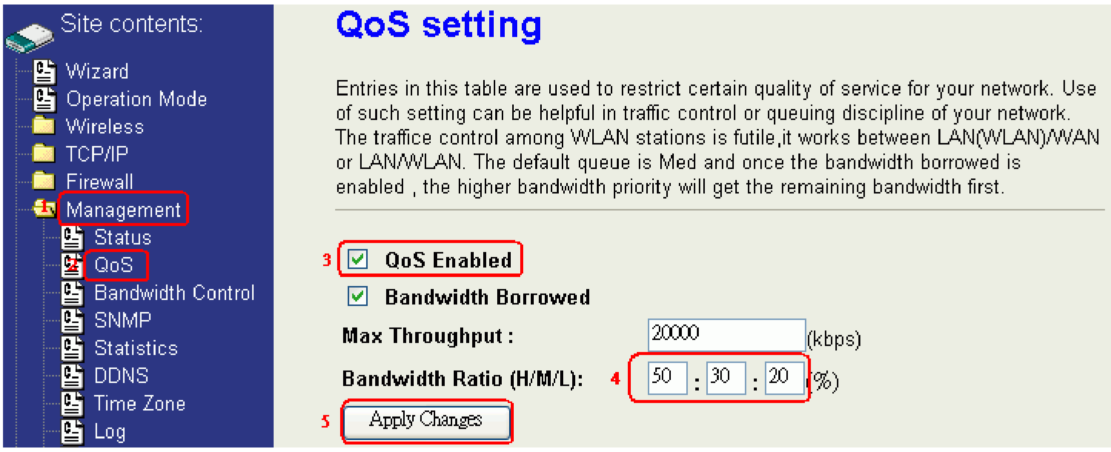
QoS (Quality of Service)

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 traffice 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 : 20000 (kbps)

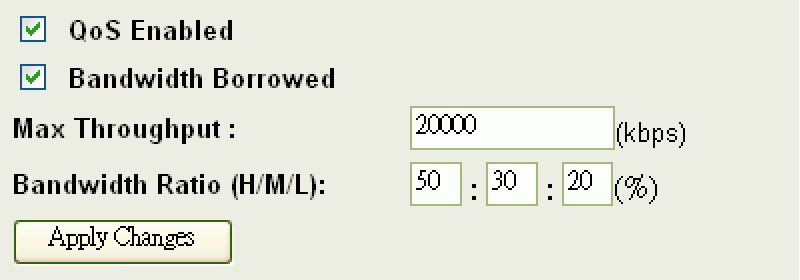
Bandwidth Ratio (H/M/L): 50 : 30 : 20 (%)

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 voice or video applications that is especially sensitive to the variations in 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

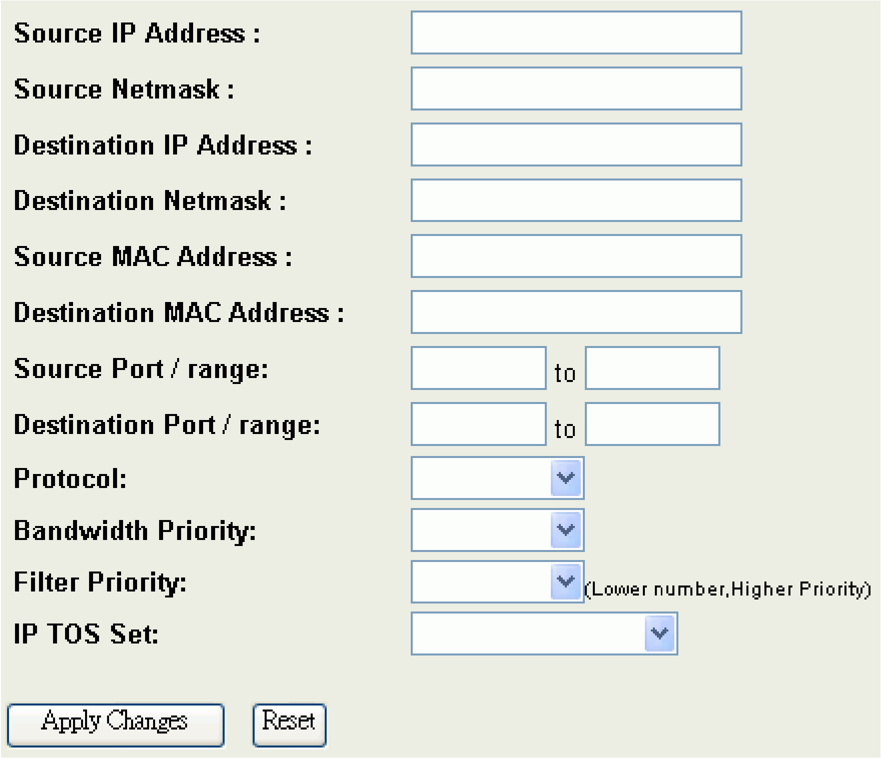
Max Throughput : 20000 (kbps)

Bandwidth Ratio (H/M/L): 50 : 30 : 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

