

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:** 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

The screenshot shows the 'WAN Interface Setup' page for a 'Wireless LAN Series' device. The left sidebar contains a 'Site contents' menu with options: Wizard, Operation Mode, Wireless, TCP/IP, LAN Interface, WAN Interface, Route, Firewall, Management, and Reboot. The main content area is titled 'WAN Interface Setup' and includes a description: '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.' The 'WAN Access Type' is set to 'DHCP Client'. Below this, there are radio buttons for 'Attain DNS Automatically' and 'Set DNS Manually', with 'Set DNS Manually' selected. There are three input fields for 'DNS 1:', 'DNS 2:', and 'DNS 3:'. The 'Clone MAC Address' field is highlighted with a red box and contains the value '001122334455'. Below this are several checkboxes: 'Enable uPNP' (unchecked), 'Enable Web Server Access on WAN' (checked), 'Enable IPsec pass through on VPN connection' (unchecked), 'Enable PPTP pass through on VPN connection' (unchecked), and 'Enable L2TP pass through on VPN connection' (unchecked).

2. Clone MAC address for Static IP WAN access type

The screenshot shows the 'WAN Interface Setup' page for a 'Wireless LAN Series' device. The left sidebar contains a 'Site contents' menu with options: Wizard, Operation Mode, Wireless, TCP/IP, LAN Interface, WAN Interface, Route, Firewall, Management, and Reboot. The main content area is titled 'WAN Interface Setup' and includes a description: '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.' The 'WAN Access Type' is set to 'Static IP'. Below this are input fields for 'IP Address:' (172.1.1.1), 'Subnet Mask:' (255.255.255.0), and 'Default Gateway:' (172.1.1.254). There are three input fields for 'DNS 1:', 'DNS 2:', and 'DNS 3:'. The 'Clone MAC Address' field is highlighted with a red box and contains the value '001122334455'. Below this are several checkboxes: 'Enable uPNP' (unchecked), 'Enable Web Server Access on WAN' (checked), 'Enable IPsec pass through on VPN connection' (unchecked), 'Enable PPTP pass through on VPN connection' (unchecked), and 'Enable L2TP pass through on VPN connection' (unchecked).

3. Clone MAC address for PPPoE WAN access type

The screenshot shows the 'WAN Interface Setup' page for a 'Wireless LAN Series' device. The left sidebar contains a 'Site contents' menu with options: Wizard, Operation Mode, Wireless, TCP/IP, LAN Interface, WAN Interface, Route, Firewall, Management, and Reboot. The main content area is titled 'WAN Interface Setup' and includes a description: '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.' The 'WAN Access Type' is set to 'PPPoE'. Below this are input fields for 'User Name:' (87043609@hinet.net) and 'Password:' (masked with dots). There is a 'Connection Type' dropdown set to 'Continuous' with 'Connect' and 'Disconnect' buttons. There are input fields for 'Idle Time:' (5 minutes) and 'MTU Size:' (1412 bytes). There are radio buttons for 'Attain DNS Automatically' and 'Set DNS Manually', with 'Set DNS Manually' selected. There are three input fields for 'DNS 1:', 'DNS 2:', and 'DNS 3:'. The 'Clone MAC Address' field is highlighted with a red box and contains the value '001122334455'. Below this are several checkboxes: 'Enable uPNP' (unchecked), 'Enable Web Server Access on WAN' (checked), 'Enable IPsec pass through on VPN connection' (unchecked), 'Enable PPTP pass through on VPN connection' (unchecked), and 'Enable L2TP pass through on VPN connection' (unchecked).

4. Clone MAC address for PPTP WAN access type

Wireless LAN Series

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

Wireless LAN Series

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](#)

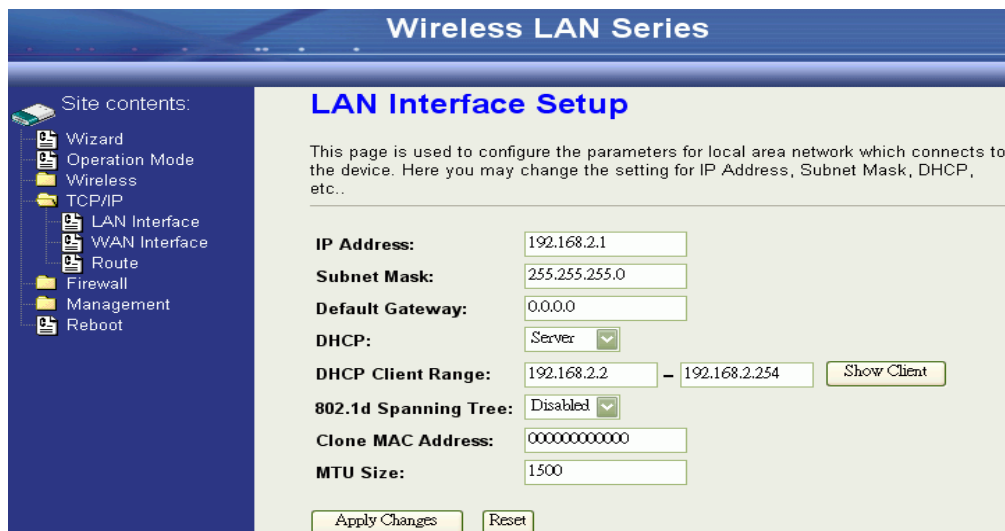
802.1d Spanning Tree: Disabled

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.



