AboCom Systems, Inc.

WR5510

WLAN 802.11b/g/n Router

User's Manual

Release 1.0

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 or more 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 needed.
- ☐ Consult the dealer or an experienced radio/TV technician for help.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

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.

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CAUTION:

1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

Table of Content

Chapter 1: Introduction

The wireless router will be the corner stone of retail push. The router will be a low cost “turn key” solution to allow us to offer a 802.11b/g/n router at retail at a low price point to draw traffic.

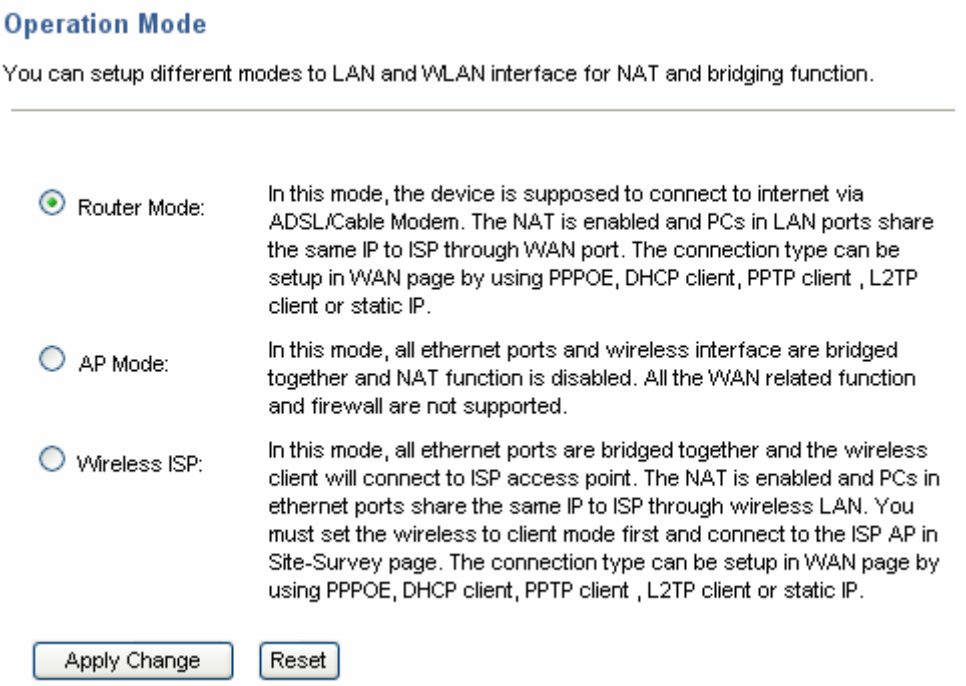
The Wireless Router is a draft 802.11n/b/g compliant Wireless Broadband Router with 4-port Fast Ethernet Switch. With the advanced MIMO technology, it can support the data transmission rate 6 times more (up to 150 Mbps) and the coverage 3 times more than IEEE 802.11b/g devices. The Wireless Router enables your whole network sharing a high-speed cable or DSL Internet connection. With it, you can share a high-speed Internet connection, files, printers, and multi-player games at incredible speeds, without the hassle of stringing wires. It also offers easy configuration for your wireless network in the home and presents wireless network to you home of high functionality, security, and flexibility.

Features

1. 4 ports 10/100M Ethernet switch interface for LAN
2. One 10/100M Ethernet interface for WAN
3. NAT function support
4. Ability to upgrade firmware and back-up configuration via web interface
5. ACL function support
6. Support passive PoE 12V/DC

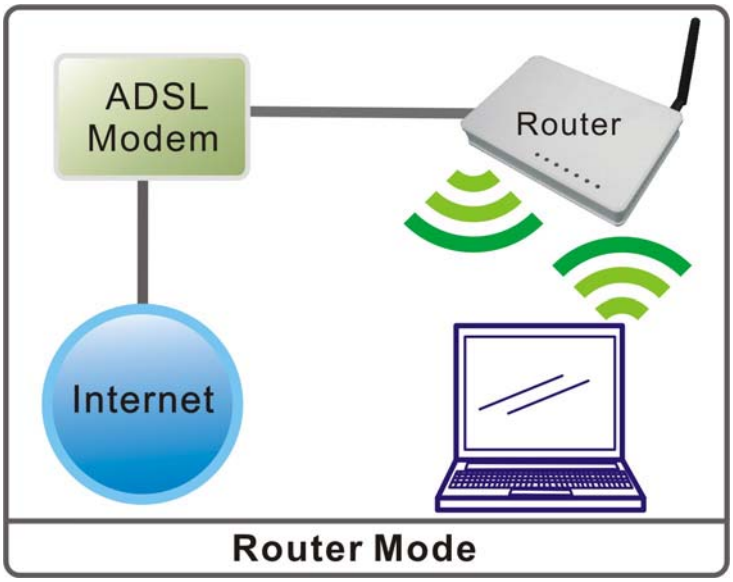
Chapter 2: About Operation Modes

This device provides operational applications with Router, AP and Wireless ISP modes, which are mutually exclusive.
If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can select the mode you desired by the manufacturer as described in the following sections.
The default setting mode is Router mode.



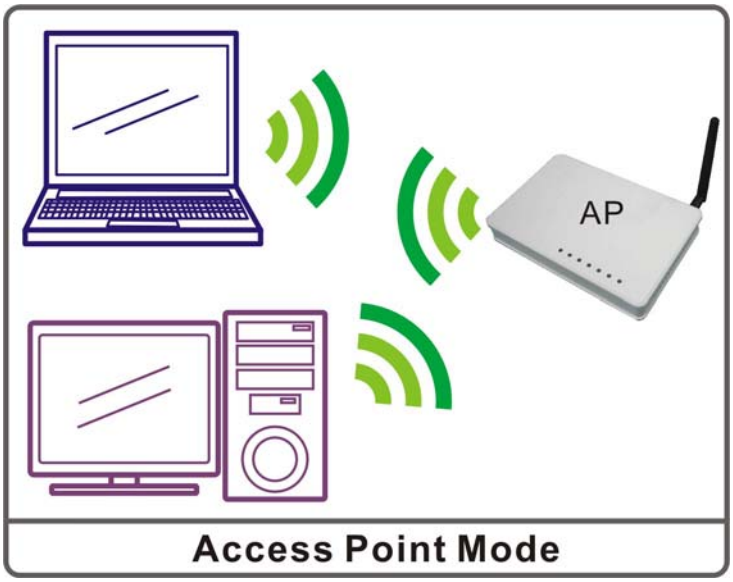
Router Mode

In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.



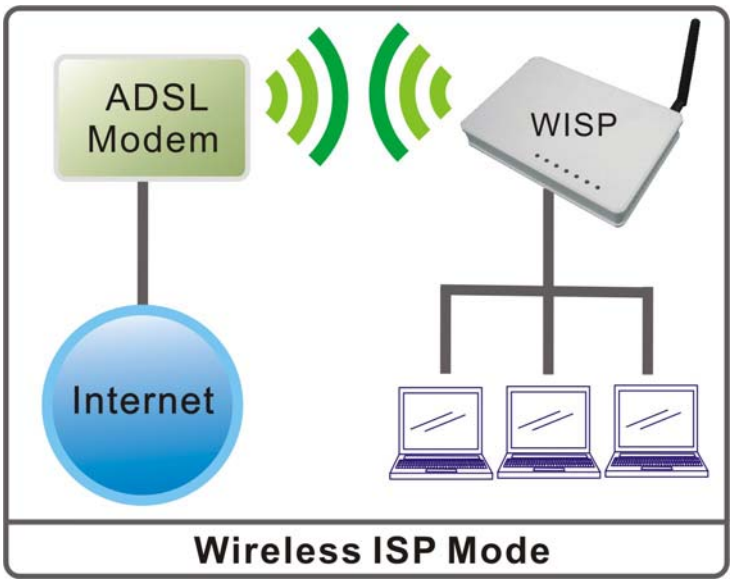
Access Point Mode

When acting as an Access Point (AP), this device connects all the stations (PC/notebook with wireless network adapter) to a wireless network. All stations can have the Internet access if only the Access Point has the Internet connection.



Wireless ISP

In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

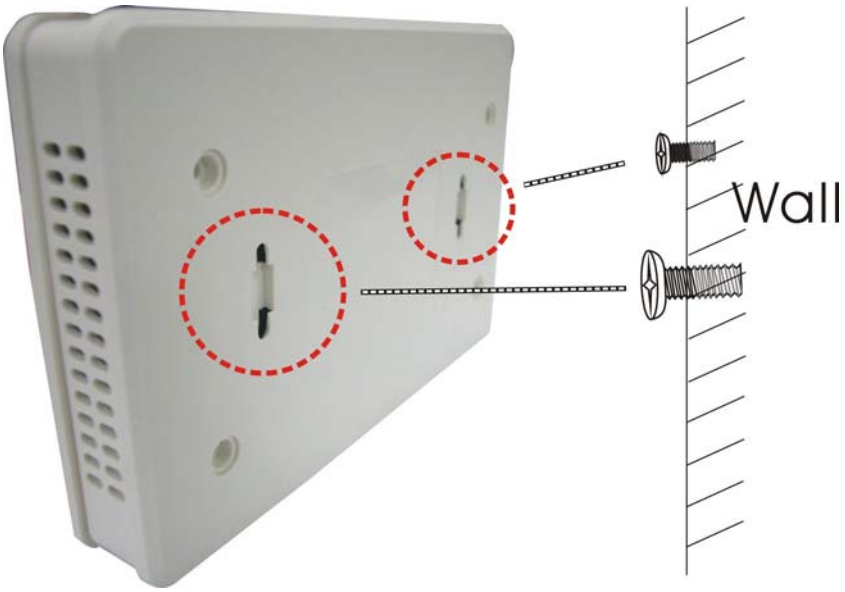


Chapter 3: Configuration

Hardware Mounting

The Wireless Router is designed to arrange on a raised flat surface like a file cabinet or a book shelf. The unit may also be converted for mounting to a wall or ceiling.

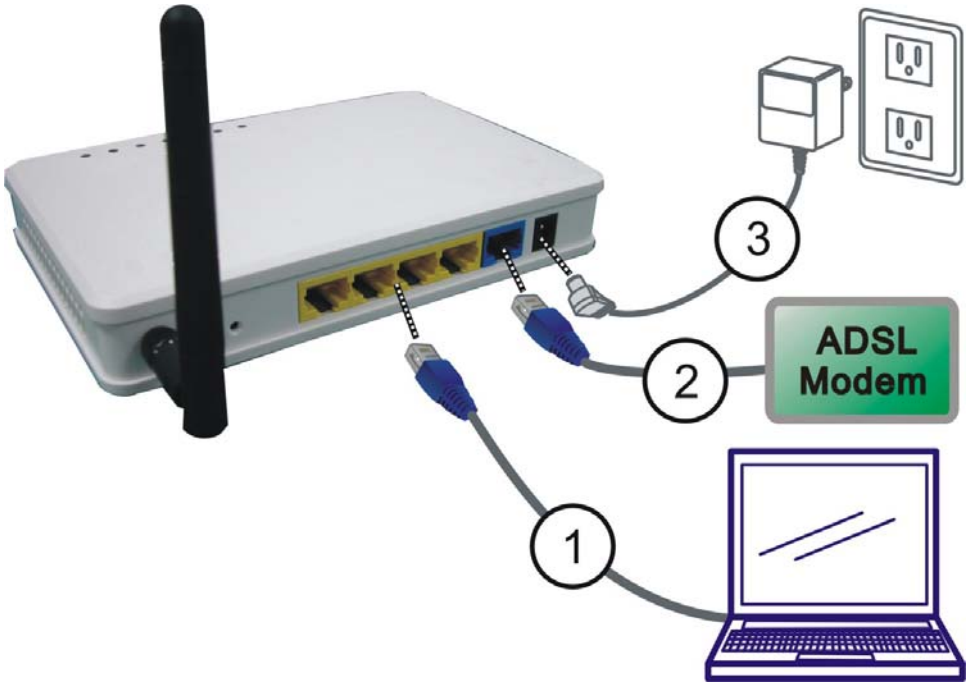
1. There are two mounting hooks on the underside.
2. Mark two upper holes on a wall or on a raised flat surface.
3. Drill the appending two screws on the flat surface until only 1/4" screws is showing.
4. Then, hang the Wireless Router onto the screws.



Note:
Please re-adjust the screws if you cannot hang the Wireless Router onto the screws or if it is loose.

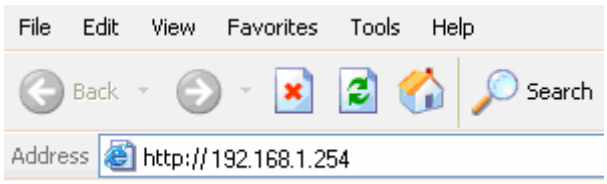
Hardware Connection

1. Connect one end of the Ethernet cable to the LAN port of the Wireless Router, another end to your PC or notebook.
2. Then, connect another Ethernet cable one end to the Internet port of the Wireless Router, the other end to the ADSL or cable modem.
3. Finally, connect the Wireless Router with a power to an outlet.



Login

1. Start your computer and make sure the connection by an Ethernet cable between your computer and the Wireless Router.
2. Start your Web Browser, in the address box, enter the IP address of the Wireless Router 192.168.1.254
3. Then press the “Enter” key to login.



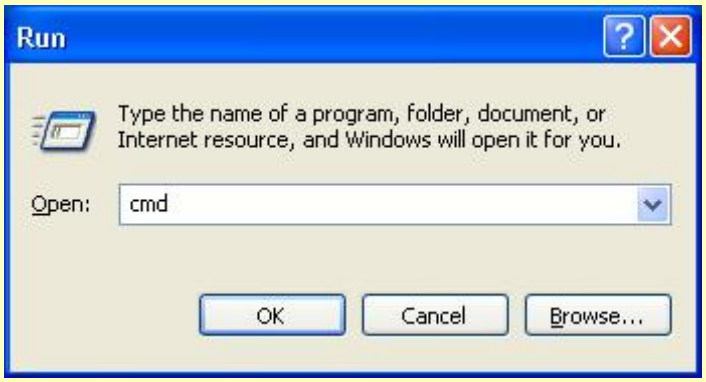
4. After connected successfully, the following screen will show up.

After login successfully, please click the **Setup Wizard** item that provides a primary configuration of this device. You may enter each screen to change the default settings step by step.

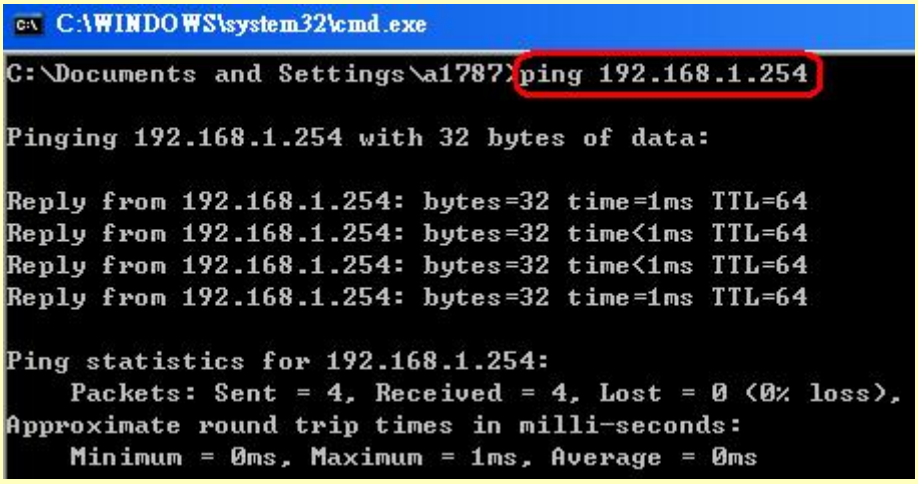
If you cannot connect...

If the Wireless Router does not respond, please check following:

- The Wireless Router is properly installed, LAN connection is OK, and it is already powered ON. You can test the connection by using the **"Ping"** command:
  - Please go to **Start>Run…**> Enter "**cmd**" command in the column to open the MS-DOS window.