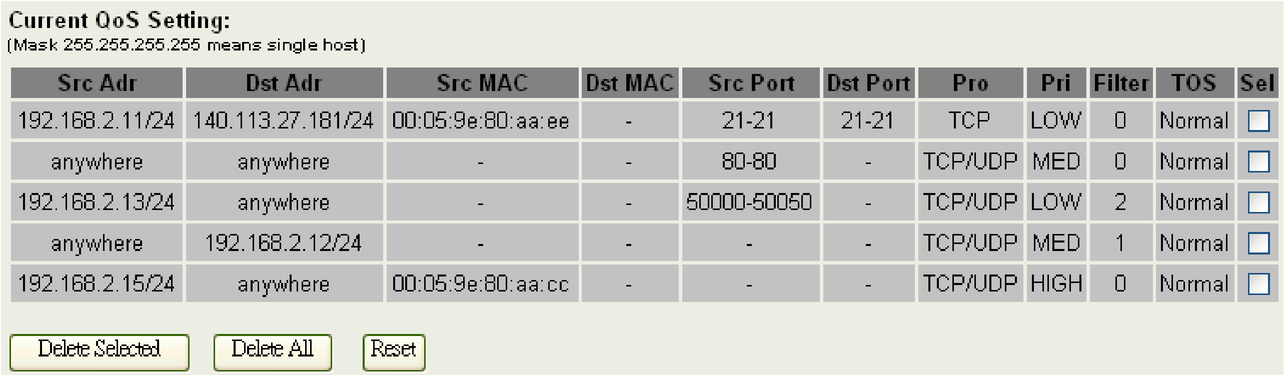


Source IP Address :	
Source Netmask :	
Destination IP Address :	
Destination Netmask :	
Source MAC Address :	
Destination MAC Address :	
Source Port / range:	to
Destination Port / range:	to
Protocol:	
Bandwidth Priority:	
Filter Priority:	(Lower number,Higher Priority)
IP TOS Set:	

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

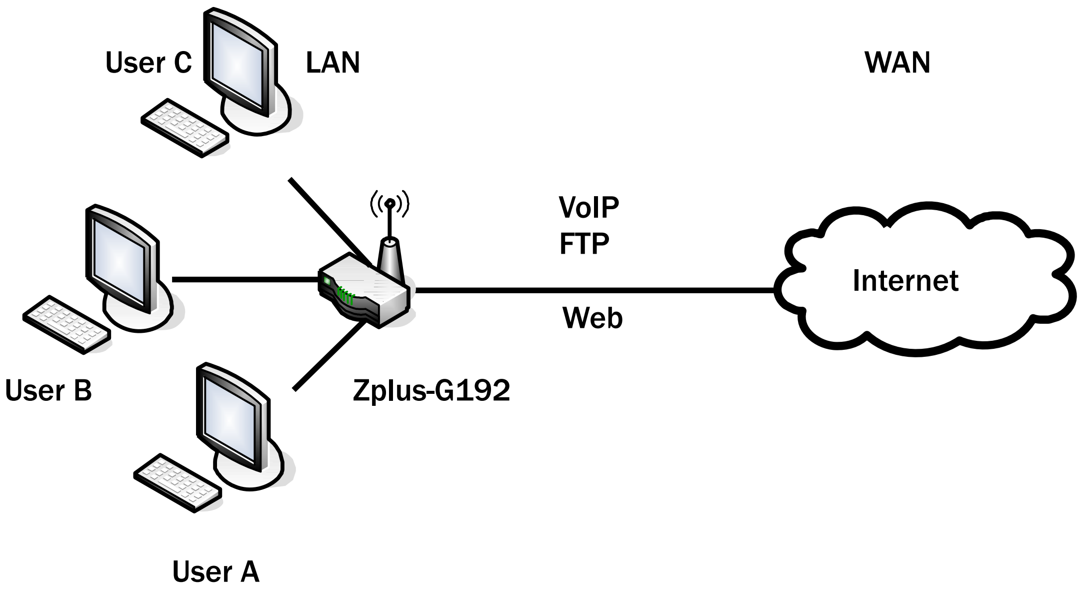
In this part, you can see how many rules have been specified. And you can see the detail about the rules and manage the rules. This table can input 50 rules at most.



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	□

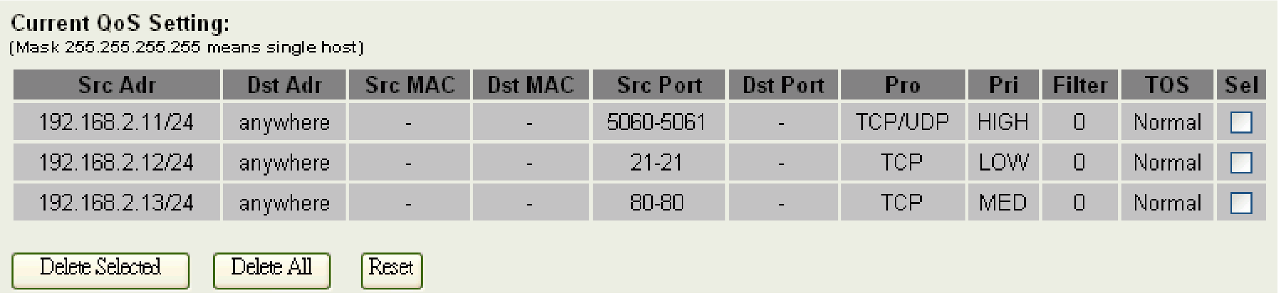
An example for usage



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.

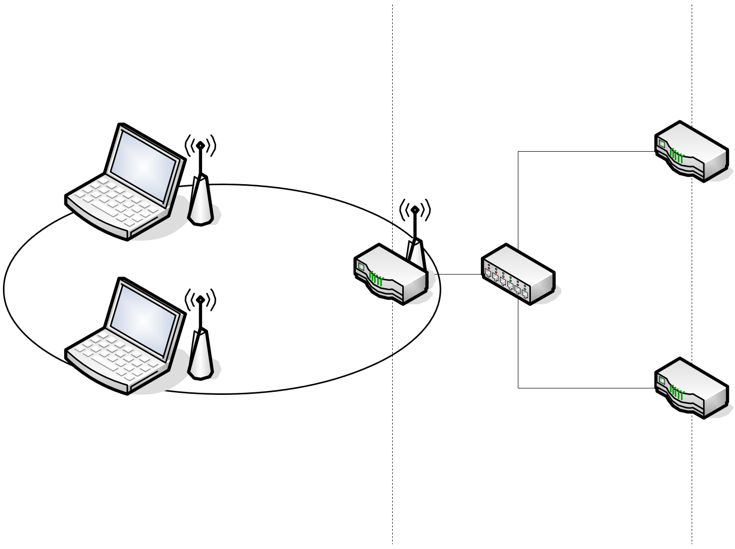


Current QoS Setting:
(Mask 255.255.255.255 means single host)