Wireless LAN Series

Site contents:

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

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

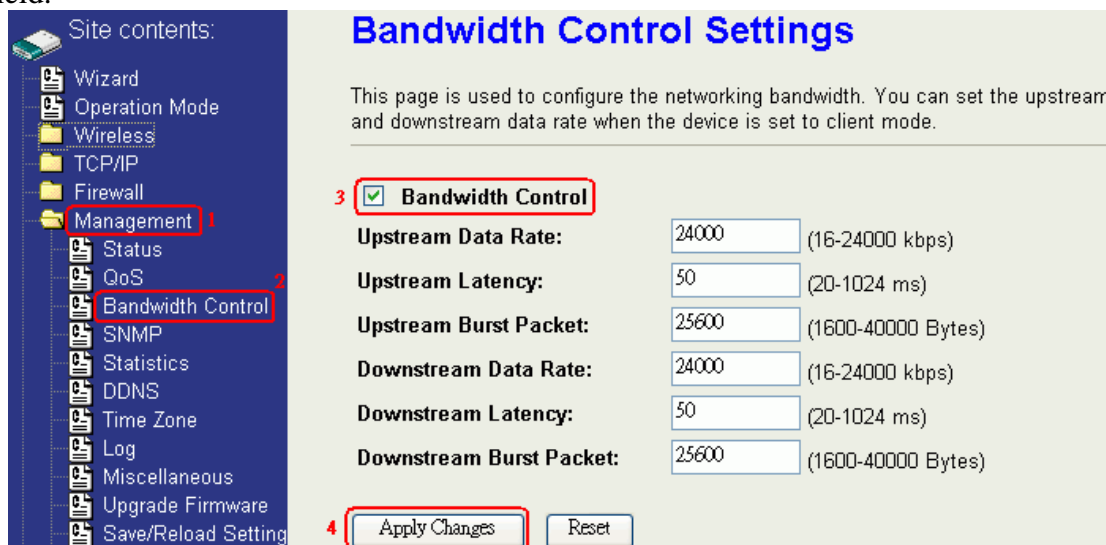
Apply Changes Reset

- 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

- 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
 - Status
 - QoS
 - Bandwidth Control
 - SNMP
 - Statistics
 - DDNS
 - Time Zone
 - Log
 - Miscellaneous
 - Upgrade Firmware
 - Save/Reload Setting

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)

Apply Changes Reset

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)

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%.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
 - Status
 - QoS
 - Bandwidth Control
 - SNMP
 - Statistics
 - DDNS
 - Time Zone
 - Log

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.

3 ☒ **QoS Enabled**

☒ **Bandwidth Borrowed**

Max Throughput : (kbps)

Bandwidth Ratio (H/M/L): 4 : : (%)

5

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 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 :	<input type="text"/>
Source Netmask :	<input type="text"/>
Destination IP Address :	<input type="text"/>
Destination Netmask :	<input type="text"/>
Source MAC Address :	<input type="text"/>
Destination MAC Address :	<input type="text"/>
Source Port / range:	<input type="text"/> to <input type="text"/>
Destination Port / range:	<input type="text"/> to <input type="text"/>
Protocol:	<input type="text" value="v"/>
Bandwidth Priority:	<input type="text" value="v"/>
Filter Priority:	<input type="text" value="v"/> (Lower number, Higher Priority)
IP TOS Set:	<input type="text" value="v"/>
<input type="button" value="Apply Changes"/> <input type="button" value="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.
-------	---

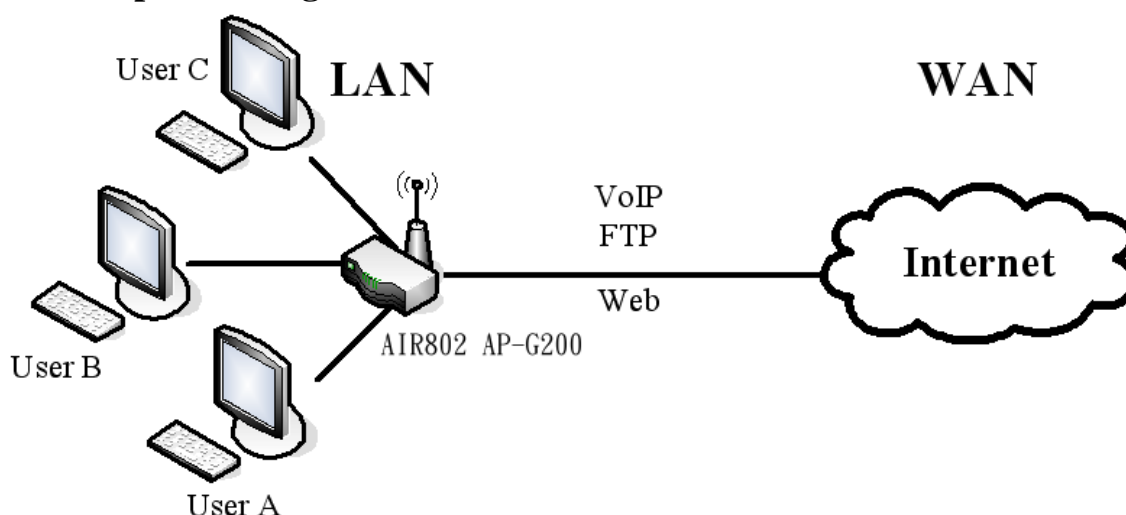
Current QoS setting table

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 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.

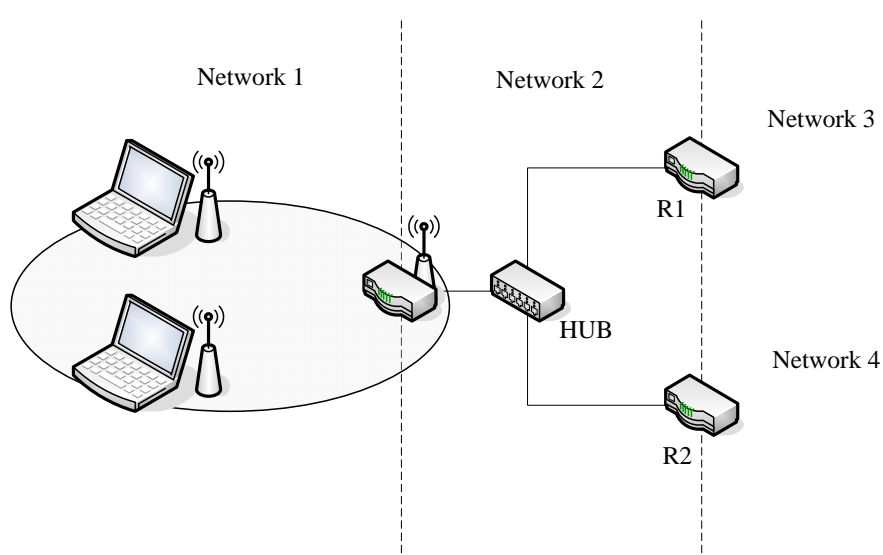
The voice is sensitive to the variations in delay; you can set **High** priority for **User C**. The FTP transmission may take a long time; you can set **Low** priority for **User B**.