  - Enter the command: **ping 192.168.1.254**



    If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Router's IP Address. (See next item.)

- If your PC is using a fixed IP address, its IP address must be within the range 192.168.1.1 to 192.168.1.253 to be compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network *Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

Common Connection Types

Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.

DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	• PPTP Server IP Address. • User name and password. • IP Address allocated to you, if Static (Fixed).
L2TP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	• L2TP Server IP Address. • User name and password. • IP Address allocated to you, if Static (Fixed).

Other Modems (e.g. Broadband Wireless)

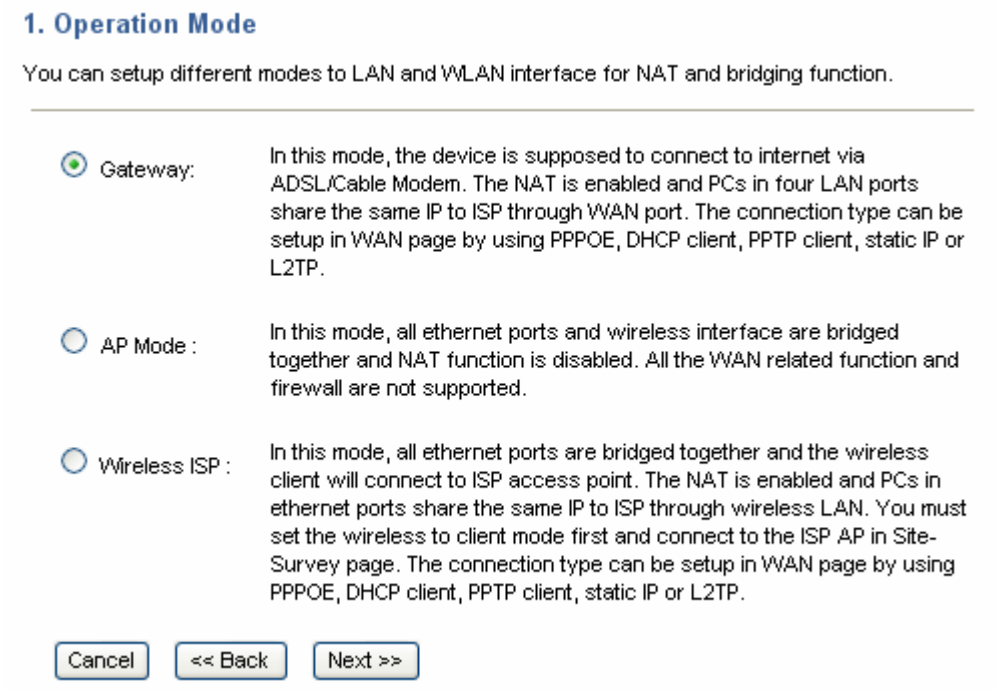
Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Step 1- Operation mode

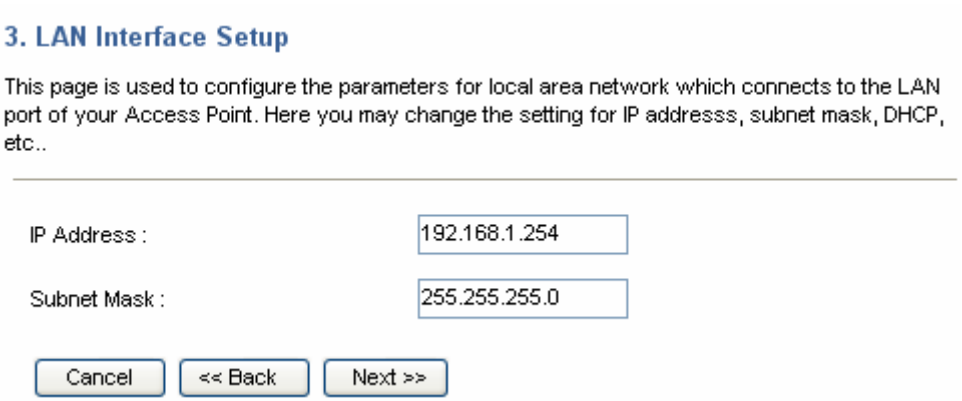
User can select the operation modes here to LAN and WLAN interface for NAT and bridging function.



Step 2- Time Zone Setting

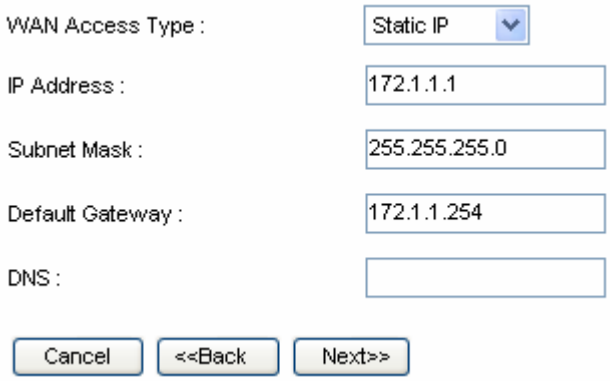
NTP Settings	
Enable NTP client update	Check the box to synchronize the time with the host PC.
Automatically Adjust Daylight Saving	Check the box to automatically adjust daylight saving.
Time Zone	Select the time zone area that you located from the pull-down list.
NTP Server	Enter the Network Time Protocol Server here. Ex: time.nist.gov, ntp0.broad.mit.edu, or time.stdtime.gov.tw.

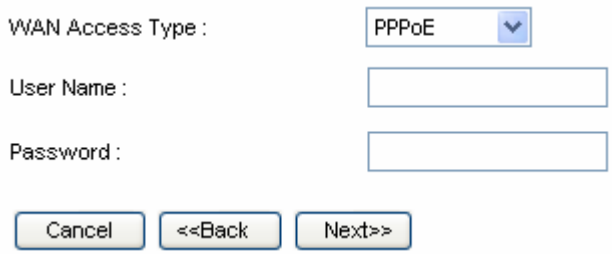
Step 3- LAN Interface Setup



IP Address	Shows the IP address of the Wireless Router (Default IP address is 192.168.1.254.)
Subnet Mask	The subnet mask of the Wireless Router (Default subnet mask is 255.255.255.0.)

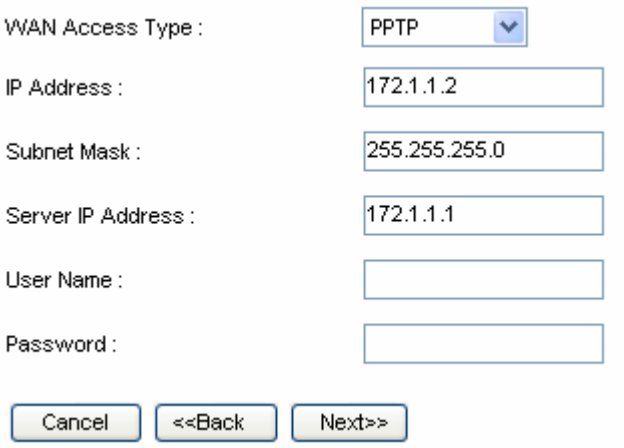
Step 4- WAN Interface Setup

WAN Access Type	**DHCP Client**  If the DHCP Client connection be selected, the PC will obtain the IP address automatically. **Static IP**  If the Static IP be selected, user have to set up the IP address, subnet mask and default gateway according to the ISP (Internet Service Provider) that provided the related information. **IP Address:** Enter the WAN IP address provided by your ISP here. **Subnet Mask:** Enter the subnet mask here. **Default Gateway:** Enter the default gateway IP address provided by your ISP here. **DNS:** Enter the DNS server IP address in the column. **PPPoE**



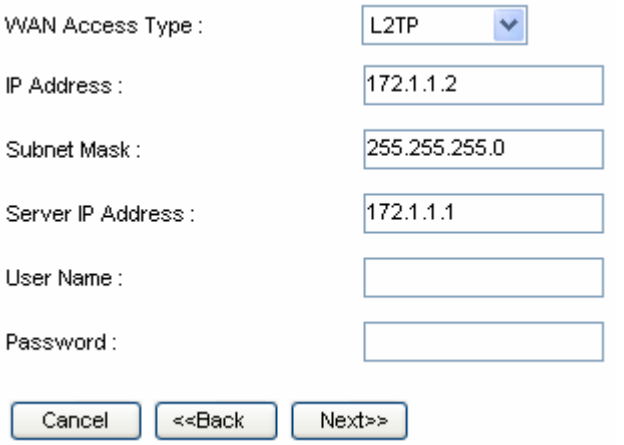
If the PPPoE be selected, user have to set up the user name and password according to the ISP that provided the related information.
User Name: Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).
Password: Enter the password that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).

PPTP



If the PPTP be selected, user have to set up the server IP address, user name and password according to the ISP that provided the related information.
IP Address: Enter the WAN IP address provided by your ISP here.
Subnet Mask: Enter the subnet mask here.
Server IP Address: Enter the PPTP Server IP Address in this column.
User Name: Maximum input is 20 alphanumeric characters (case sensitive).
Password: Maximum input is 32 alphanumeric characters (case sensitive).

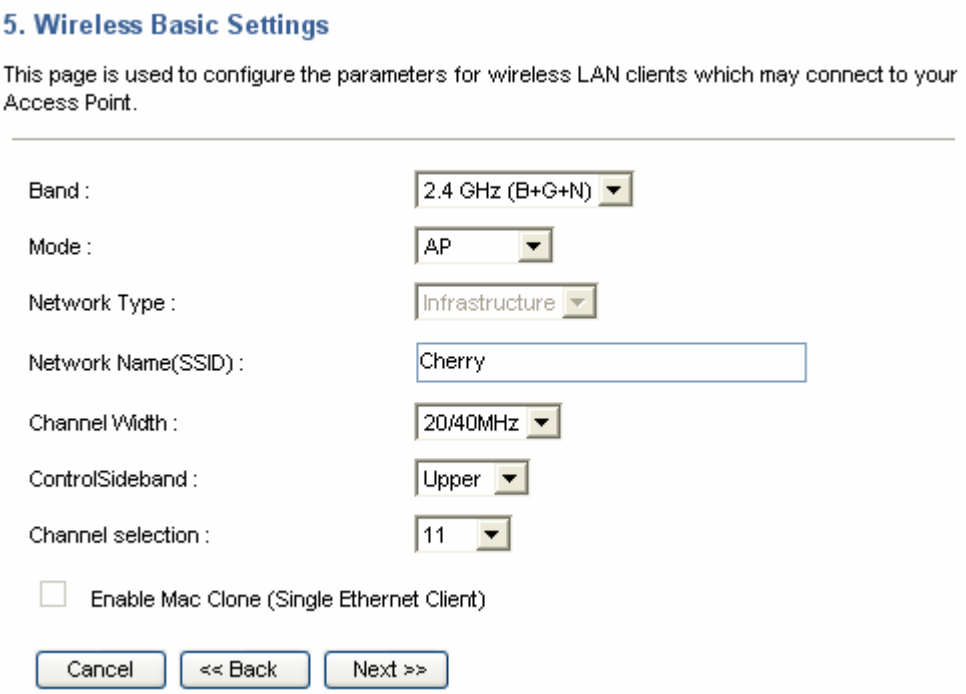
L2TP



If the L2TP be selected, user have to set up the server IP address, user name

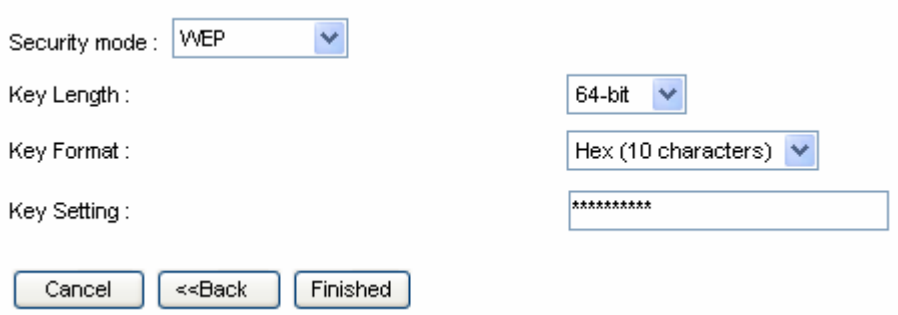
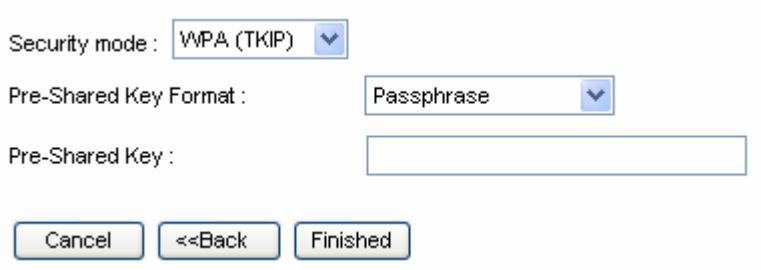
	and password according to the ISP that provided the related information. **IP Address:** Enter the WAN IP address provided by your ISP here. **Subnet Mask:** Enter the subnet mask here. **Server IP Address:** Enter the L2TP Server IP Address in this column. **User Name:** Maximum input is 20 alphanumeric characters (case sensitive). **Password:** Maximum input is 32 alphanumeric characters (case sensitive).

Step 5- Wireless Basic Settings



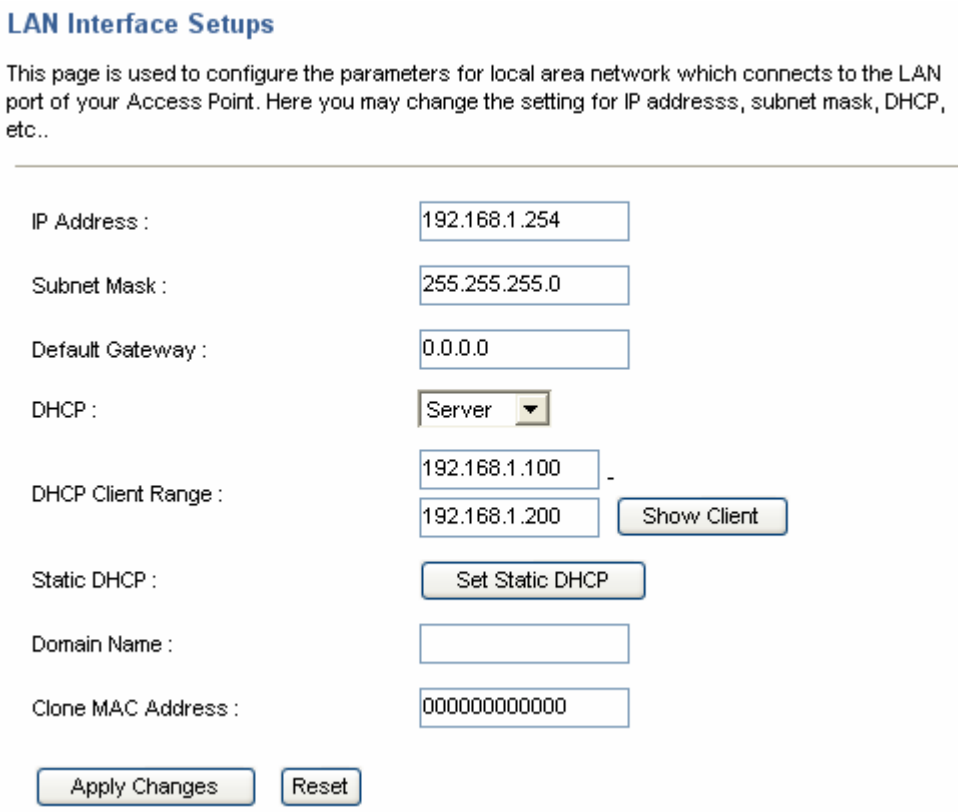
Band	Select 2.4 GHz (B+G+N), 2.4 GHz (B), 2.4 GHz (G), 2.4 GHz (N), 2.4 GHz (B+G), and 2.4 GHz (G+N).
Mode	Select 11b/g mixed, 11b only, 11g only, or 11b/g/n mixed mode from the pull-down menu. (Default is 11b/g/n mixed mode.)
Network Type	This type here is fixed and cannot be changed.
Network Name (SSID)	A SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Channel Width	Select 20/40MHz or 20MHz for the transmitting band width.
Control Sideband	Select Upper or Lower from pull-down menu.
Channel selection	Select **1~11** or **Auto Select** from the pull-down menu.