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	□

Static Route Setup

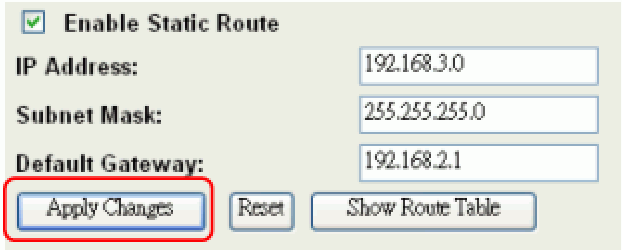
User can set the routing information let the Router knows what routing is correct also it can not learn automatically through other means.



For example, if user wants to link the Network 3 and Network 4 separately from

Network 1 that Routing Table configuration as blow:

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.



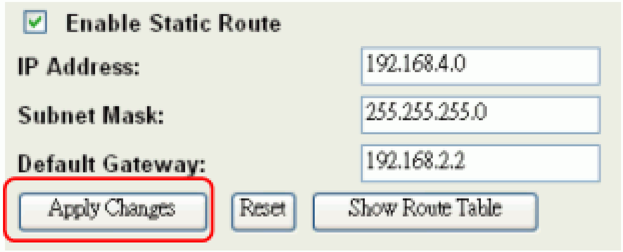
☑ Enable Static Route

IP Address: 192.168.3.0

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

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



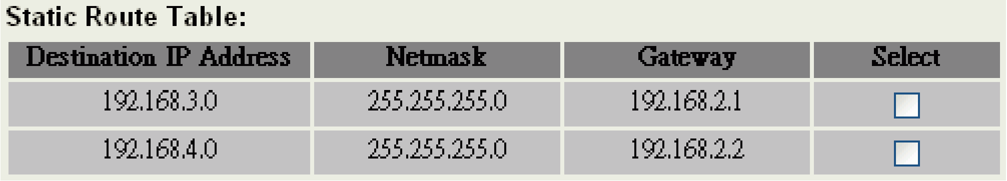
☑ Enable Static Route

IP Address: 192.168.4.0

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.2

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



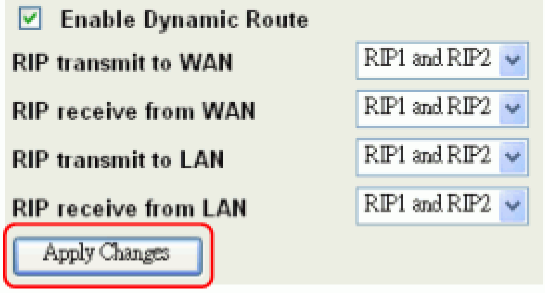
Static Route Table:

Destination IP Address	Netmask	Gateway	Select
192.168.3.0	255.255.255.0	192.168.2.1	□
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.



☑ Enable Dynamic Route

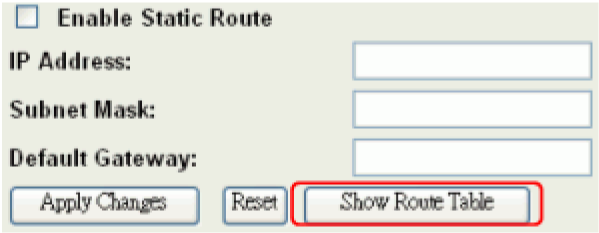
RIP transmit to WAN: RIP1 and RIP2

RIP receive from WAN: RIP1 and RIP2

RIP transmit to LAN: RIP1 and RIP2

RIP receive from LAN: RIP1 and RIP2

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



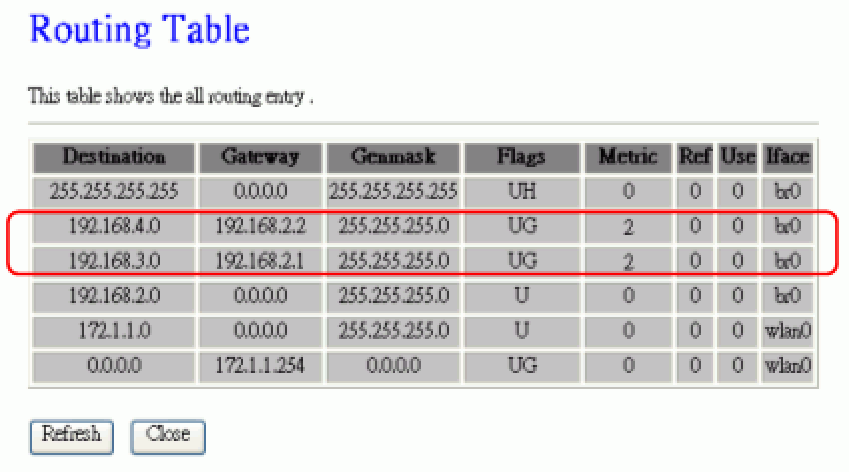
□ Enable Static Route

IP Address:

Subnet Mask:

Default Gateway:

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



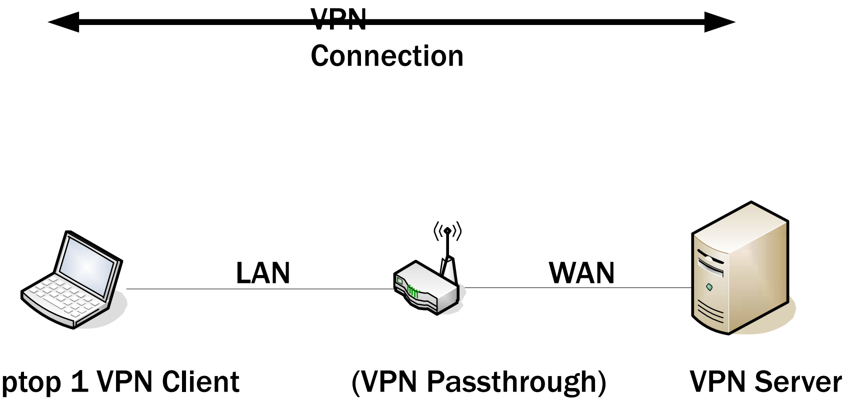
Routing Table

This table shows the all routing entry .