Current QoS Setting:
(Mask 255.255.255.255 means single host)

Src 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	<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 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:

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.

☒ Enable Dynamic Route
 RIP transmit to WAN:
 RIP receive from WAN:
 RIP transmit to LAN:
 RIP receive from LAN:

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 4

Routing Table

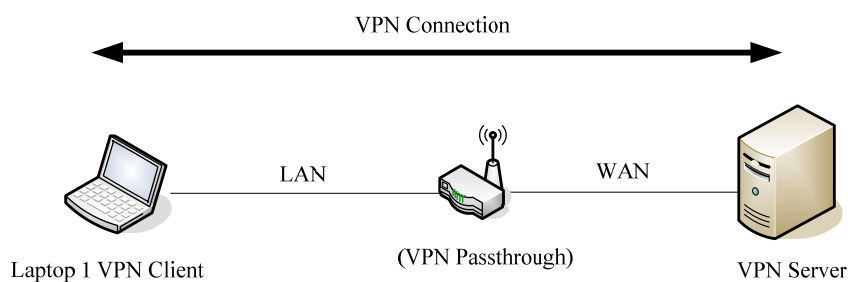
This table shows the all routing entry .

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

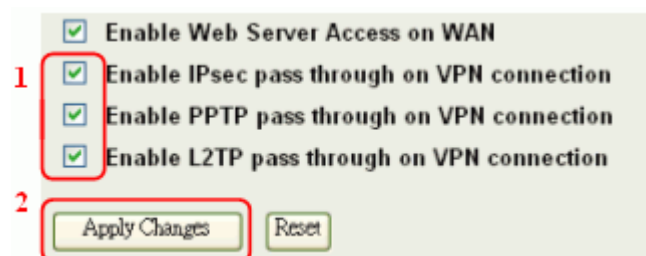
Refresh Close

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

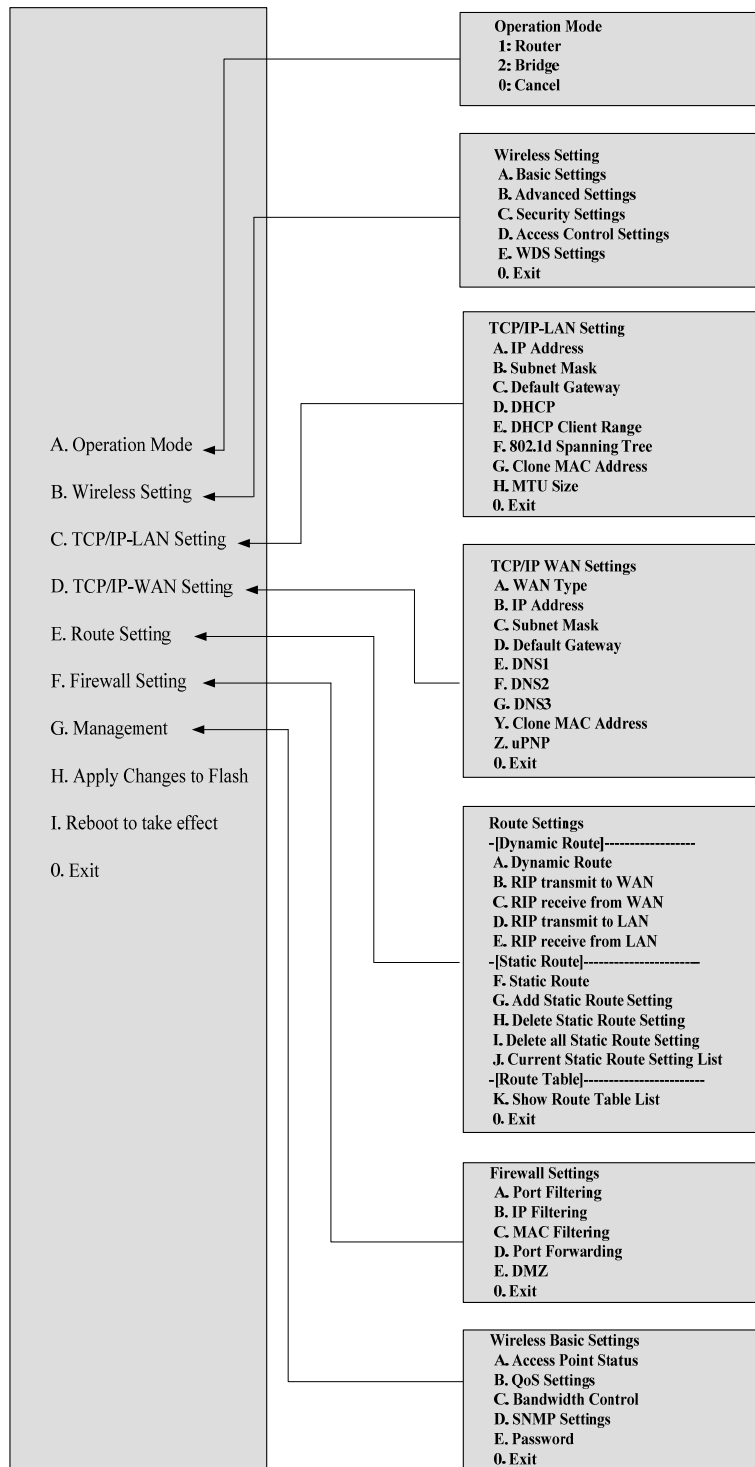
Start a SSH(Secure Shell) client session to login the device