Step 6- Wireless Security Setup

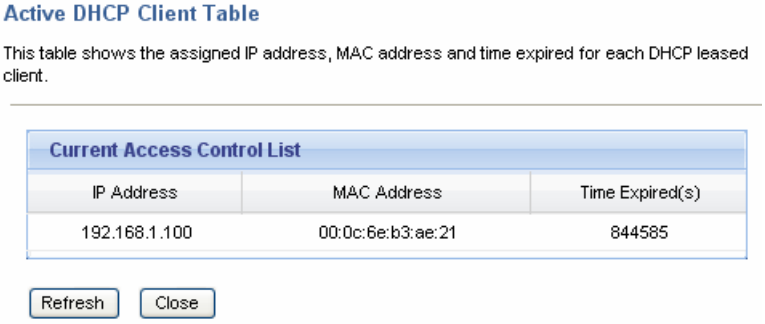
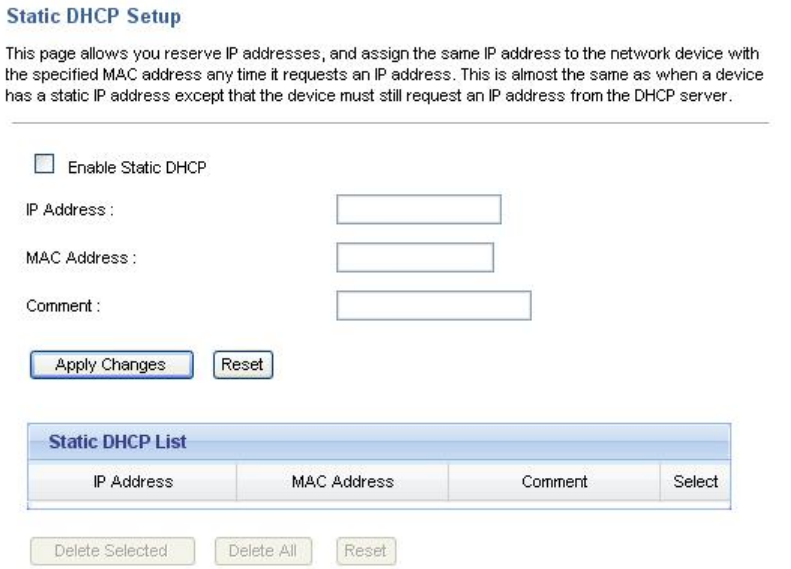
Security Mode	Select desired security type from the pull-down menu **None, WEP, WPA(TKIP), WPA2(AES)** and **WPA2 Mixed**. The default setting is **None**. It is strongly recommended to set up security mode (WEP, WPA(TKIP), WPA2(AES) and WPA2 Mixed) to prevent any unauthorized accessing. Both your PC and the Wireless Router must have the same settings for security. **WEP**  **Key Length:** select key length 64-bit or 128-bit. **Key Format**: Select the Hex(10 characters) or ASCII (5 characters). ● **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f). ● **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f). ● **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive). ● **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive). **Key Setting:** Enter the key in the key setting field. **WPA(TKIP)/WPA2(AES)/WPA2 Mixed**  **Pre-Shared Key Format**: There are two formats for choosing to set the pre-shared key, **Passphrase** and **Hex (64 characters)**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.

	Pre-Shared Key : Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

LAN



IP Address	Shows the IP address of the Wireless Router (Default IP address is 192.168.1.254.)
Subnet Mask	The subnet mask of the Wireless Router (Default subnet mask is 255.255.255.0.)
Default Gateway	Enter the Internet default gateway LAN IP address in this column. And, the default gateway should has a connection with the Internet.
DHCP	**Disable**: Select to disable this Wireless Router to distribute IP addresses to connected clients. **Server**: Select to enable this Wireless Router to distribute IP Addresses (DHCP Server) to connected clients. And the following field will be activated for you to enter the starting IP address.
DHCP Client Range	The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 192.168.1.33 should work for most cases. • Maximum: 254. Default value 254 should work for most cases. ***Note:*** If "Continuous IP address poll starts" is set at 192.168.1.33 and the "Number of IP address in pool" is 254, the device will distribute IP addresses from 192.168.1.33 to 192.168.1.254 to all the computers in the network that request IP addresses from DHCP server (Router)

Show Client	Click to show Active DHCP Client Table.  **Refresh**: Click this button to refresh the table. **Close**: Click this button to close the window.
Static DHCP	Check the box to enable the Static DHCP function, default setting is disabled. When set to enabled, user can click **Static DHCP** button to set the **Static DHCP** function.  **IP Address**: Enter the fixed IP address that DHCP Server assigned to a certain connected station. **MAC Address**: Enter the MAC address of a certain station, and then the DHCP Server will to distribute a fixed IP address to the station automatically once they connected. **Comment**: You can enter a comment to description above IP address or MAC address. **Apply Changes:** After completing the settings on this page, click Apply changes button to save the settings. **Reset:** Click Reset to restore to default values. **Static DHCP List**: Here shows the static IP address that have been assigned according to the MAC address. **Delete Selected**: Click Delete Selected to delete items which are selected. **Delete All**: Click **Delete All** button to delete all the items. **Reset**: Click **Reset** button to rest.
Domain Name	Enter the Domain Name here.
Clone MAC Address	This table displays you the station MAC information.

Password

User Name	Key in a new login user name in the blank field.
New Password	Maximum input is 36 alphanumeric characters (case sensitive.)
Confirmed Password	Key in the password again to confirm.

Status

Status

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

System Status	
System Up Time	0day:5h:26m:23s
Firmware Version	v2.3
Build Time	Fri Oct 9 17:30:51 CST 2009
Sys OP Mode	Router Mode
System Setting	
- Bandwidth Management	Disabled
- UPnP	Enabled

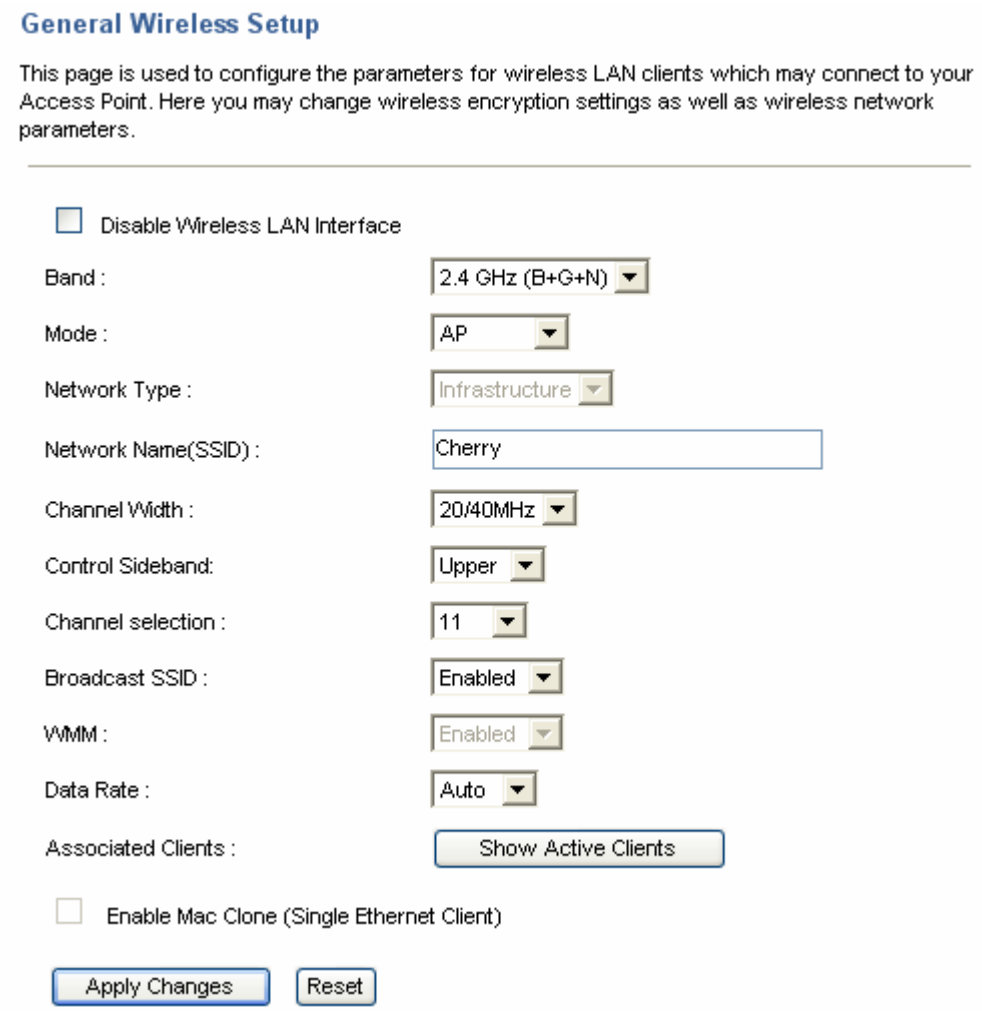
Wireless Configuration	
Op Mode	AP
802.11 Mode	2.4 GHz (B+G+N)
Network Name(SSID)	Cherry
Channel selection	11
Security mode	Disabled
BSSID	00:e0:4c:81:96:b1
Associated Clients	0
WPS Mode	Configured

LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:b1

WAN Configuration	
Attain IP Protocol	Fixed IP Connected
IP Address	10.0.2.225
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.252
MAC Address	00:e0:4c:81:96:b9
WAN Link Status	LinkUp

Wireless

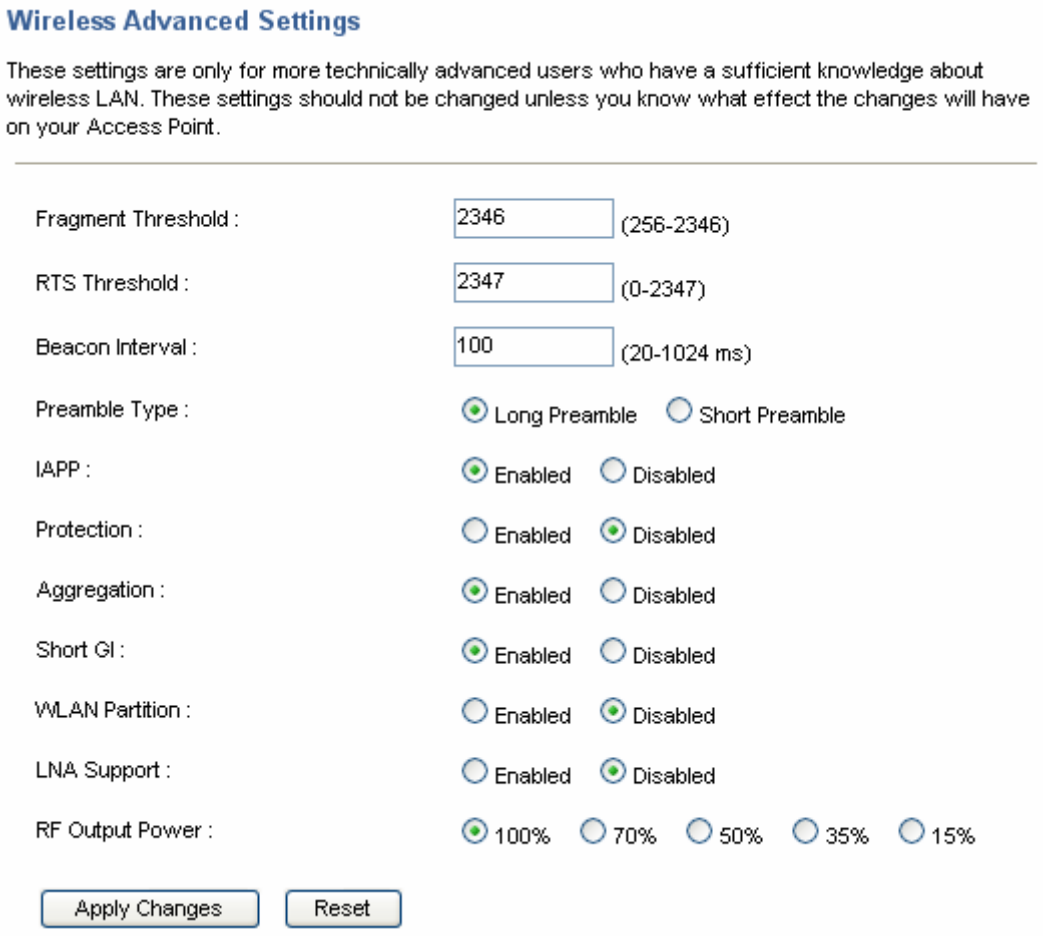
General Setup



Disable Wireless LAN Interface	Check to disable the wireless function.
Band	You can choose one mode of the following you need. ● 2.4GHz **(B):** 802.11b supported rate only. ● 2.4GHz **(G):** 802.11g supported rate only. ● 2.4GHz **(N):** 802.11n supported rate only. ● 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. ● 2.4GHz **(G+N):** 802.11g supported rate and 802.11n supported rate. ● 2.4GHz **(B+G+N):** 802.11b, 802.11g and 802.11n supported rate. The default is 2.4GHz **(B+G+N)** mode.
Mode	Select the AP, Client, WDS or AP+WDS modes from the pull-down menu.
Network Type	If the mode be set to Client mode that the network type can be set to Infrastructure or Ad hoc.
SSID	A SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Channel Width	Select 20MHz/40MHz channel width, the channel number will be form 5~11 and auto; Select 20MHz channel width the channel number will be

	form 1~11 and auto. Default is 20MHz/40MHz.
Control Sideband	You can select Lower or Upper form the pull-down list.
Channel Number	The channel number base on the channel width you select.
Broadcast SSID	**Enabled**: This wireless AP will broadcast its SSID to stations. **Disabled**: This wireless AP will not broadcast its SSID to stations. If stations want to connect to this wireless AP, this AP's SSID should be known in advance to make a connection.
WMM	The WiFi Multiple Media function is available under 2.4GHz (B), 2.4GHz (G) and 2.4GHz (B+G) band, and is **disabled** under 2.4GHz (N), 2.4GHz (G+N) and 2.4GHz (B+G+N) band.
Data Rate	There are several data rate that you can select from the pull-down menu.
Associated Clients	Click **Show Active Clients** button to show all the listed active clients.
Enable Mac Clone (Single Ethernet Client)	This function will be enabled under Client mode.