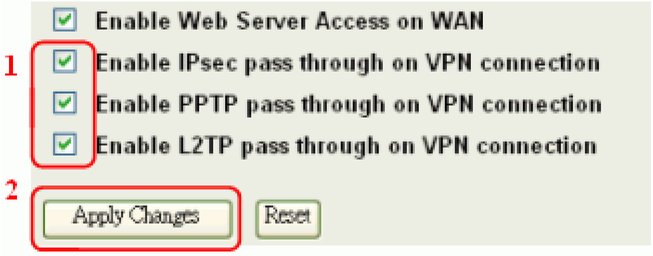
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
255.255.255.255	0.0.0.0	255.255.255.255	UH	0	0	0	br0
192.168.4.0	192.168.2.2	255.255.255.0	UG	2	0	0	br0
192.168.3.0	192.168.2.1	255.255.255.0	UG	2	0	0	br0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
172.1.1.0	0.0.0.0	255.255.255.0	U	0	0	0	wlan0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

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.



☑ 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

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.

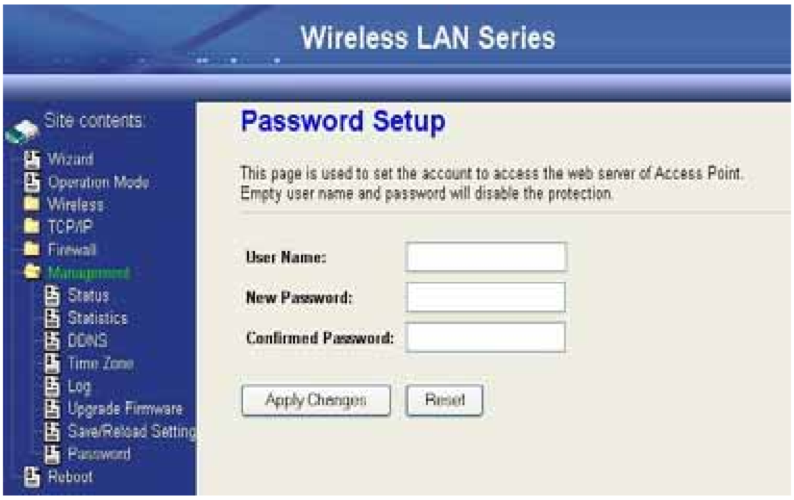
Execute CLI program

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.

The System Management

Password Protection

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



Password Setup

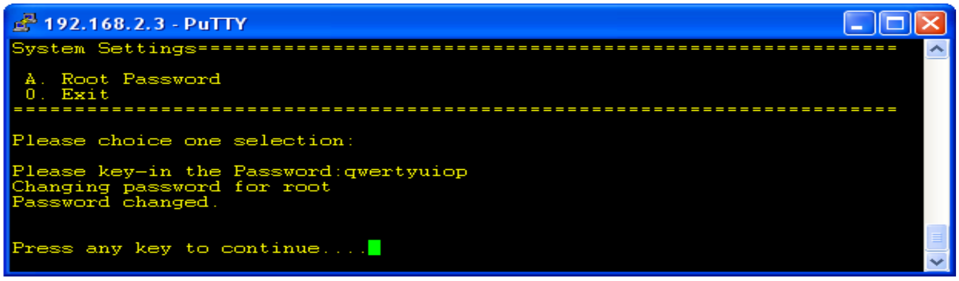
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

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



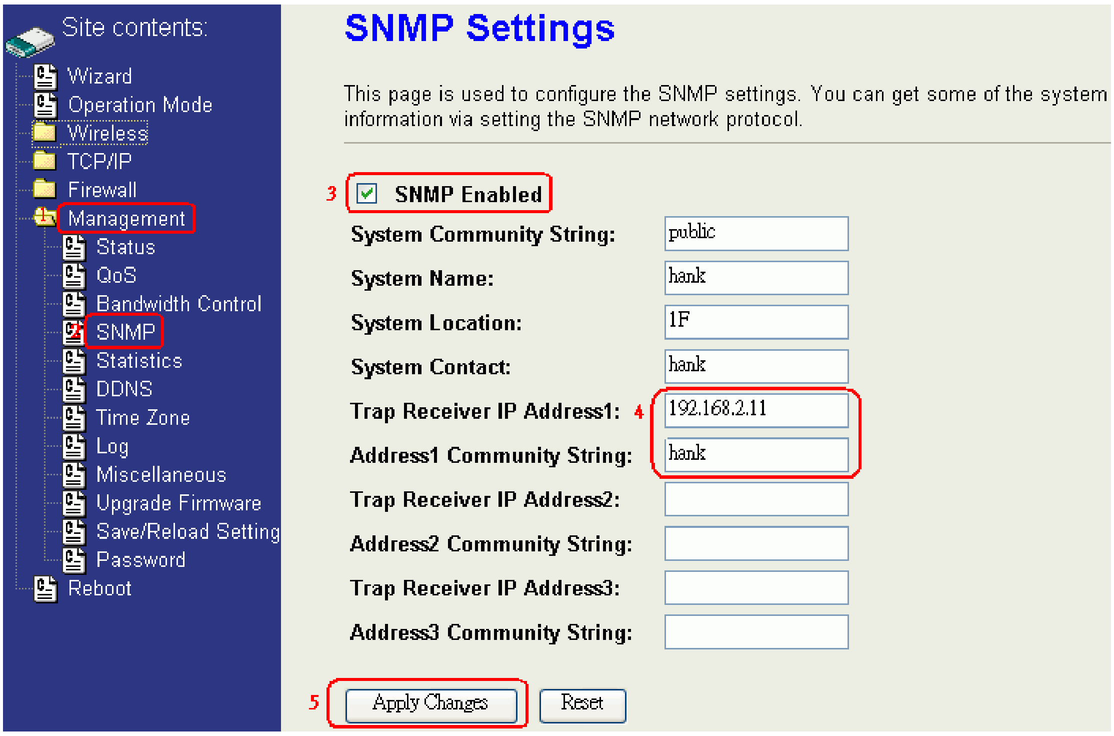
```
System Settings=================================================================

 A. Root Password
 0. Exit
================================================================================

Please choice one selection:

Please key-in the Password:qwertyuiop
Changing password for root
Password changed.

Press any key to continue....
```