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

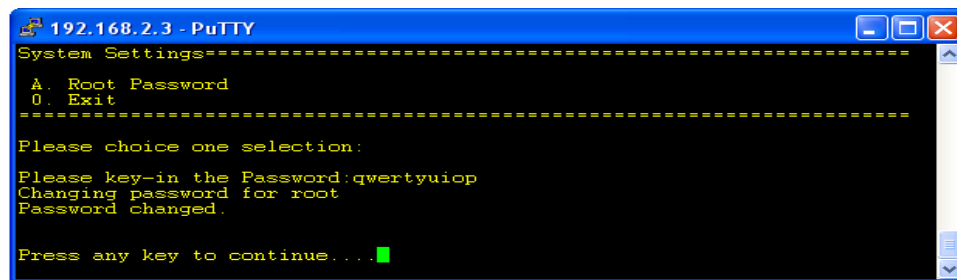
Password Protection

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



The screenshot shows a web browser window titled "Wireless LAN Series". On the left is a navigation menu with items: Site contents, Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management (highlighted), Status, Statistics, DDNS, Time Zone, Log, Upgrade Firmware, Save/Reload Setting, Password, and Reboot. The main content area is titled "Password Setup" and contains the following text: "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 text are three input fields: "User Name:", "New Password:", and "Confirmed Password:". At the bottom of the form 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.



The screenshot shows a PuTTY terminal window titled "192.168.2.3 - PuTTY". The terminal displays the following text: "System Settings====", "A. Root Password", "0. Exit", "====", "Please choice one selection:", "Please key-in the Password:qwertyuiop", "Changing password for root", "Password changed.", and "Press any key to continue....".

To change the password of user "root" for SSH session, please use the CLI menu item G. System Setting→A. Root 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.

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

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: hank

System Location: 1F

System Contact: hank

Trap Receiver IP Address1: 4 192.168.2.11

Address1 Community String: hank

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
.1.3.6.1.4.1.99.7.101.1	MAC Data Rate RSSI 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	AP-WEP 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 **g200webpage.bin** and **g200linux.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.