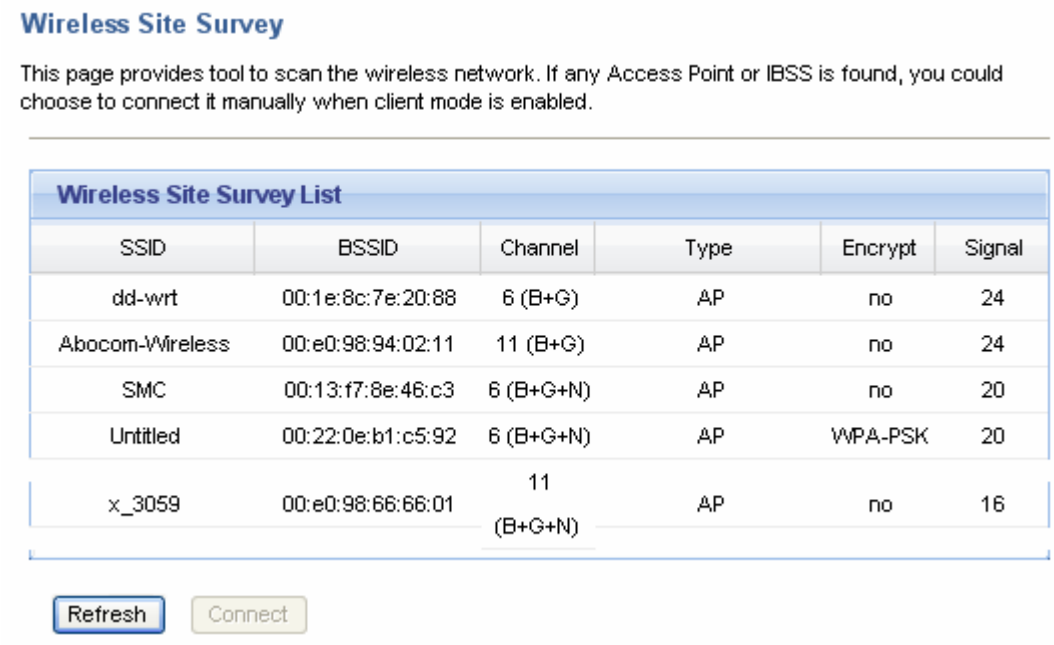
Advanced Settings



Fragment Threshold	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If the 802.11g MIMO Wireless Router often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from

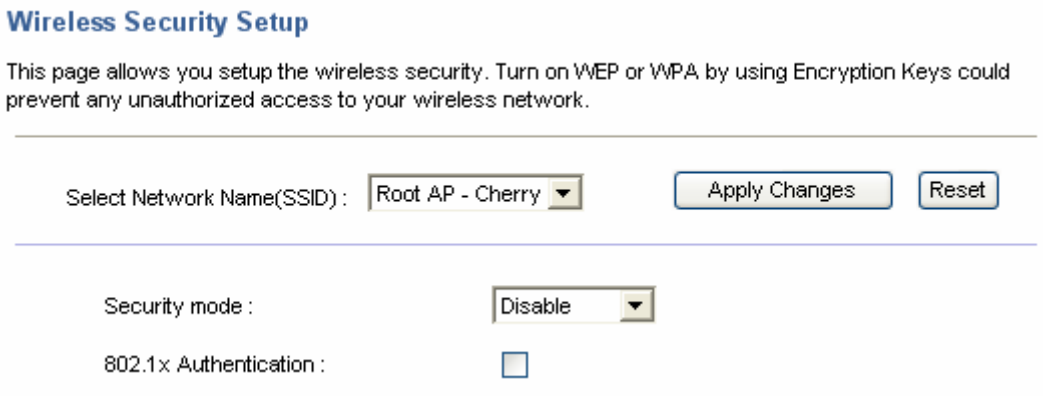
	256 to 2346. The default value is 2346.
RTS Threshold	RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. If the "Hidden Node" problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Beacon Interval	Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon. Range 20-1024 ms, default is 100.
Preamble Type	A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. You can select Long or Short for the preamble type.
IAPP	Select Enabled or Disabled to execute this function.
Protection	Select Enabled or Disabled to execute the security function.
Aggregation	Select Enabled or Disabled to execute this function.
Short GI	Select Enabled or Disabled to execute this function.
WLAN Partition	Select Enabled or Disabled to execute this function.
LNA support	Select Enabled or Disabled to execute this function.
RF Output Power	Select the transmitting power rate 100%, 70%, 50%, 35%, 15%.

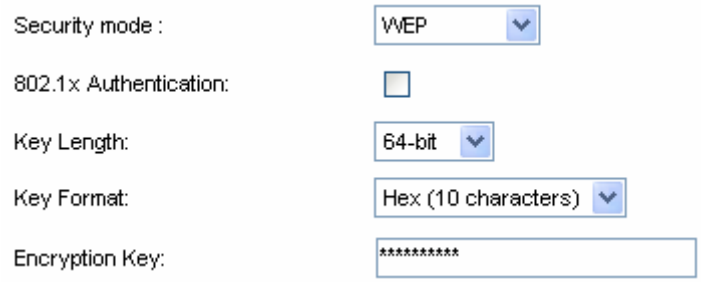
Site Survey

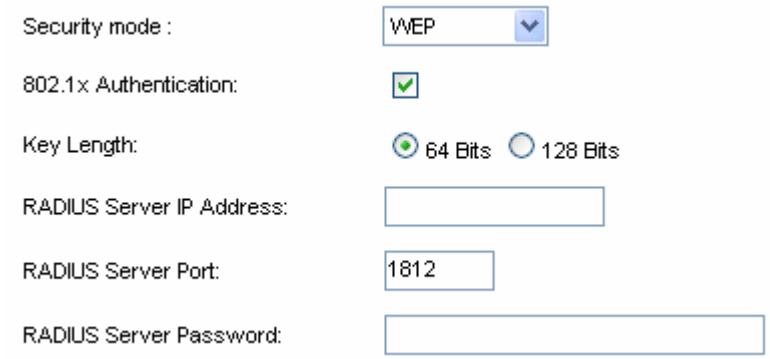


Refresh	Check this button to refresh all the Site Survey statistics.
Connect	Under the Client mode and select a site that you would like to communicate, and then click the Connect button.

Security

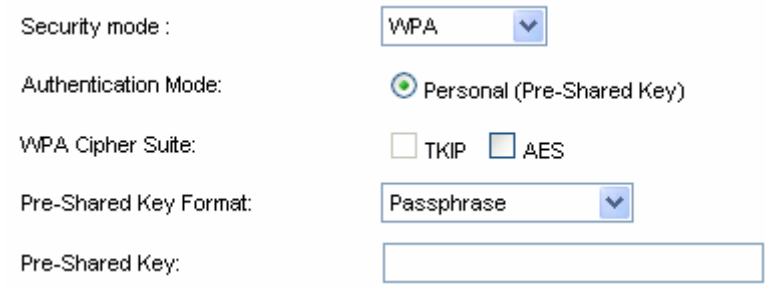


Security Mode	Select desired security type from the pull-down menu **Disable, WEP, WPA, WPA2** and **WPA-Mixed**. The default setting is **Disable**. It is strongly recommended to set up security mode (WEP, WPA, WPA2 and WPA-Mixed) to prevent any unauthorized accessing. **WEP**  **Key Length:** select key length 64-bit or 128-bit. **Key Format**: Select the default key Key1~4. • **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f). • **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f). • **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive). • **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive). **Encryption Key:** Enter the key in the key setting field. **802.1x Authentication**



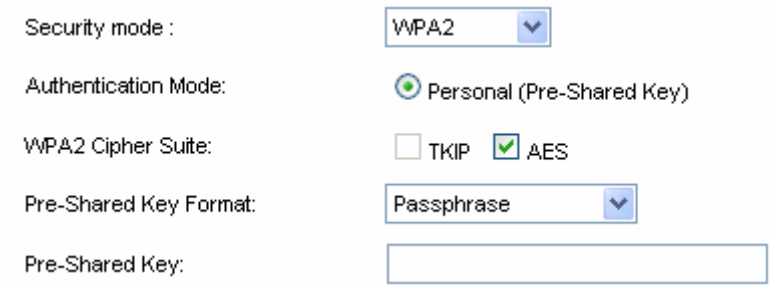
Key Length: select key length 64-bit or 128-bit.
RADIUS Server IP Address: Enter the RADIUS Server's IP Address provided by your ISP.
RADIUS Server Port: Enter the RADIUS Server's port number provided by your ISP. The default is **1812**.
RADIUS Server Password: Enter the password that the AP shares with the RADIUS Server.

WPA



Authentication Mode: Personal (Pre-Shared Key).
WPA Cipher Suite: here supported AES only.
Pre-Shared Key Format: There are two formats for choice to set the Pre-shared key, **Passphrase** and **Hex (64 characters)**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Pre-Shared Key : Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

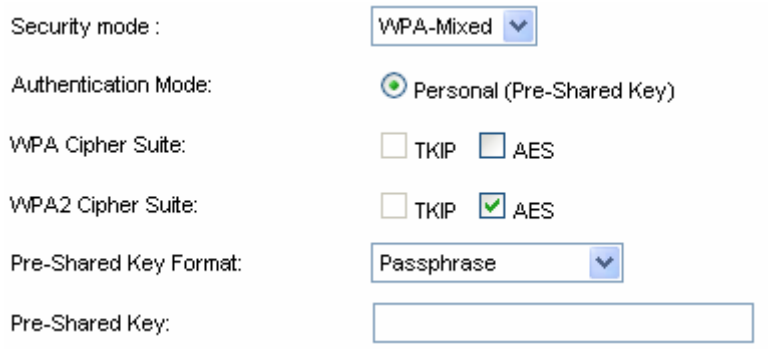
WPA2



Authentication Mode: Personal (Pre-Shared Key).

WPA2 Cipher Suite: here supported AES only.
Pre-Shared Key Format: There are two formats for choice to set the Pre-shared key, **Passphrase** and **Hex (64 characters)**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Pre-Shared Key : Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

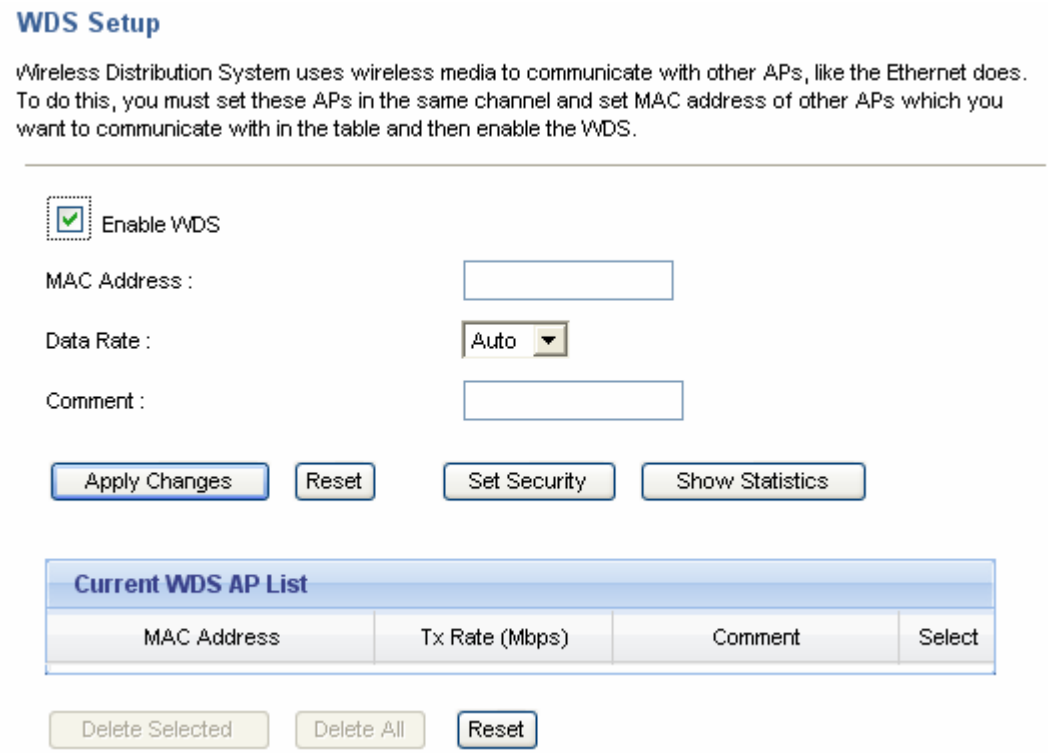
WPA-Mixed



Authentication Mode: Personal (Pre-Shared Key).
WPA Cipher Suite: here supported AES only.
WPA2 Cipher Suite: here supported AES only.
Pre-Shared Key Format: There are two formats for choice to set the Pre-shared key, **Passphrase** and **Hex (64 characters)**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Pre-Shared Key : Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.

WDS Setup

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS. If you would like to setup this WDS function, please go to **Wireless > General Setup**, and then select the **Mode** into **WDS** mode. Then go to the WDS Setup page to enable the WDS.

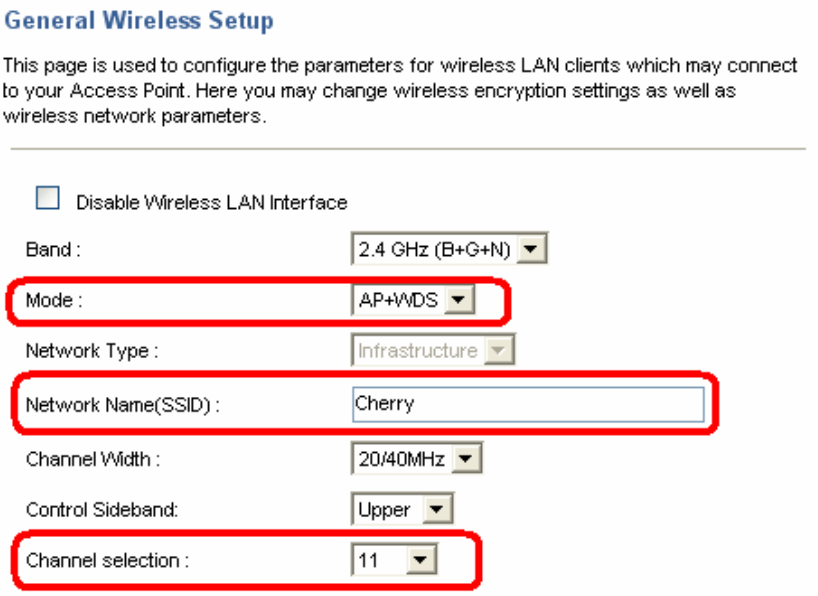


To use WDS function:

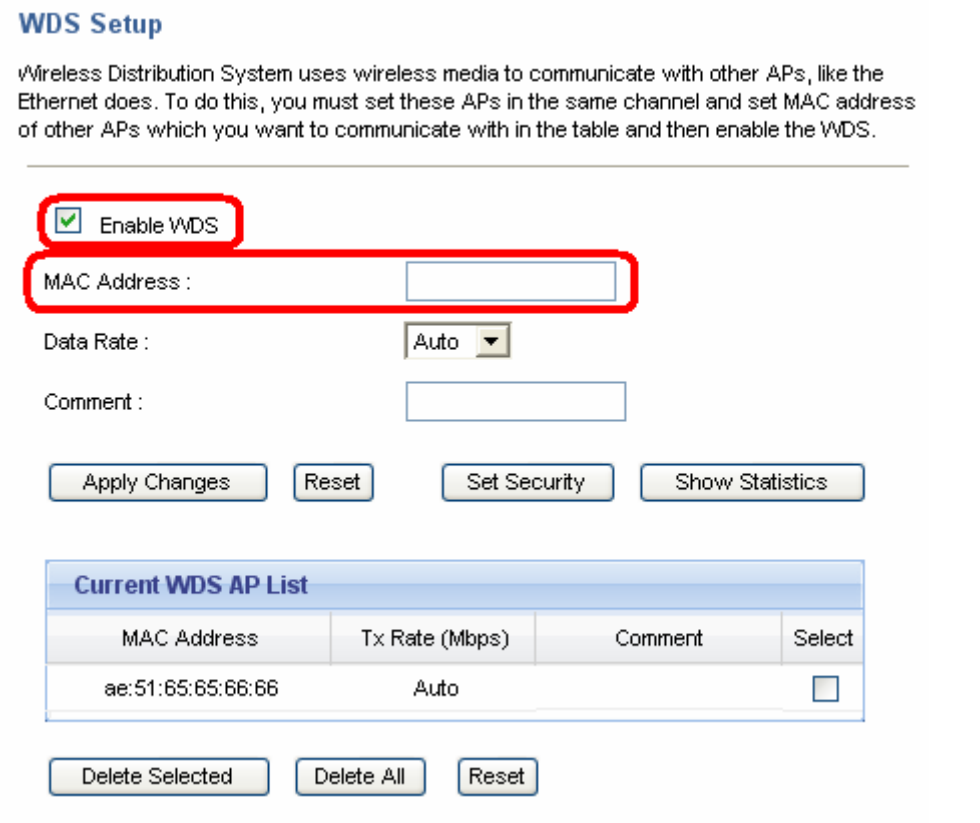
1. The APs must support WDS function.
2. (To set WDS must use the same wireless products (the same model will be better); due to different wireless products might support different WDS settings. Thus, it is suggested that to use the same wireless products that support WDS function.)
3. To set the same SSID and channel on the APs.
4. To set the same Wireless MAC address(BSSID) on the APs.
5. To set same security (WEP or WPA) on the APs.