To change the password of user “root” for SSH session, please use the CLI menu item G. System SettingÆA. Root Password

SNMP Agent

This device is compatible with SNMP v1/v2c and provide 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.

☑ SNMP Enabled

System Community String: public

System Name: hank

System Location: 1F

System Contact: hank

Trap Receiver IP Address1: 192.168.2.11

Address1 Community String: hank

Trap Receiver IP Address2:

Address2 Community String:

Trap Receiver IP Address3:

Address3 Community String:

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).

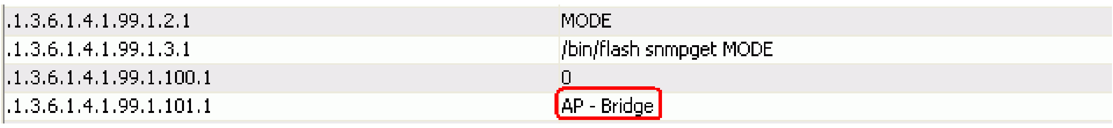
3. SNMP Traps

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

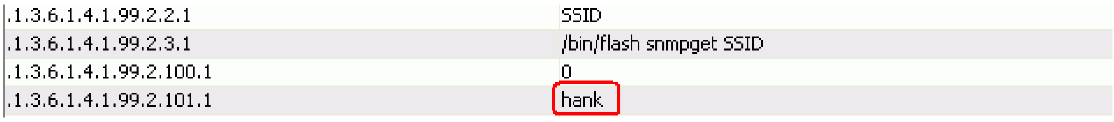
OID	Description
1.3.6.1.4.1.99.1	Mode, Operation Mode in device.
1.3.6.1.4.1.99.2	SSID, SSID of the device
1.3.6.1.4.1.99.3	Channel, Channel of the device in WLAN
1.3.6.1.4.1.99.4	Band, 802.11g / 802.11b only
1.3.6.1.4.1.99.5	RSSI, Receive Signal Strength Index (Support AP and Client RSSI)
1.3.6.1.4.1.99.6	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



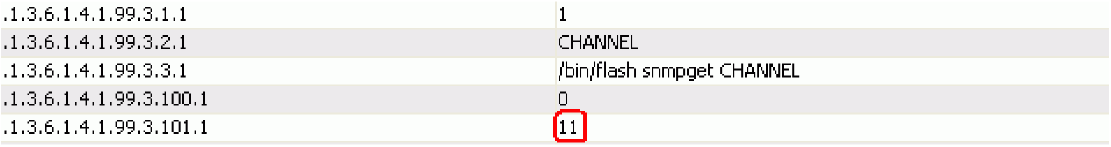
```
.1.3.6.1.4.1.99.1.2.1      MODE
.1.3.6.1.4.1.99.1.3.1      /bin/flash snmpget MODE
.1.3.6.1.4.1.99.1.100.1    0
.1.3.6.1.4.1.99.1.101.1    AP - Bridge
```

1.3.6.1.4.1.99.2 - SSID



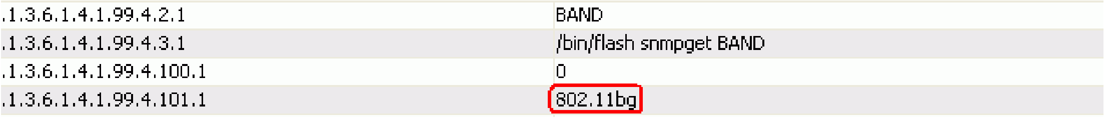
```
.1.3.6.1.4.1.99.2.2.1      SSID
.1.3.6.1.4.1.99.2.3.1      /bin/flash snmpget SSID
.1.3.6.1.4.1.99.2.100.1    0
.1.3.6.1.4.1.99.2.101.1    hank
```

1.3.6.1.4.1.99.3 - Channel



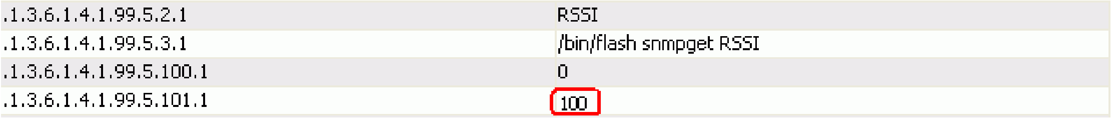
.1.3.6.1.4.1.99.3.1.1	1
.1.3.6.1.4.1.99.3.2.1	CHANNEL
.1.3.6.1.4.1.99.3.3.1	/bin/flash snmpget CHANNEL
.1.3.6.1.4.1.99.3.100.1	0
.1.3.6.1.4.1.99.3.101.1	11