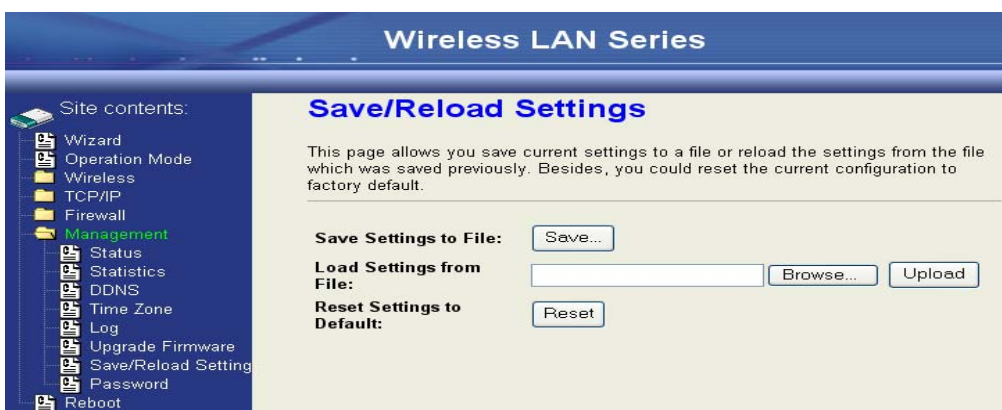


Configuration Data Backup & Restore

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

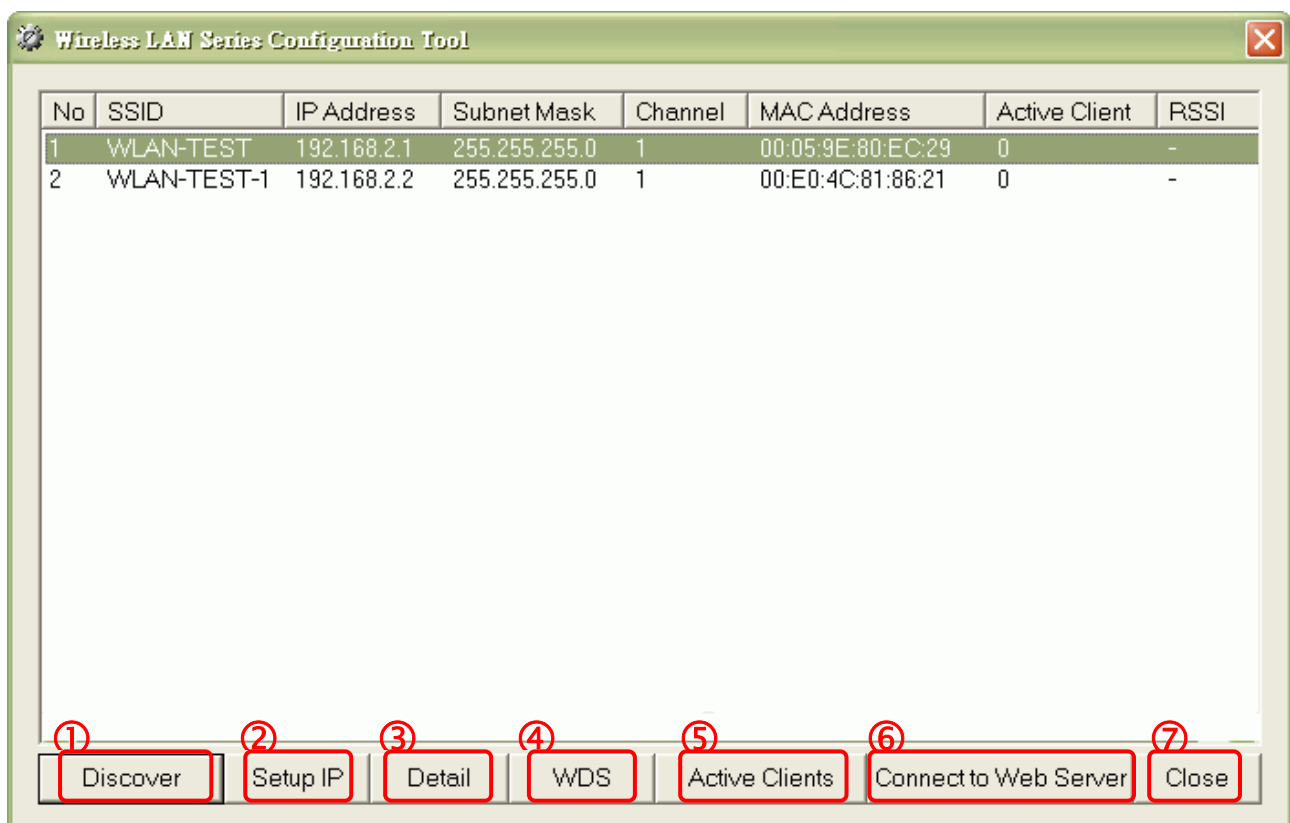


To save & restore configuration data of device, just assign the target filename with full path at your local host, then you can backup configuration data to local host or restore configuration data to the device.

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.



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 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.

The screenshot shows a 'Setup IP Address' dialog box. It contains a checkbox for 'DHCP Client Enabled' which is currently unchecked. Below the checkbox are five input fields: 'IP Address' with the value '192 . 168 . 2 . 1', 'Netmask' with '255 . 255 . 255 . 0', 'Default Gateway' with '0 . 0 . 0 . 0', 'User Name' with 'test', and 'Password' which is masked with 'x's. At the bottom of the dialog are two buttons: 'Apply Changes' and 'Close'.

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.

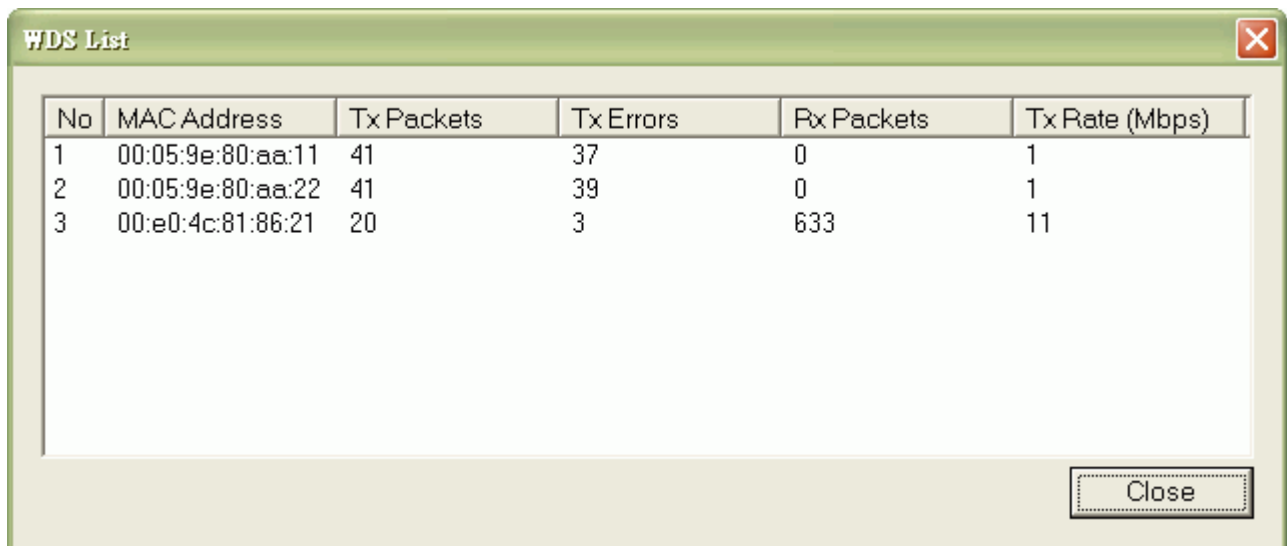
Detail

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)