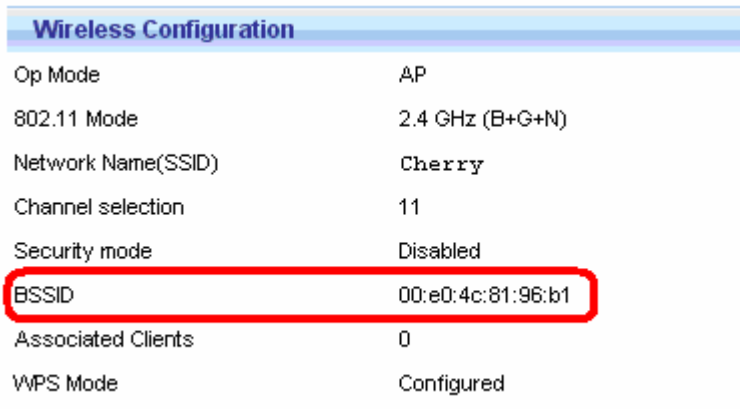
If the users would like to set up the WDS function, please go to **Wireless> General Setup** page to set up the mode into **WDS** or **AP+ WDS** (Repeater) mode. The APs that should use the same **SSID** and **Channel**, then go back to **Wireless > WDS Setup** page to enter **Wireless MAC(BSSID)** of each other to make the WDS connection.

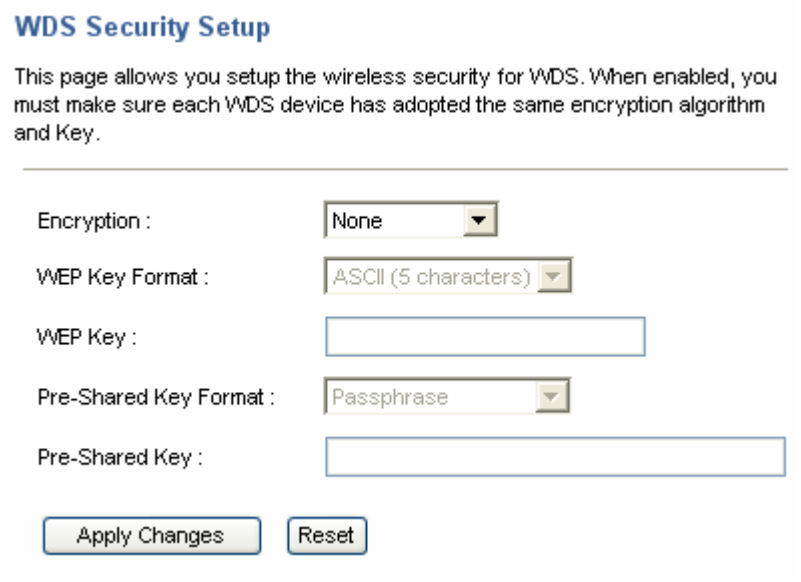
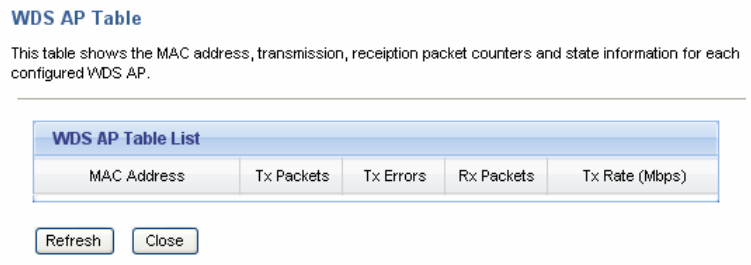
Step 1: Setup the same **SSID** and **Channel** on wireless APs.



Step 2: Enter **Wireless MAC (BSSID) address** to each other. (According to the WDS mode that user selected, for example, Lazy mode is unnecessary to enter another AP's MAC address.)



Enable WDS	Check the box to enable the WDS function.
MAC Address	**MAC Address**: Enter the Wireless BSSID (MAC) of the wireless AP that you want to connect with. To check your wireless router's MAC address, please go to **Status** > **Wireless Configuration** to find your **BSSID** (Wireless MAC address). 
Data Rate	Select the data rate form the pull-down list.
Comment	Enter a description for the device.
Apply Changes	After completing the settings on this page, click **Apply changes** button to save the settings.
Reset	Click **Reset** to restore to default values.

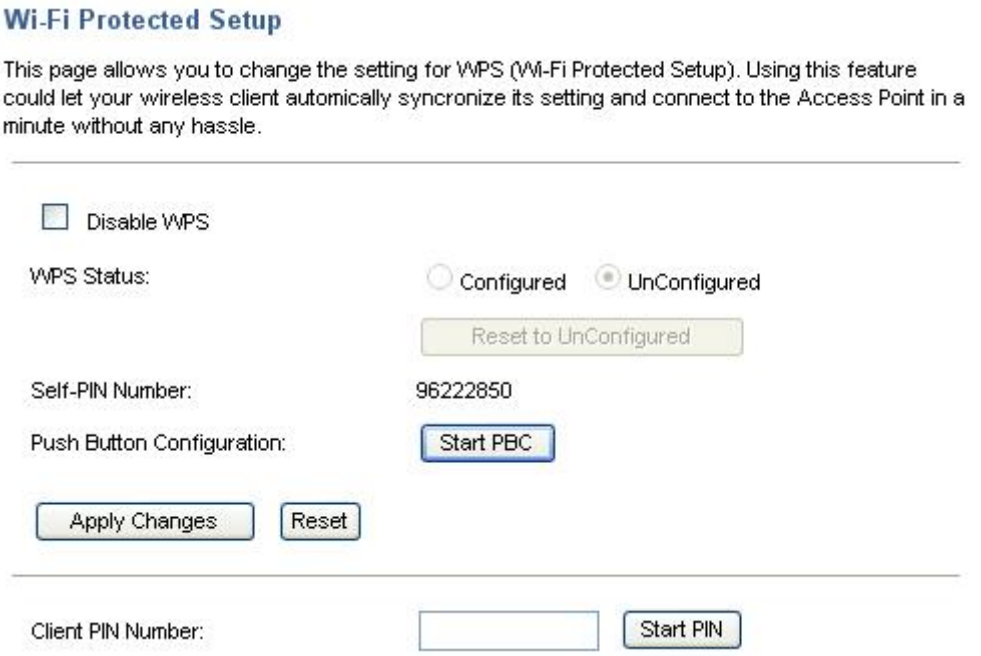
Set Security	Enable the WDS function and then click **Set Security** button to set up the WDS security.  **WDS Security Setup** **Encryption:** Select the encryption type **None, WEP 64 bits, WEP 128 bits, WPA (TKIP)** and **WPA2 (AES)** from the pull-down menu. **WEP Key Format:** For **WEP 64 bits** and **WEP 128 bits** encryption type, the selection of **WEP Key Format** are **Hex** and **ASCII**. **WEP Key**: If select Hex if you are using hexadecimal numbers (0-9, or A-F). Select ASCII if you are using ASCII characters (case-sensitive). ● **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f). ● **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f). ● **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive). ● **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive). **Pre-Shared Key Format**: The **Pre-shared Key Format** will be enabled when **WPA (TKIP)** and **WPA2 (AES)** encryption be selected. There are two formats for choice to set the Pre-shared key, **Passphrase** and **Hex (64 characters)**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended. **Pre-Shared Key:** Pre-Shared-Key serves as a password. Users may key in 8 to 63 characters string to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.
Show Statistics	Click to show the current WDS AP table. This table shows the MAC address, transmission packets and errors, reception packets and Tx Rate (Mbps) counters for each configured WDS AP.  **Refresh**: Click to renew the counters information. **Close**: Click to leave the screen.
Current WDS AP List	Here shows the current WDS AP information.

Delete Selected	Click **Delete Selected** to delete the selected AP information.
Delete All	Click **Delete All** to delete all the items.
Reset	Click **Reset** to restore the settings.

Access Control

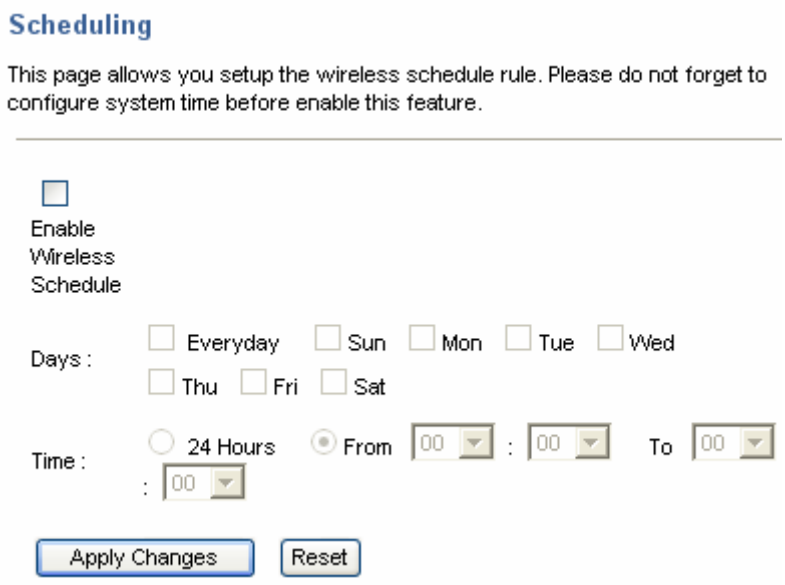
Wireless Access Control Mode	Select **Allow Listed** or **Deny Listed** form the pull-down menu to enable access control function. Default setting is **Disable**.
MAC Address	Enter the MAC address of a station that is allowed to access this Access Point.
Comment	You may enter up to 20 characters as a remark to the previous MAC address.
Current Access Control List	This table displays you the station MAC information.
Delete Selected	Click **Delete Selected** to delete items which are selected.
Delete All	Click **Delete All** to delete all the items.
Reset	Click **Reset** to rest.

WPS



Disable WPS	Check the box to Disable the WPS function, default setting is Enabled.
WPS Status	Here shows the current status of the WPS function.
Self-PIN Number	Here shows the PIN code of the router itself.
Push Button Configuration	Click **Start PBC** button to make a WPS connection with client.
Client PIN Number	Enter the client PIN code into the blank field then click the **Start PIN** button to make a WPS connection with client.

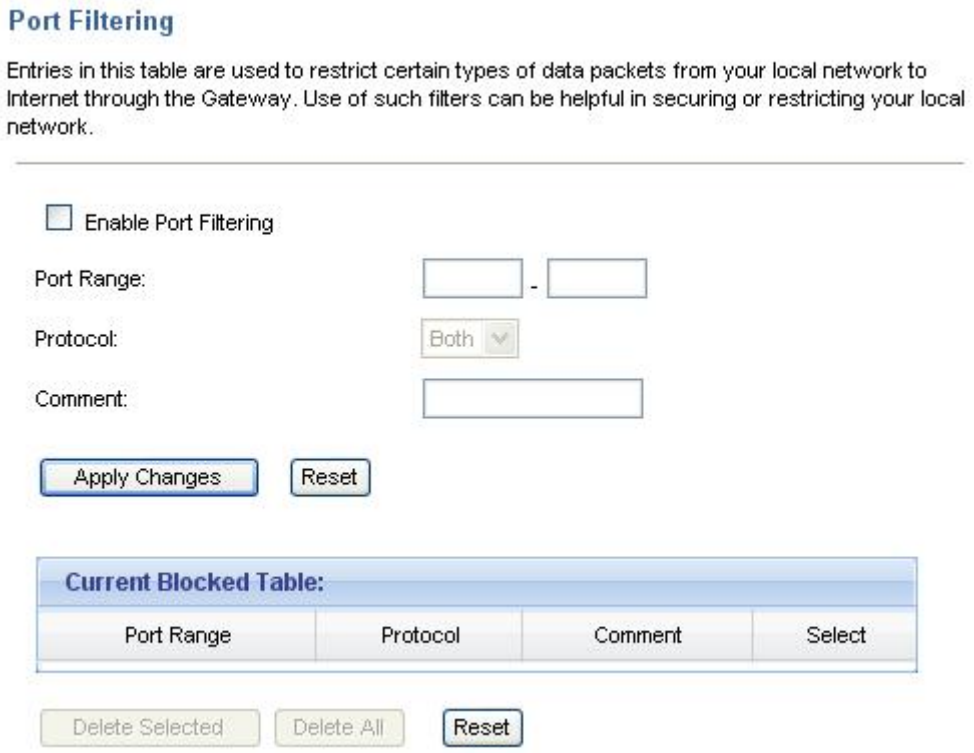
Scheduling



Enable Wireless Schedule	Check the box to enable the schedule function. Set up the time to schedule the wireless access rule.

Advanced

Access Control

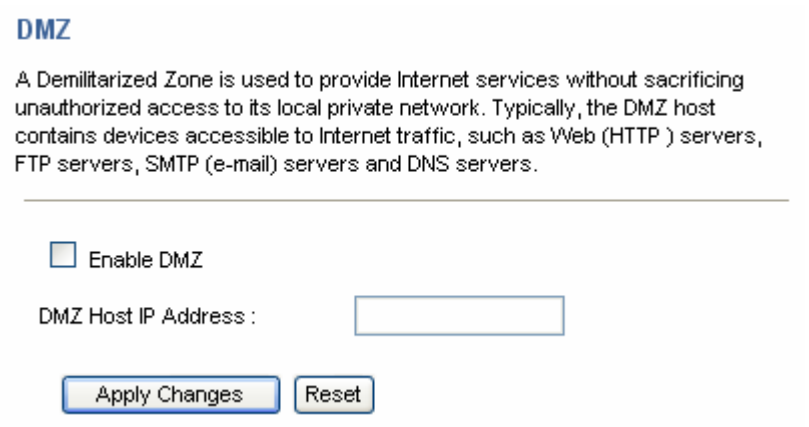


Enable Port Filtering	Check to enable this port filtering function.
Port Range	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Comment	You may key in a description for the port range.
Current Filter Table	Shows the current port filter information.
Delete Selected	Click **Delete Selected** button to delete items which are selected.
Delete All	Click **Delete All** button to delete all the items.
Reset	Click **Reset** button to rest.