1.3.6.1.4.1.99.4 - Band



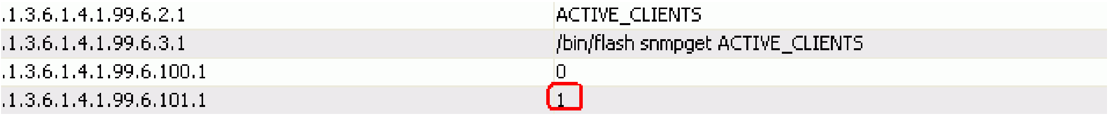
.1.3.6.1.4.1.99.4.2.1	BAND
.1.3.6.1.4.1.99.4.3.1	/bin/flash snmpget BAND
.1.3.6.1.4.1.99.4.100.1	0
.1.3.6.1.4.1.99.4.101.1	802.11bg

1.3.6.1.4.1.99.5 - RSSI



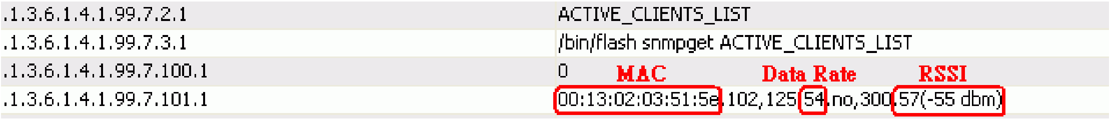
.1.3.6.1.4.1.99.5.2.1	RSSI
.1.3.6.1.4.1.99.5.3.1	/bin/flash snmpget RSSI
.1.3.6.1.4.1.99.5.100.1	0
.1.3.6.1.4.1.99.5.101.1	100

1.3.6.1.4.1.99.6 - Active_Clients



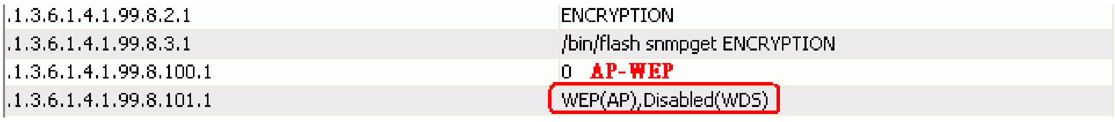
.1.3.6.1.4.1.99.6.2.1	ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.3.1	/bin/flash snmpget ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.100.1	0
.1.3.6.1.4.1.99.6.101.1	1

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
.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
.1.3.6.1.4.1.99.8.101.1	WEP(AP),Disabled(WDS)

Firmware Upgrade

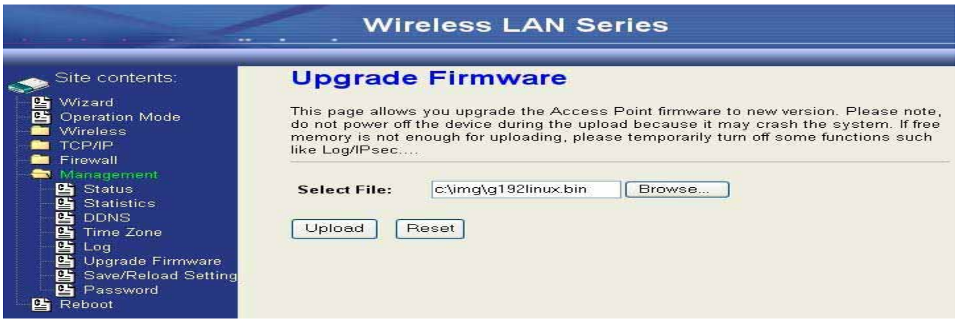
Firmware Types

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 g120webpage.bin and g120linux.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.



This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system. If free memory is not enough for uploading, please temporarily turn off some functions such like Log/IPsec....

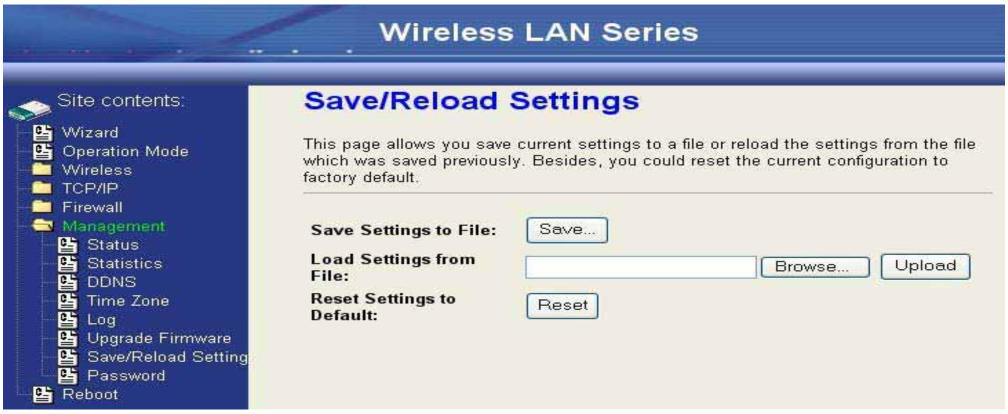
Select File: c:\img\g192linux.bin

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



Save/Reload Settings

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

Save Settings to File:

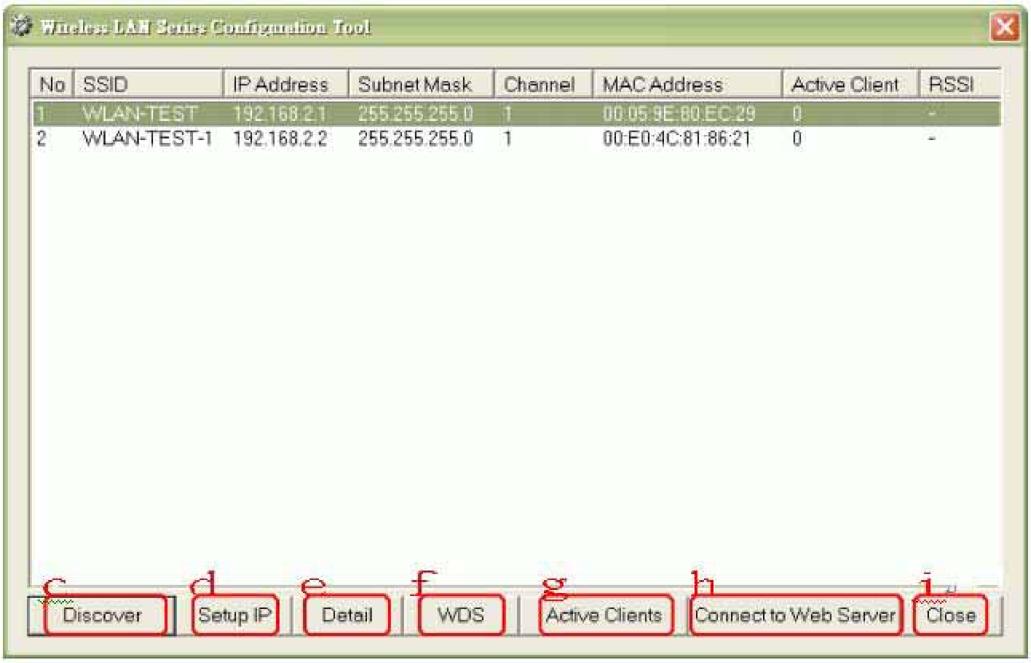
Load Settings from File:

Reset Settings to Default:

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.



No	SSID	IP Address	Subnet Mask	Channel	MAC Address	Active Client	RSSI
1	WLAN-TEST	192.168.2.1	255.255.255.0	1	00:05:9E:80:EC:29	0	-
2	WLAN-TEST-1	192.168.2.2	255.255.255.0	1	00:E0:4C:81:86:21	0	-

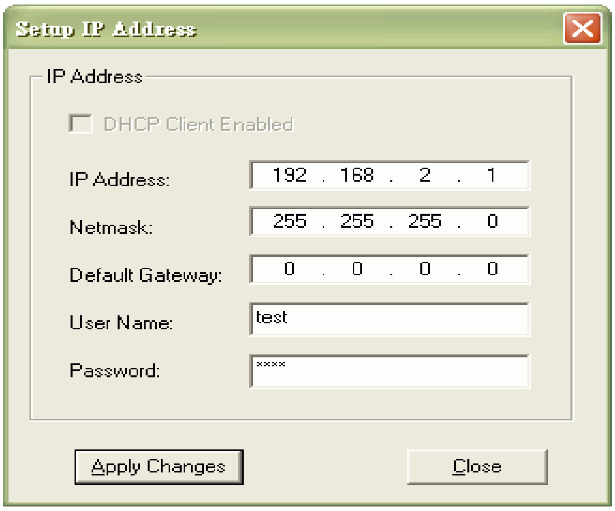
1. Discover

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
- Channel number
- MAC Address
- Active Client: this field shows how many clients associated with the device
- RSSI: this field shows Received Signal Strength I indication while device is on AP-Client mode

2. 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.