Close

4. WDS

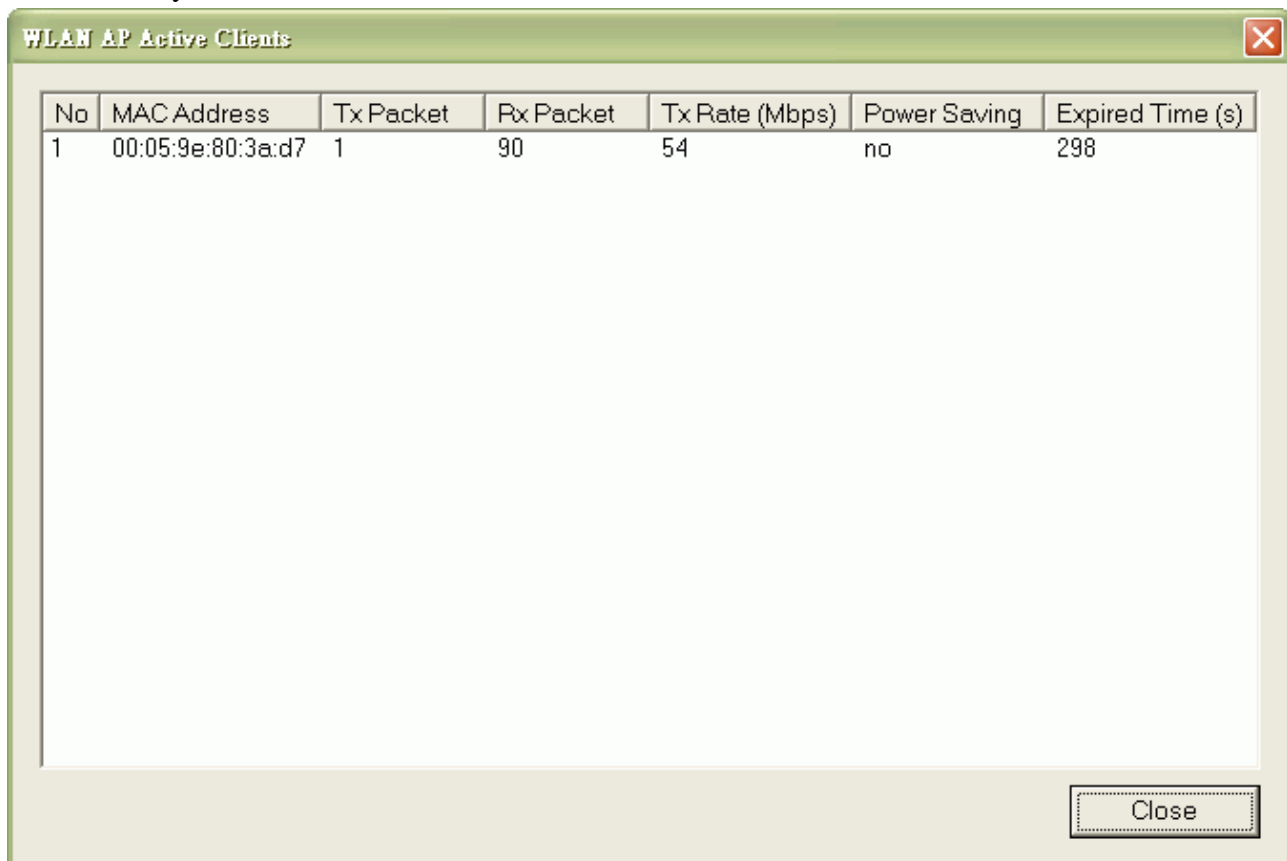
If the device you selected is on WDS mode or AP+WDS mode, you could press **WDS** button, and then you would see the **WDS List** window.



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.

Appendix A

Bridged Wireless Network Configuration

This configuration is for an application where there are two different wireless networks. For example, you are in a home, yacht or office where there are multiple computers on a wireless network. Perhaps the only access to broadband networks is a WiFi Broadband wireless network. Typical home broadband wireless routers such as manufactured by, Linksys, DLink, etc. are designed for use with DSL or Cable Modem as the Wide Area Network (WAN) or broadband access. The wireless computers connected to the home broadband router access the Internet via the Broadband wired interface (the DSL or Cable Modem). This configuration utilizes an AIR802 AP-G200 Indoor Wireless router plus a home networking router, which may or may not already exist.



If you already have a wireless broadband router, then it can be used in this application to provide your computers wireless network connectivity. If you don't have a wireless broadband router existing, there are many on the market, such as the Linksys WRT-54G or WRT-54GS models. The AIR802 AP-G200 router will be the client device to an outside wireless network access point. This means the AP-G200 will pickup the wireless network desired in your area. Then the two routers will be hard wired together for a bridged network between your internal wireless network and the exterior network.

1. Powering

The AP-G200 is powered through a power-over-Ethernet (PoE) injector. The AP-G200 does not plug directly into an AC power outlet. The PoE injector has two modular plug connections. They are labeled: DATA IN and P+DATA OUT. A third connection is for the power transformer connection to the AC outlet. The connection labeled P+DATA OUT will have an Ethernet (Cat5, Cat5e) type cable between this connector and the

AP-G200. There is 48VDC power carried on extra pairs in the Ethernet cable. The other connection is labeled, "DATA IN". This will be connected to the home broadband wireless router such as the Linksys WRT-54G. See Photo, "A" above.

2. Antenna Installation for the AIR802 AP-G200

Before configuring the AP-G200, the antenna should be installed. For your application, an antenna for outdoor installation probably was chosen for the most effective coverage of networks in your installation area. A professional grade cable should be chosen. AIR802 recommends for longer distance than 20 to 30 foot, a 400 series coaxial cable assembly. Otherwise a 195 series cable assembly should be adequate. The AP-G200 requires a RP-SMA plug for mating. Most outdoor antennas use N (male) type connectors. Your cable assembly should be purchased with the correct connector types at each end.

For the most professional installation and to meet the National Electric Code requirements, you should also purchase a lightning protector to be inserted into the coax line. This in turn will have a ground wire connected to earth ground.

3. Gaining Configuration Access to the AIR802 AP-G200 Router

If you have already installed the cable between the PoE injector's (DATA IN) connector and the home wireless broadband router, remove the end of the cable from the home broadband wireless router. Plug it into the Ethernet port of a computer. There are two ways to configure the AP-200, either through a configuration tool on the CD or by directly entering the default address into the web browser. Choose either method (a) or (b) listed below. Before doing so, you should power down and back up your computer.

- a) Insert the CD and click on the file labeled, "WirelessConf" to access the configuration tool.
- b) Alternatively you may access the configuration directly by entering the default IP address into a web browser like, Microsoft Internet Explorer. Instead of entering a web address, clear the space and enter 192.168.2.254. Then press the enter key. You should be directed to the configuration screen.