Dynamic DNS

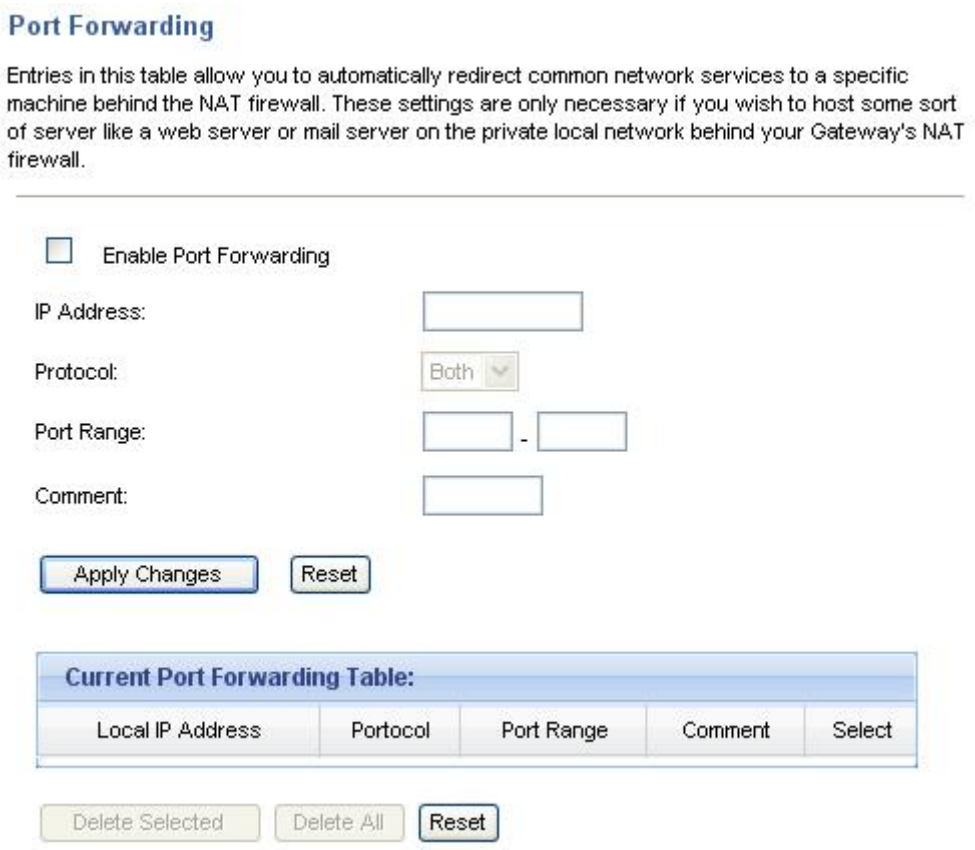
Enable DDNS	Check to enable the DDNS function.
Service Provider	Select the desired DDNS Service Provider DynDNS, TZO or Oray from the pull-down list.
Domain Name	Here shows the domain name of the service provider.
User Name/Email	Enter your email that you registered in service provider website. (You can refer to below Note information to apply a account form the service provider website.)
Password/Key	Enter your passwords that you registered in service provider website. Maximum input is 30 alphanumeric characters (case sensitive).
Apply Change	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.

DMZ



Enable DMZ	Check the box to enable DMZ function. If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two-way connections.
DMZ Host IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above. **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.
Apply Changes	After completing the settings on this page, click **Apply Changes** button to save the settings.
Reset	Click **Reset** button to restore to default values.

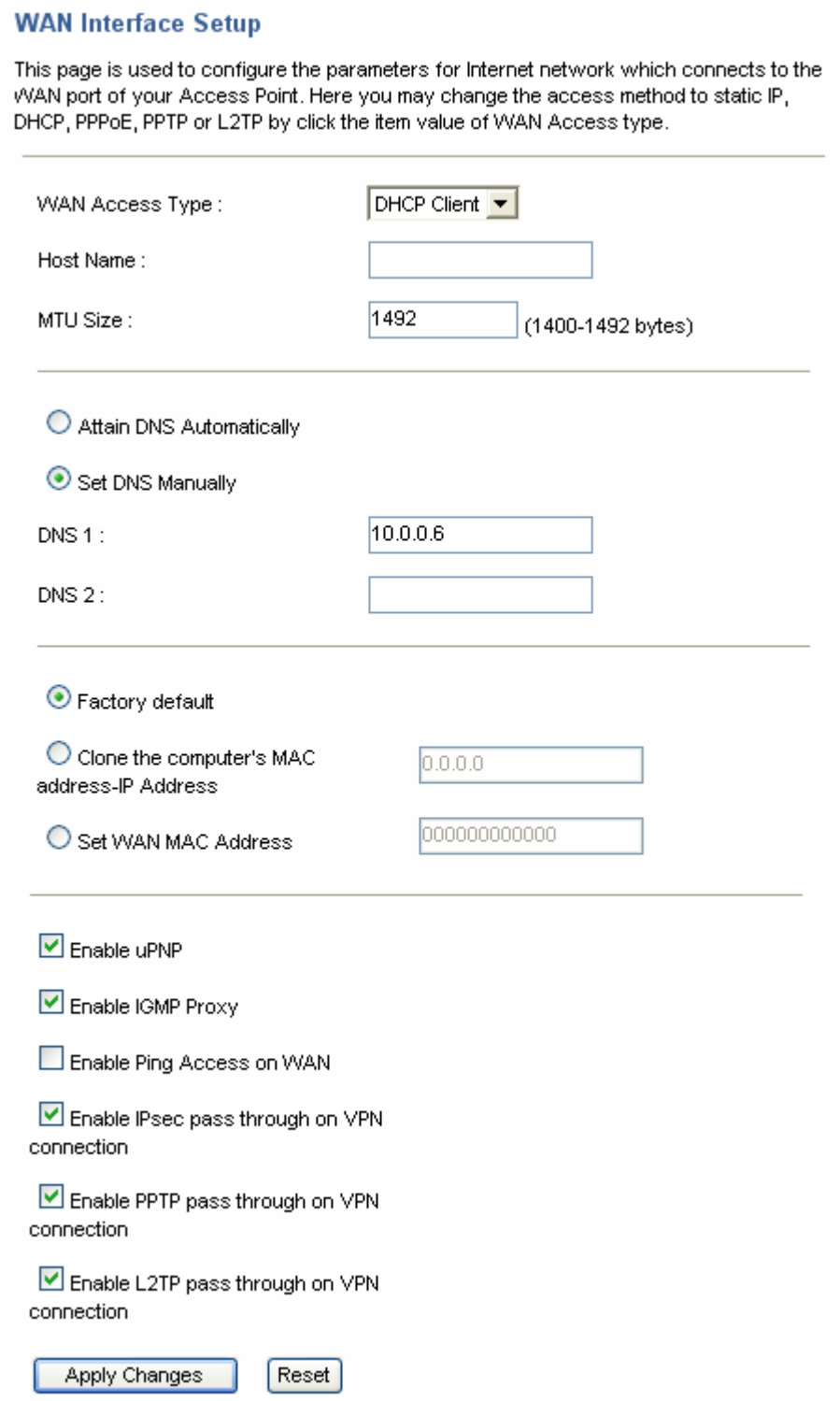
Virtual Servers



Enable Port Forwarding	Check to enable Port Forwarding function.
IP Address	Enter the IP address in the field.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Port Range	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

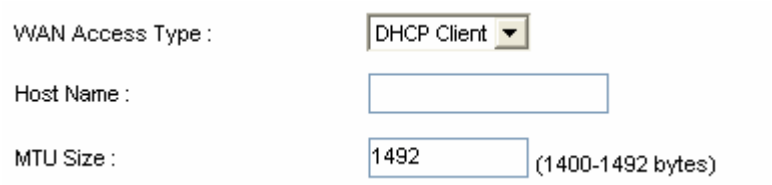
Comment	You may key in a description MAC address.
Apply Changes	After completing the settings on this page, click **Apply Changes** button to save the settings.
Reset	Click **Reset** button to restore to default values.
Current Port Forwarding Table	Shows the current Port Forwarding information.
Delete Selected	Click **Delete Selected** button to delete items which are selected.
Delete All	Click **Delete All** button to delete all the items.
Reset	Click **Reset** button to rest.

WAN Port


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type :
DHCP Client
Host Name :
MTU Size :
1492
(1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1 :
10.0.0.6
DNS 2 :
Factory default
Clone the computer's MAC address-IP Address
0.0.0.0
Set WAN MAC Address
000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping 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

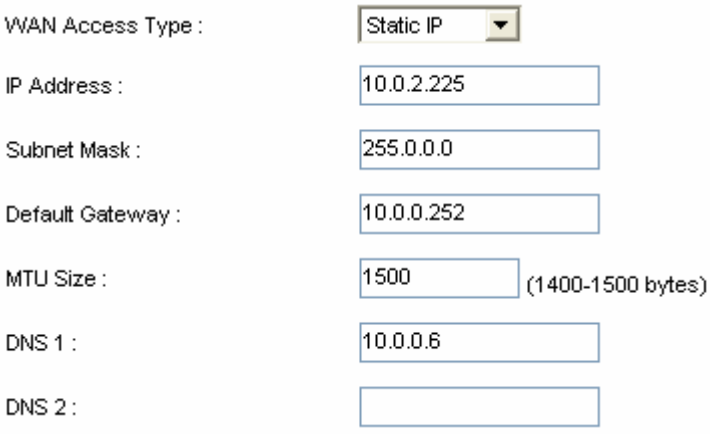
WAN Access Type

DHCP Client



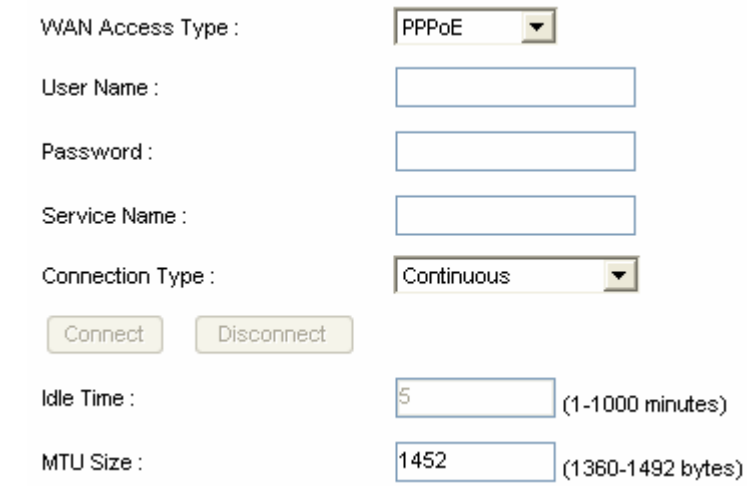
If the DHCP Client connection be selected, the PC will obtain the IP address automatically.
Host Name: Enter the host name here.
MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size, the default value is 1492 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.

Static IP



If the Static IP be selected, user have to set up the IP address, subnet mask and default gateway according to the ISP (Internet Service Provider) that provided the related information.
IP Address: Enter the WAN IP address provided by your ISP here.
Subnet Mask: Enter the subnet mask here.
Default Gateway: Enter the default gateway IP address provided by your ISP here.
MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size, the default value is 1492 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.
DNS 1: Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es).
DNS 2: This servers are optional. You can enter another DNS server's IP address as a backup. DNS 2 servers will be used when the DNS 1 server fails.

PPPoE



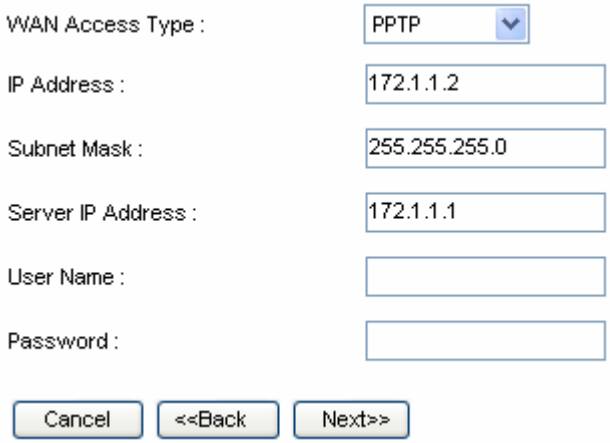
If the PPPoE be selected, user have to set up the user name and password according to the ISP that provided the related information.
User Name: Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).
Password: Enter the password that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).
Service Name: Enter the Internet service provider name in the column.

Connection Type: Select the connection type **Continuous**, **Connect on Demand** or **Manual** from the pull-down menu. If selected **Manual** user can click **Connect** button to make a connection.

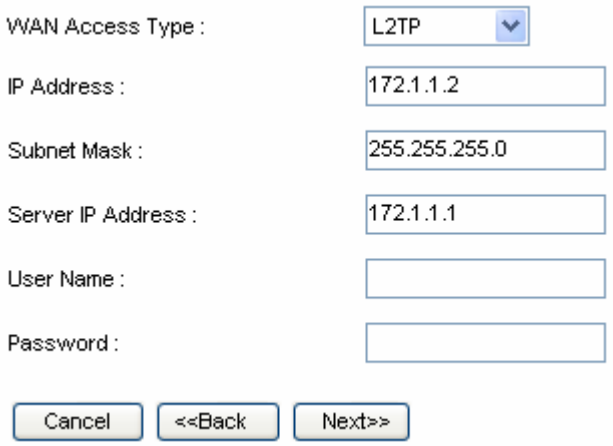
Idle Time: It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the **Connection Type** is selected to **Connect on Demand**.

MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size, the default value is 1492 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.

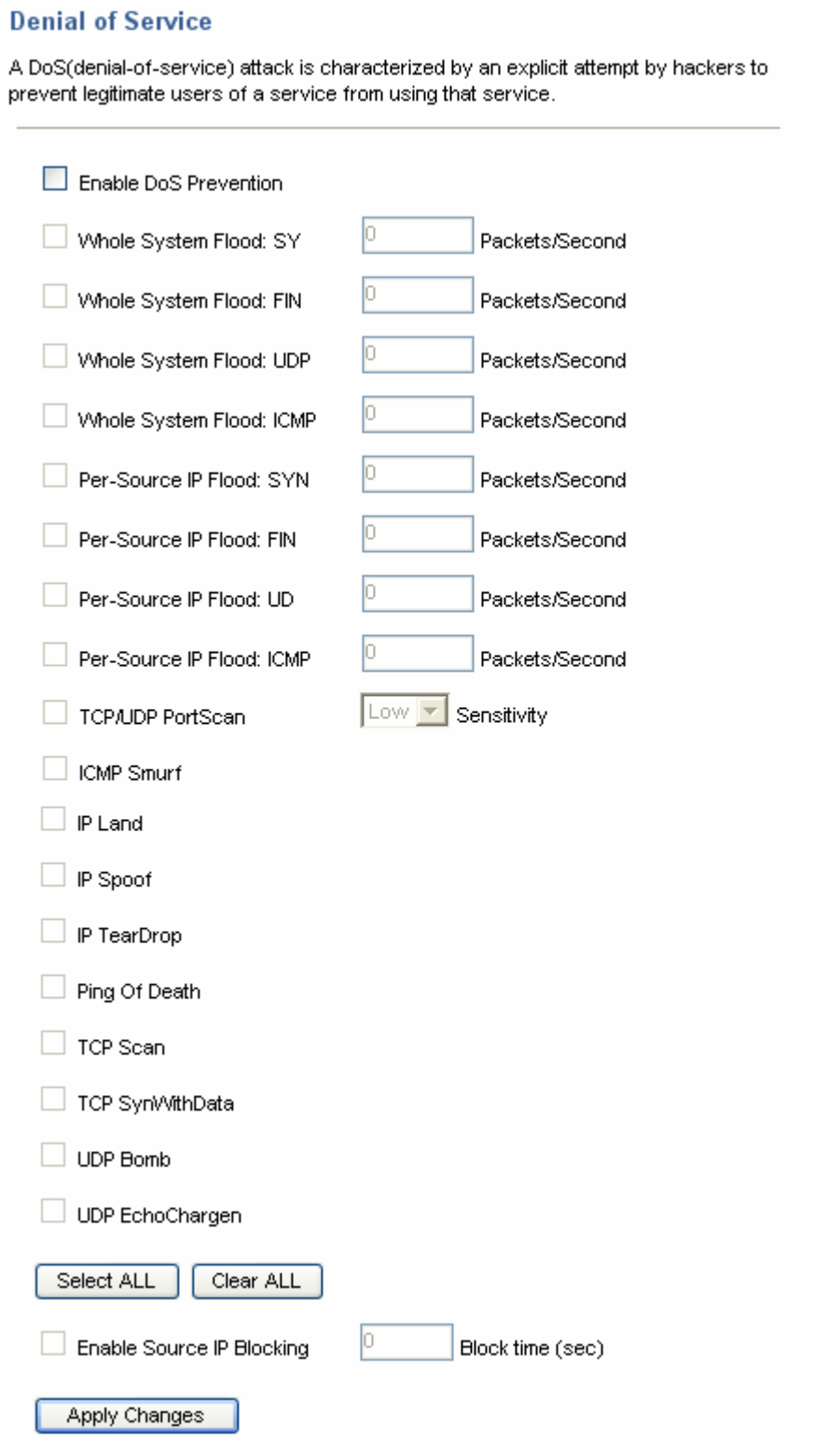
PPTP



If the PPTP be selected, user have to set up the server IP address, user name and password according to the ISP that provided the related information.