Setup IP Address

IP Address

□ DHCP Client Enabled

IP Address: 192 . 168 . 2 . 1

Netmask: 255 . 255 . 255 . 0

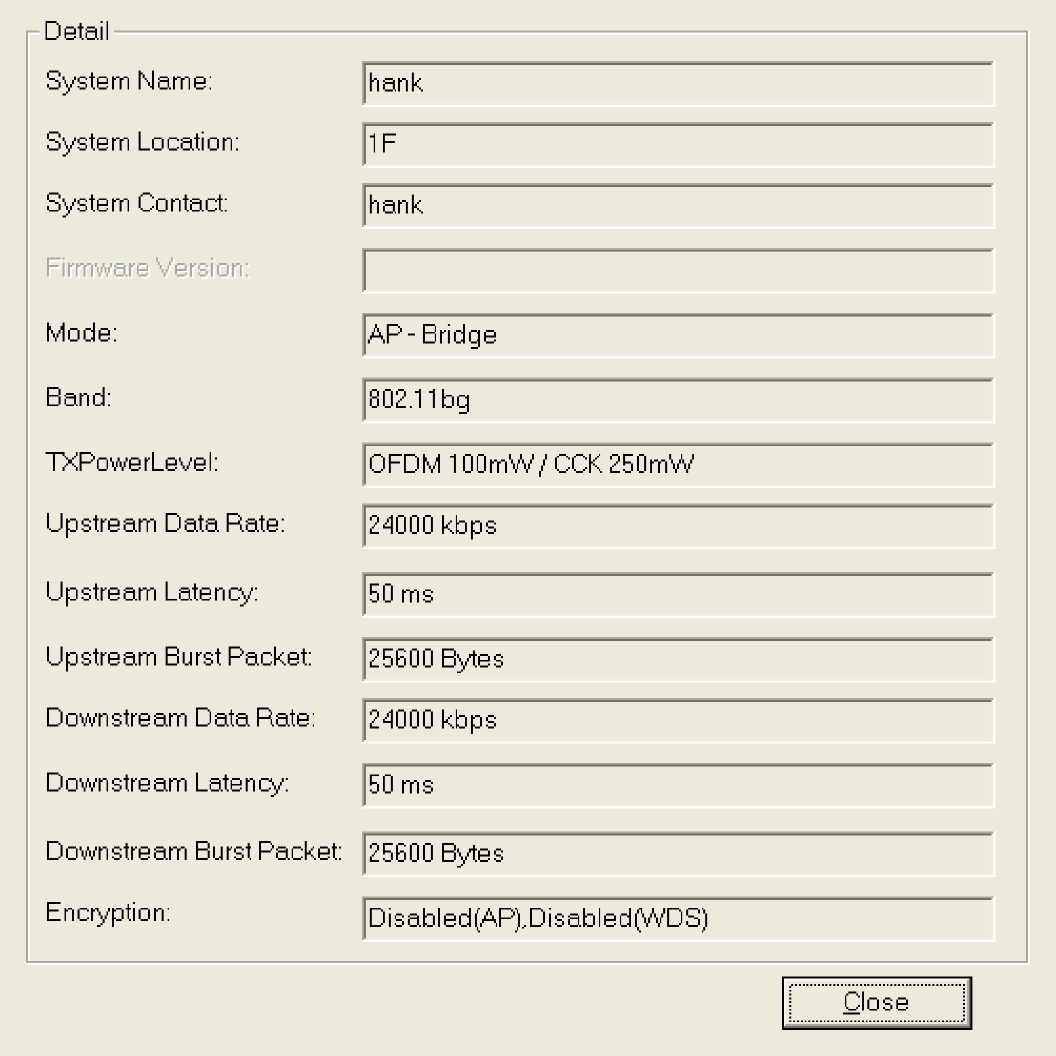
Default Gateway: 0 . 0 . 0 . 0

User Name: test

Password: ****

3. **Detail.**

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

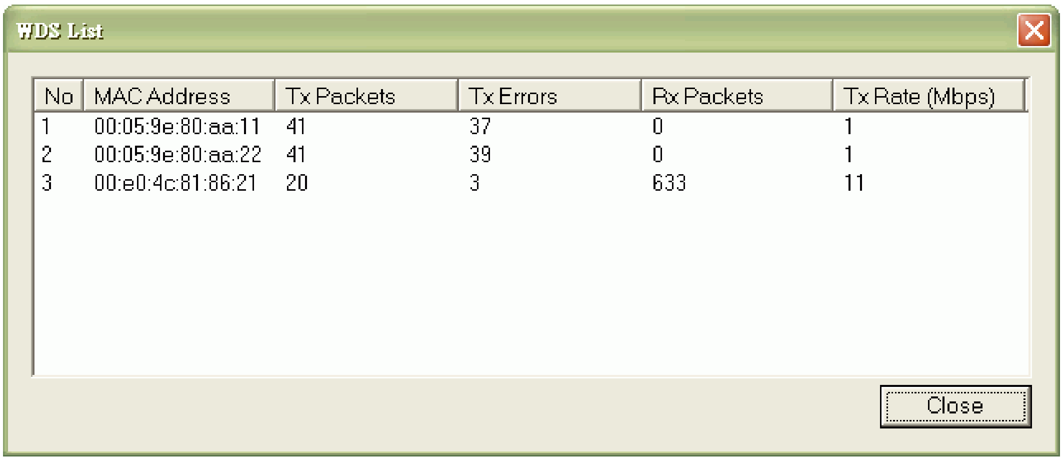


Detail

System Name:	hank
System Location:	1F
System Contact:	hank
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)

4. **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

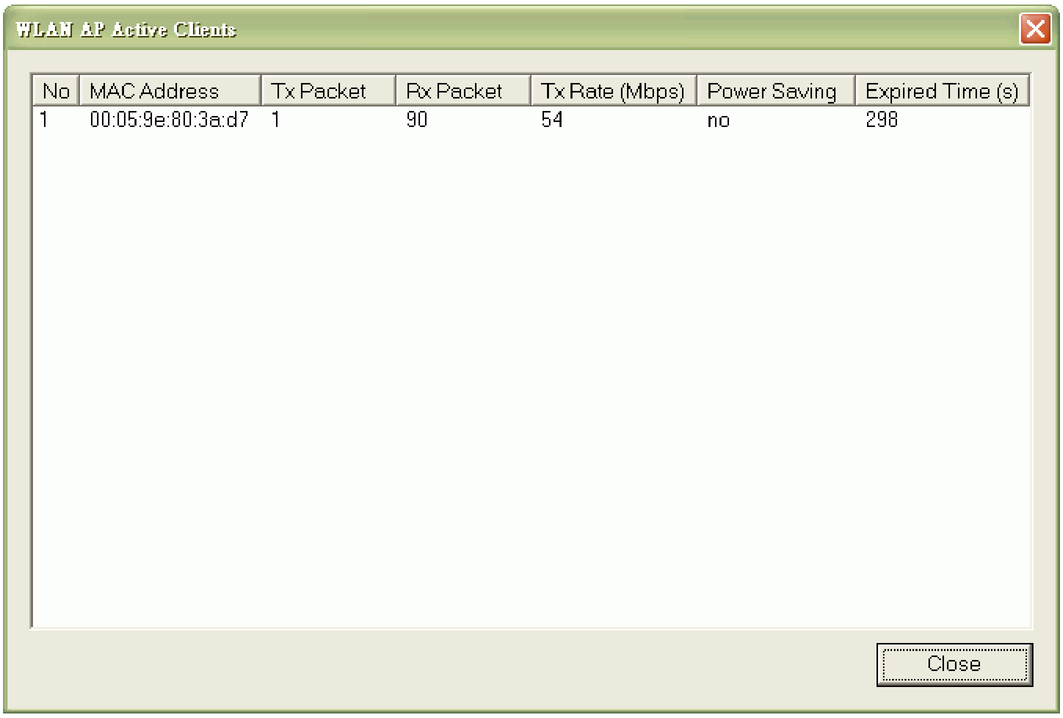


WDS List

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

5. **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:



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

6. **Connect to Web Server**

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

7. **Close**

You could press this button to leave this tool.