If you have not gained access at this point, it maybe that your computer does not have its TCP/IP Properties set to "Obtain an IP address automatically" Your computer must be on the same network as the AP-G200. The default IP address of the device is

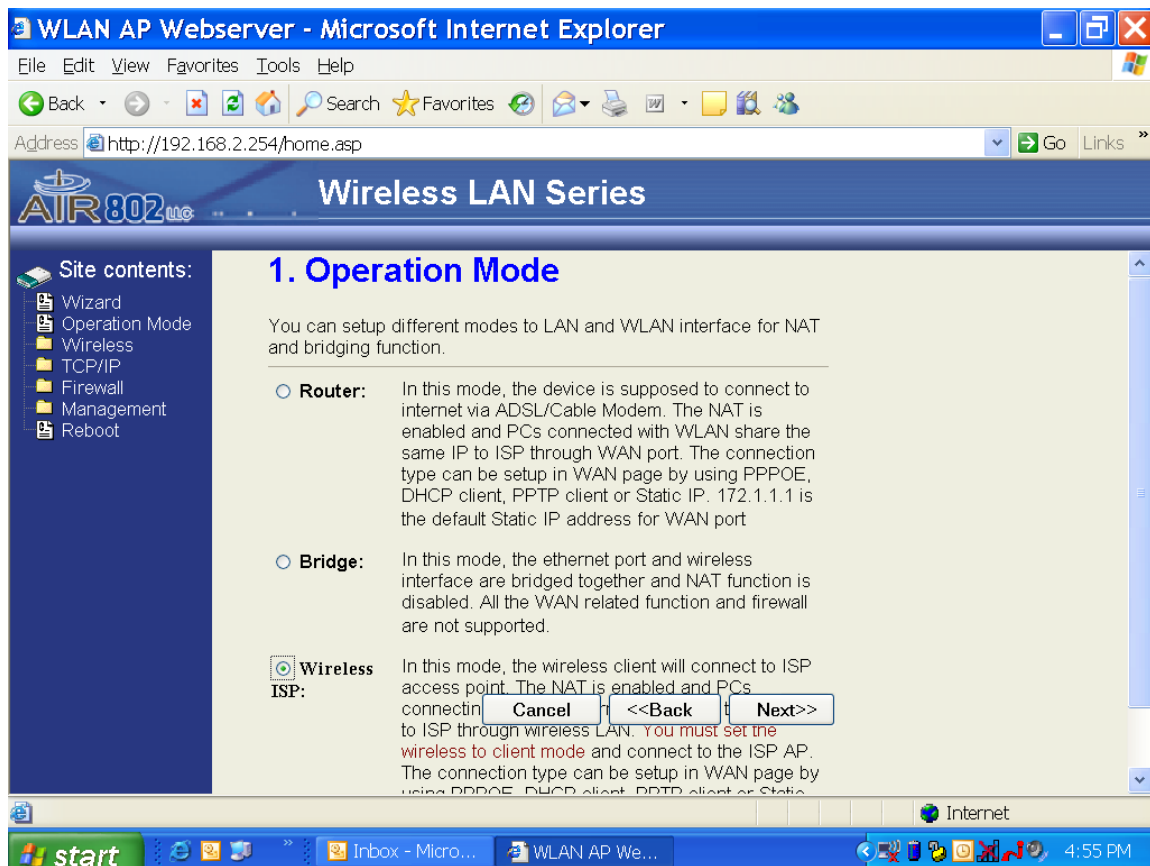
192.168.2.254 and the subnet mask is 255.255.255.0. For example in Microsoft Windows XP, you will need to click under the control panel, then Network Connections, then Local Area Connection, then scroll down to Internet Protocol (TCP/IP), highlight it and click on Properties. If your computer has the “Use the following IP address” clicked with an IP address entered below, you will either need to change it or click, “Obtain an IP address automatically”. Then retry.

4. Configuring the AIR802 AP-G200

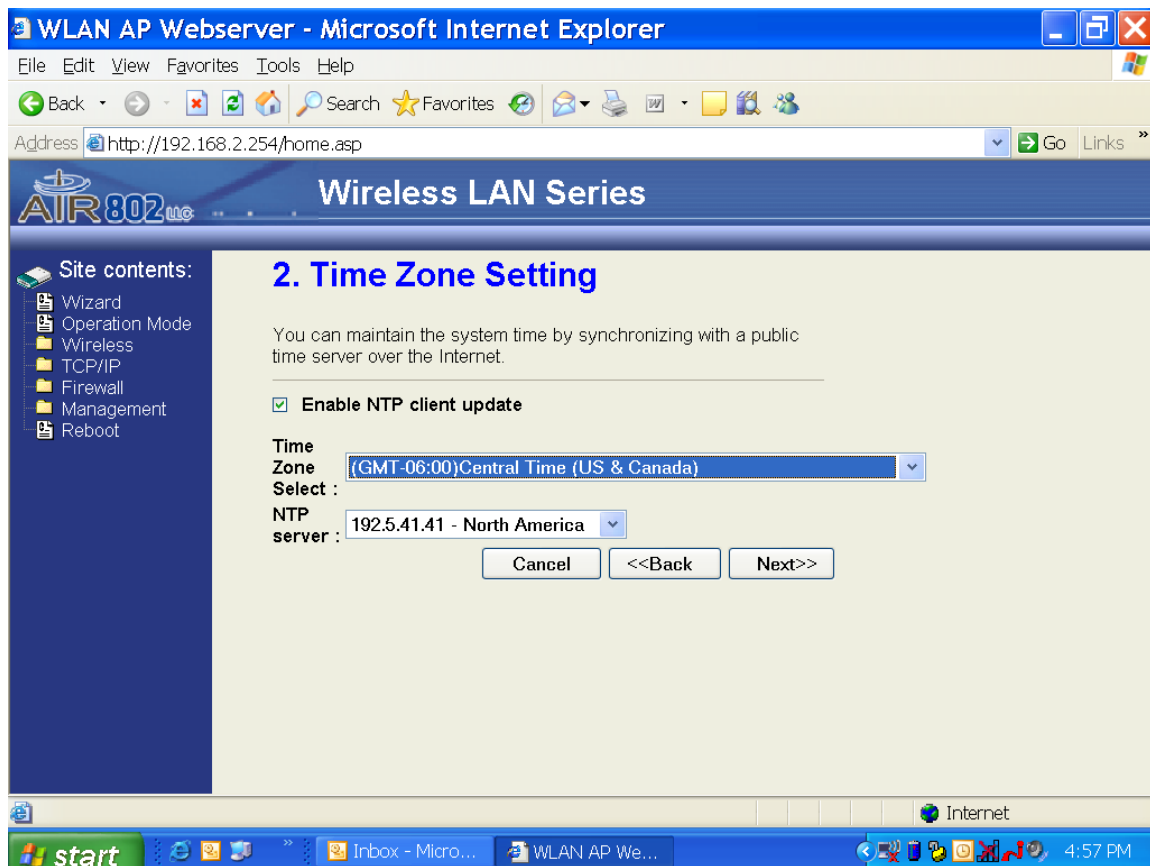
If you have gained access, you should have the screen shown below:



Click “Next>>”. The following screen should appear:



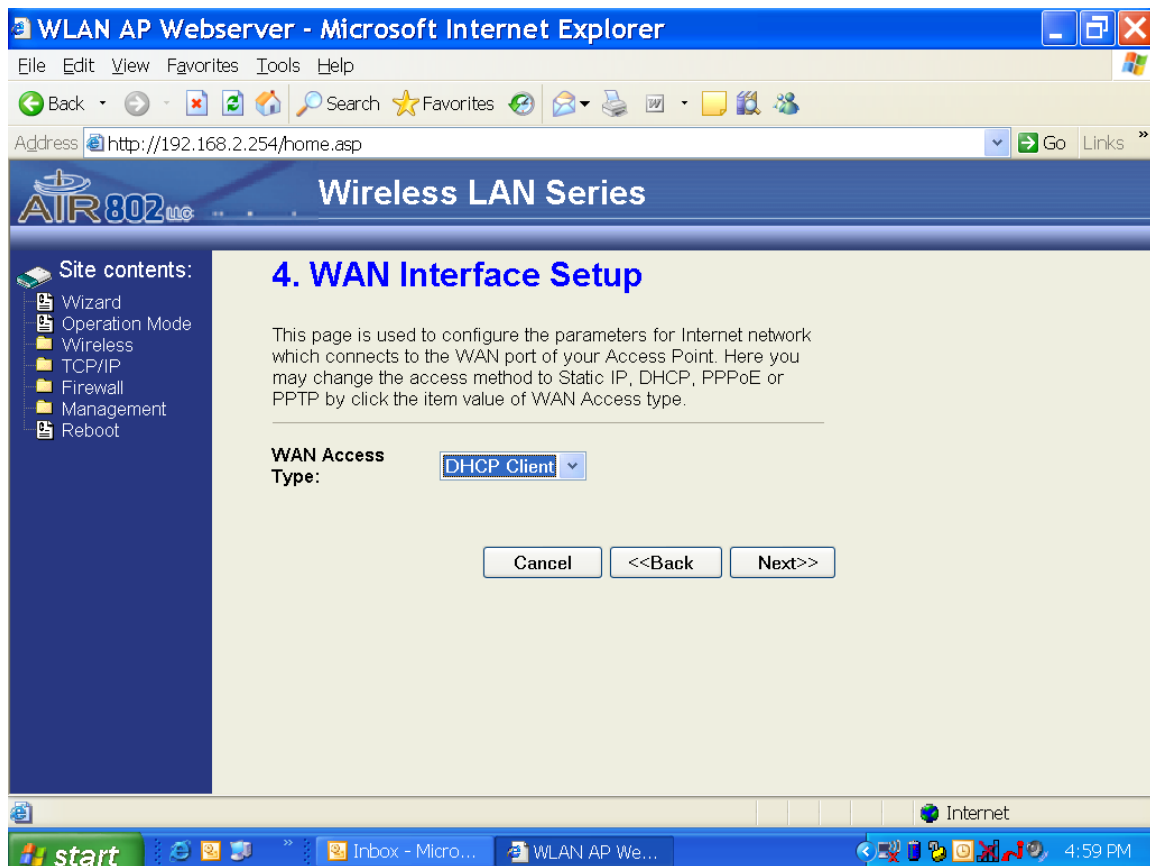
Click the option, “Wireless ISP” and then “Next>>”. The following screen should appear:



You may elect to either click “Enable NTP client update” and selecting the proper time zone and location or click, “Next>>”. Once finished, the following screen should appear:



The default address will be used by most folks. Do not attempt to change this information unless you are an experienced networking professional. Click "Next>>". The following screen should appear:



The WAN interface screen will not have DHCP Client as the default value. Please use the drop down menu and select DHCP client for this application. Then click, “Next>>” and the following screen should appear:



The band should be set as shown for both (B+G) in order to receive all possible networks in your area. The Mode will need to be set to “Client”. The Network Type will be Infrastructure. You will need to set the SSID. This is the name of the transmitting access point that you are attempting to gain access. You may not know the SSID. In this case, on the left-hand side of the screen, click on “Wireless”, followed by a click on, “Site Survey”. After you have the Wireless Site Survey page, click on “Refresh”. A list of the available networks will appear. Click on “Select” to the right of the SSID you choose to be a client. You may elect to click back on the right-hand side, the “Basic Settings” tab and double check that your SSID is now shown.

Note: If you move from one location to another, as in a yacht moving from one marina to another, then you will need to reset the SSID to the network of your new location.

The only other screen that you might need to consider for basic considerations is the “Security” tab on the right-hand side. This screen is shown below:



Here you can options for Encryption as: None or one of various encryption levels as they may apply to your network. Likely for your configuration, you will be selecting none, if you are accessing a public access point.

At this point, simply close the browser. Remove the cable from your computer and plug it back into the WAN (DSL or Cable Modem) port on the home broadband wireless router. Wait one or two minutes for the routers to establish communication. The computers in your network should now be communicating with the home broadband wireless network router and through the AIR802 AP-G200 into the public accessible network.



Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.