	IP Address: Enter the WAN IP address provided by your ISP here. **Subnet Mask:** Enter the subnet mask here. **Server IP Address:** Enter the PPTP Server IP Address in this column. **User Name:** Maximum input is 20 alphanumeric characters (case sensitive). **Password:** Maximum input is 32 alphanumeric characters (case sensitive). **L2TP**  If the L2TP be selected, user have to set up the server IP address, user name and password according to the ISP that provided the related information. **IP Address:** Enter the WAN IP address provided by your ISP here. **Subnet Mask:** Enter the subnet mask here. **Server IP Address:** Enter the L2TP Server IP Address in this column. **User Name:** Maximum input is 20 alphanumeric characters (case sensitive). **Password:** Maximum input is 32 alphanumeric characters (case sensitive).
Attain DNS Automatically **Set DNS Manually**	Select to **Attain DNS Automatically** or select **Set DNS Manually** to set the DNS server IP address at the following DNS 1~3 columns. Default setting is **Attain DNS Automatically**.
DNS 1 **DNS 2**	Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es). DNS 2 server is optional. You can enter another DNS server's IP address as a backup. DNS 2 server will be used when the DNS 1 server fails.
Factory Default **Clone the computer's MAC address-IP Address** **Set WAN MAC Address**	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
Enable uPNP…	Check to enable the listed functions.
Apply Changes	After completing the settings on this page, click **Apply changes** button to save the settings.
Reset	Click **Reset** to restore to default values.

DoS Setting

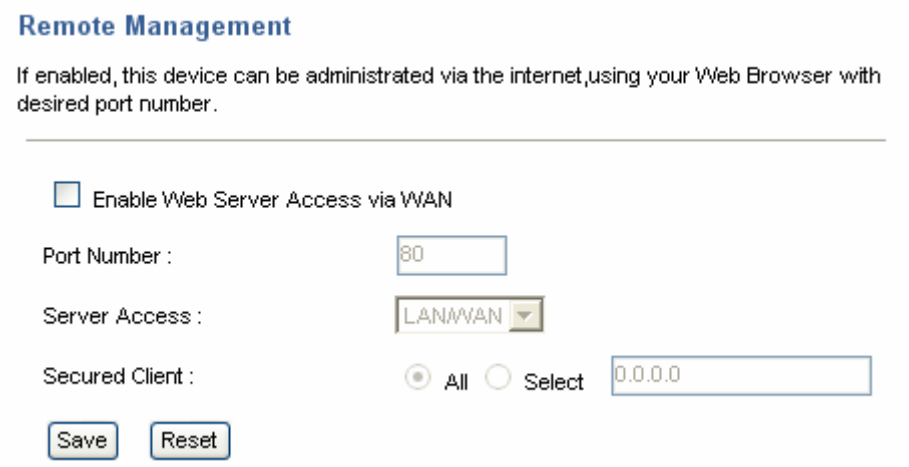


Enable DoS Prevention	DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks. This screen allows you to configure DoS protection. Check the box to enable the DoS settings.

Select All	After you enabled the DoS prevention, you can click to select all DoS preventions.
Clear All	After you enabled the DoS prevention, you can click to uncheck all DoS preventions.
Apply Changes	After completing the settings on this page, click **Apply Change** button to save current settings.

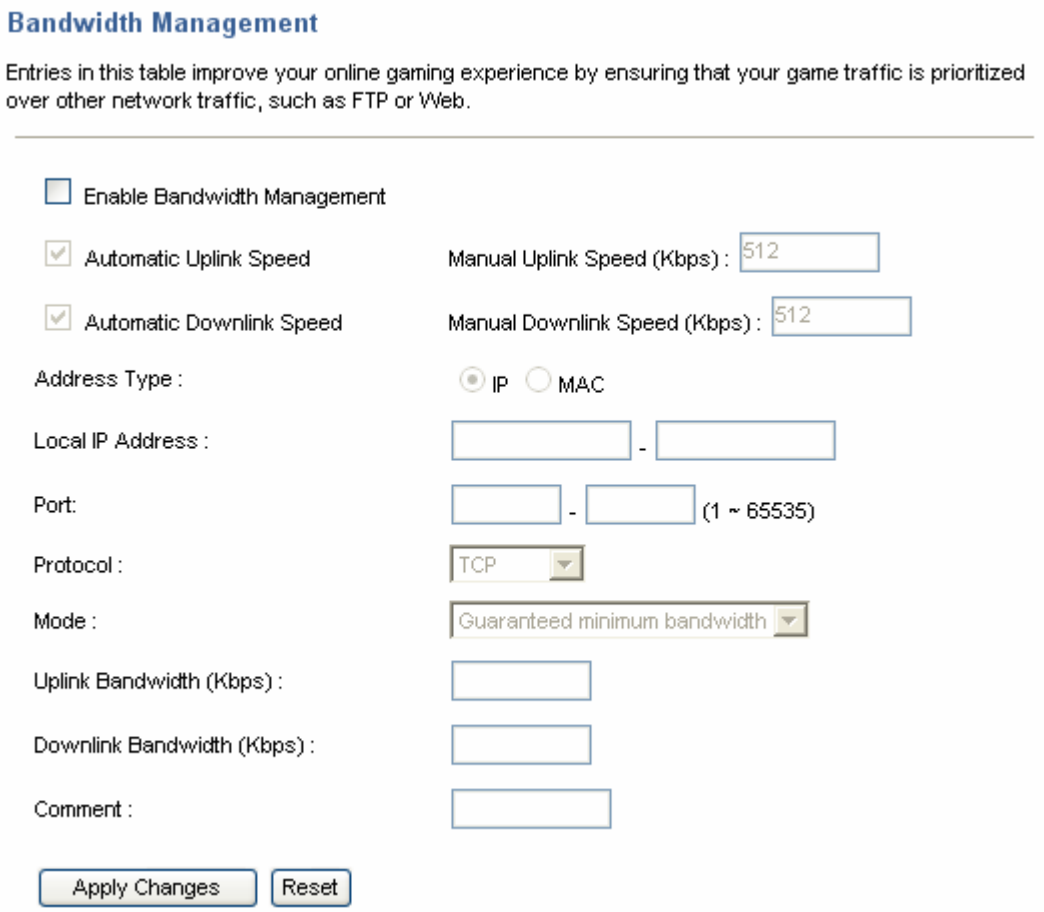
Administrator

Remote Management



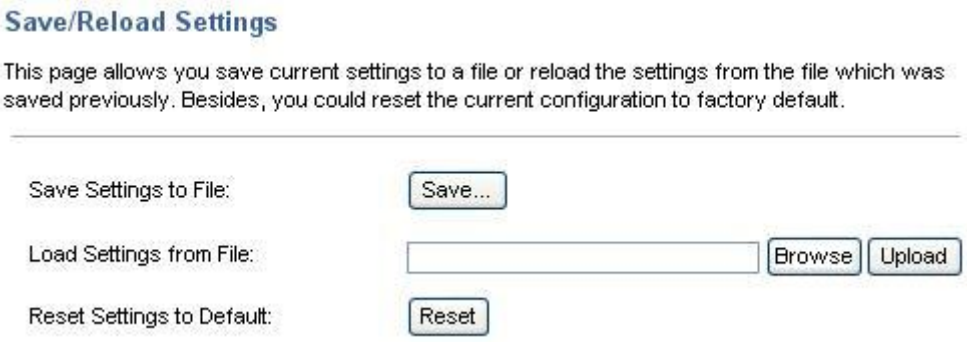
Enable Web Server Access via WAN	Check to enable remote control function.
Port Number	Enter the port number in the field.
Server Access	Select LAN/WAN, LAN or WAN from the pull-down menu.
Secured Client	Select All to allow remote control clients to access the wireless router or enter certain client's IP address to allow the remote management.

Bandwidth Mgmt



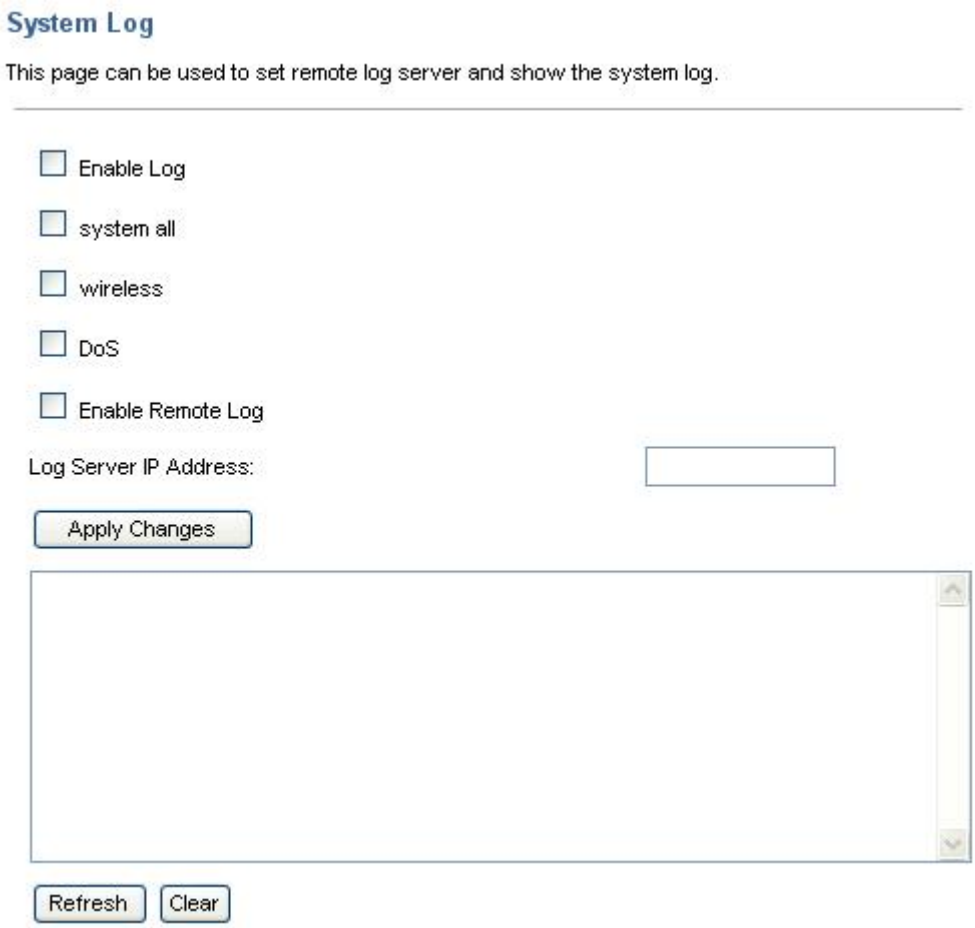
Enable Bandwidth Management	Check the box to enable this function. If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two-way connections. You can select automatic or manual uplink speed.
Automatic Uplink Speed	Check the box to enable the automatic uplink speed function.
Manual Uplink Speed	You can manually enter the transmission rate in the blank field.
Address Type	Select IP or MAC address type.
Local IP address **MAC address**	Depend on the address type that selected, user can enter the IP address or MAC address of client to set up the bandwidth of the transmission.
Port	Enter the beginning of port range numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Protocol	Select the protocol (TCP, UDP, TCP/UDP, ICMP or ANY) used to the remote system or service.
Mode	Select Guaranteed minimum bandwidth or Restricted maximum bandwidth modes.
Uplink Bandwidth (Kbps)	Enter the Uplink Bandwidth (Kbps) in the column.
Downlink Bandwidth (Kbps)	Enter the Downlink Bandwidth (Kbps) in the column.
Comment	Enter the note for the setting.

Config File



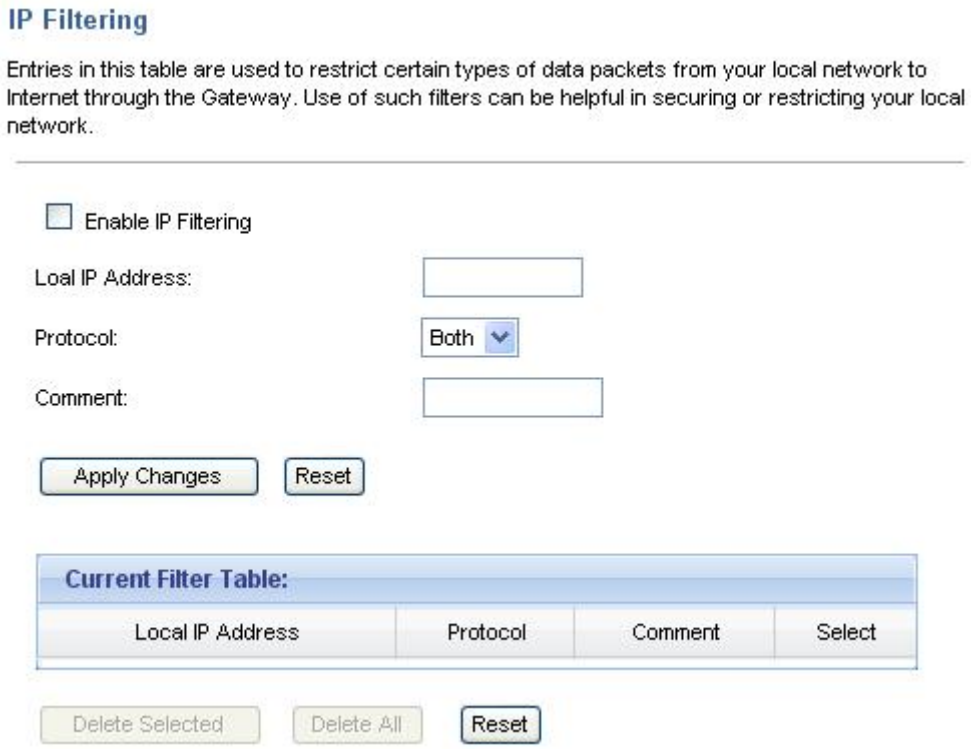
Save Settings to File	Click the **Save** button to save the current settings file in the PC.
Load Settings form File	Click the **Browse** button to find and open the previous saved file (the browser will display to correct file path.) Then, click **Upload** button to upload the previous file.
Reset Settings to Default	Click **Reset** button to set the device back to default settings.

Logs



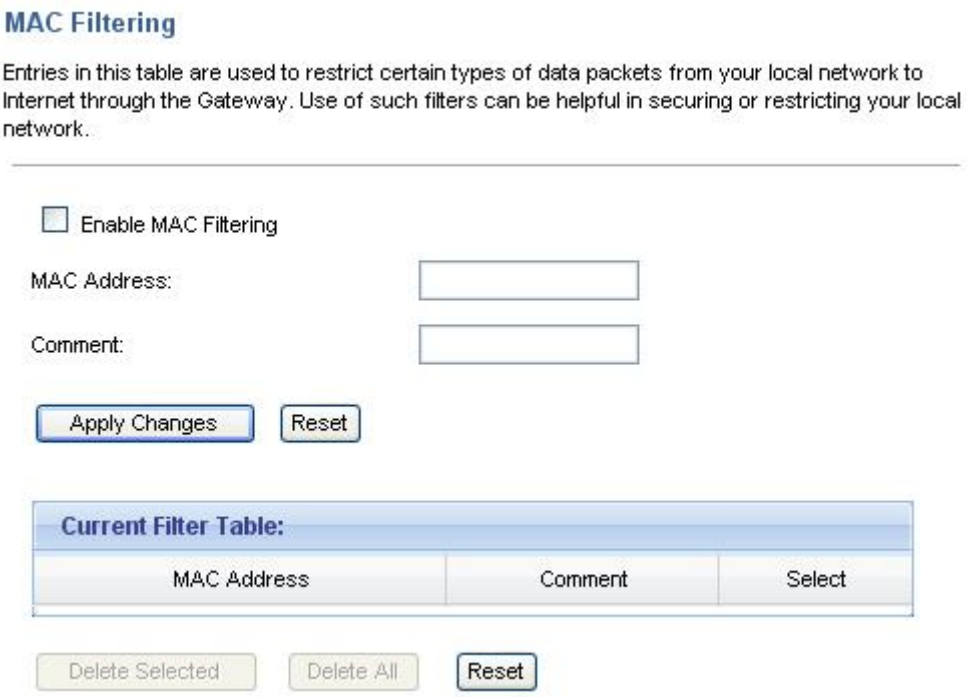
Enable Log	Check to enable logging function.
System all	Activates all logging functions.
Wireless	Only logs related to the wireless LAN will be recorded.
DoS	Only logs related to the DoS protection will be recorded.
Enable Remote Log	Only logs related to the Remote control will be recorded.
Log Server IP address	Only logs related to the server will be recorded.
Apply Changes	After completing the settings on this page, click **Apply Changes** button to save current settings.
Refresh	Click **Refresh** button to renew the logs.
Clear	Click **Clear** button to delete the logs.

IP Filtering



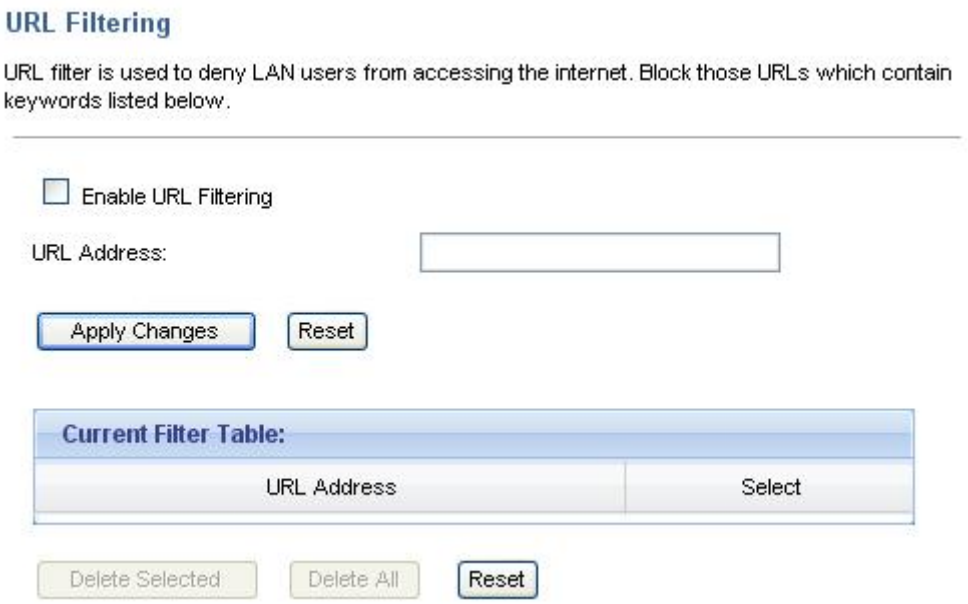
Enable IP Filtering	Check to enable IP filtering function.
Local IP Address	Enter the local server's IP address.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Comment	You may key in a description for the port range.
Apply Changes	After completing the settings on this page, click **Apply Changes** button to save the settings.
Reset	Click **Reset** button to restore to default values.
Current Filter Table	Shows the current IP filter information.
Delete Selected	Click **Delete Selected** button to delete items which are selected.
Delete All	Click **Delete All** button to delete all the items.
Reset	Click **Reset** button to rest.

MAC Filtering



Enable MAC Filtering	Check to enable MAC filtering function.
MAC Address	Enter the client MAC address in the field.
Comment	You may key in a description MAC address.
Apply Changes	After completing the settings on this page, click **Apply Changes** button to save the settings.
Reset	Click **Reset** button to restore to default values.
Current Filter Table	Shows the current MAC filter information.
Delete Selected	Click **Delete Selected** button to delete items which are selected.
Delete All	Click **Delete All** button to delete all the items.
Reset	Click **Reset** button to rest.

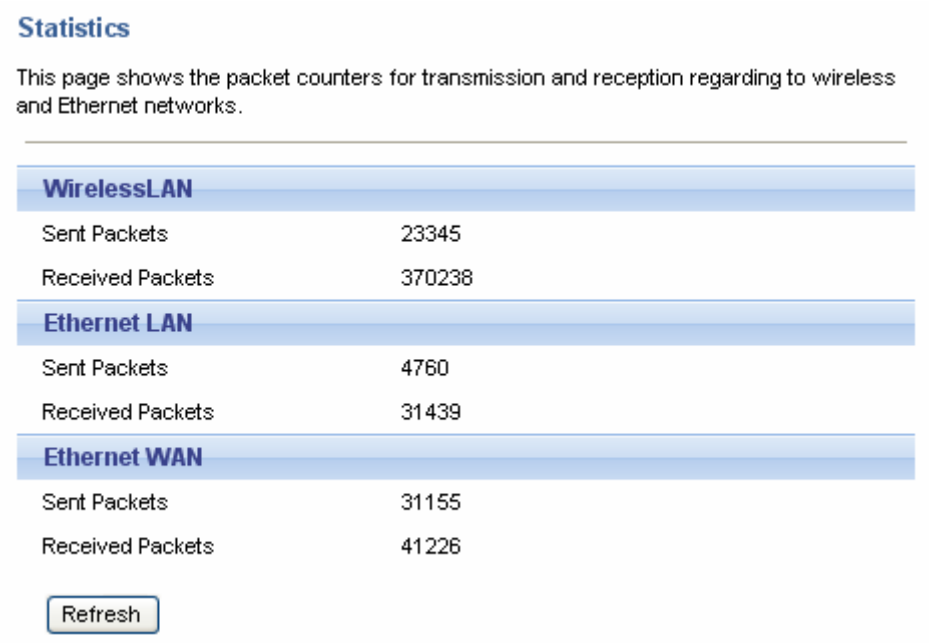
URL Filtering



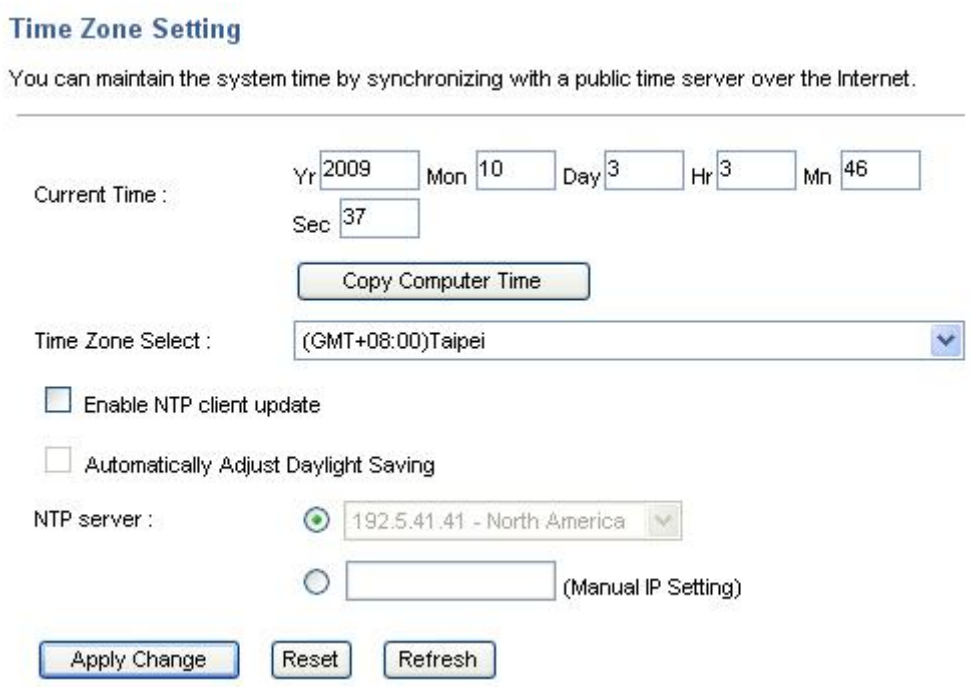
Enable URL Filtering	Check to enable URL filtering function.
URL Address	Enter the URL address in the field.
Apply Changes	After completing the settings on this page, click **Apply Changes** button to save the settings.
Reset	Click **Reset** button to restore to default values.
Current Filter Table	Shows the current URL address filter information.
Delete Selected	Click **Delete Selected** button to delete items which are selected.
Delete All	Click **Delete All** button to delete all the items.
Reset	Click **Reset** button to rest.

Statistics

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

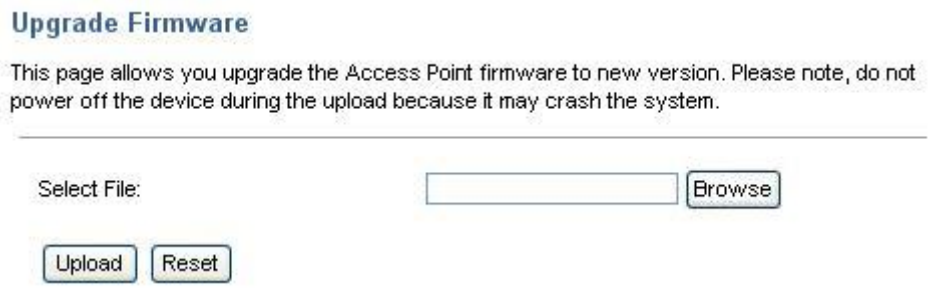


Time Zone Setting



Current Time	Enter the current time of this wireless router or click the **Copy Computer Time** button to insert the time automatically.
Time Zone Select	Select the local time zone from the pull-down menu.
Enable NTP client update	Check to enable **NTP (**Network Time Protocol Server) **client update** function.
Automatically Adjust Daylight Saving	Check the box to enable this function.
NTP server Manual IP setting	You may choose to select NTP server from the pull-down menu or enter an IP address of a specific server manually.
Apply Change	After completing the settings on this page, click **Apply Change** button to save current settings.
Reset	Click **Reset** button to restore to default values.
Refresh	Click **Refresh** button to renew current time.

Upgrade Firmware



Select File	Click the **Browse** button to find and open the firmware file (the browser will display to correct file path.)
Upload	Click the **Upload** button to perform.
Reset	Click **Reset** button to restore to default values.

Chapter 4: PC Configuration

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

Windows Clients

- This section describes how to configure Windows clients for Internet access via the Wireless Router.
- The first step is to check the PC's TCP/IP settings.
- The Wireless Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

If using default Wireless Router settings, and default Windows TCP/IP settings, no changes need to be made.

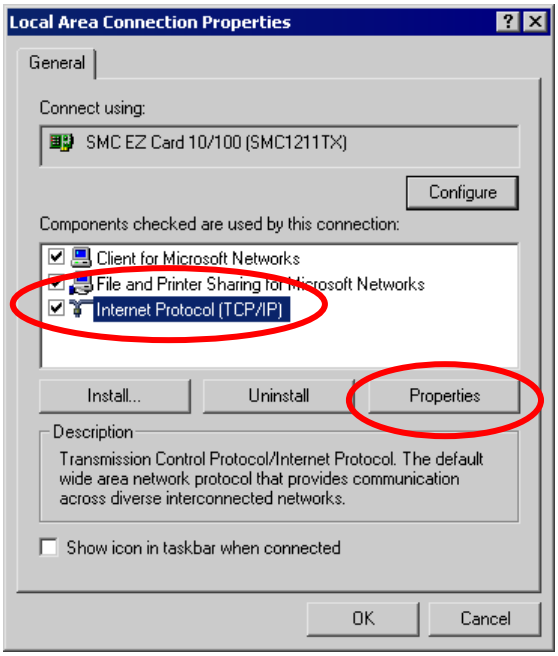
- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

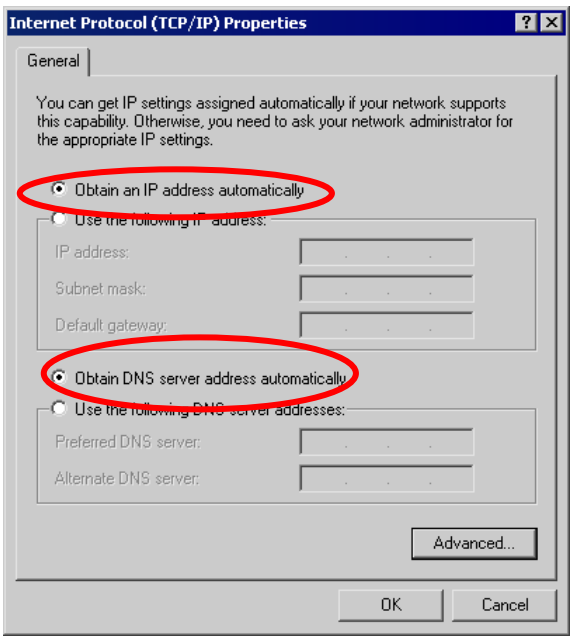
- The *Gateway* must be set to the IP address of the Wireless Router.
- The *DNS* should be set to the address provided by your ISP.

Checking TCP/IP Settings - Windows 2000

1. Select Control Panel - Network and Dial-up Connection.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:



3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



5. Ensure your TCP/IP settings are correct, as described below.

Using DHCP

- To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Router.

Using a fixed IP Address ("Use the following IP Address")

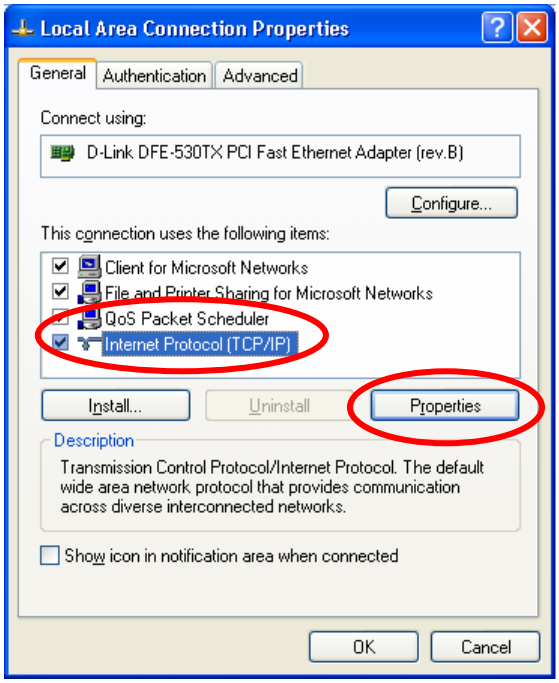
If your PC is already configured, check with your network administrator before making the following changes.

- Enter the Wireless Router 's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.)

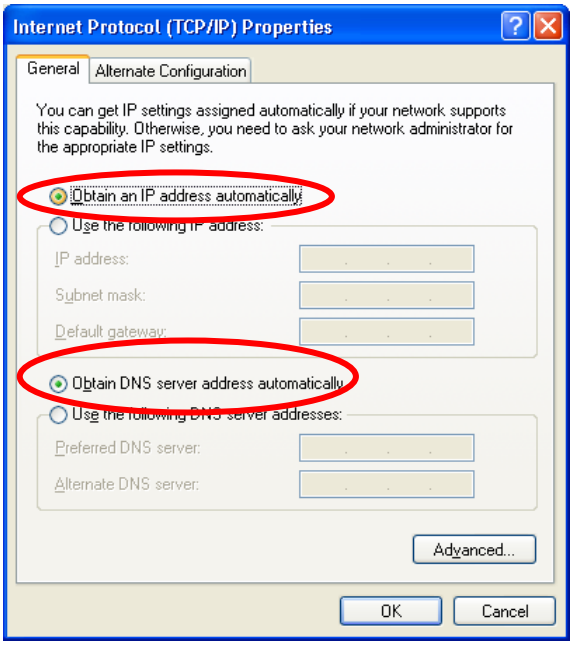
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

1. Select Control Panel - Network Connection.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:



3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



5. Ensure your TCP/IP settings are correct.

Using DHCP

- To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP address from the Wireless Router.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the Wireless Router 's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

Internet Access

To configure your PCs to use the Wireless Router for Internet access:

- Ensure that the ADSL modem, DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 2000

1. Select Start menu - Settings - Control Panel - Internet Options.
2. Select the Connection tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are unchecked.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click *Finish* to close the Internet Connection Wizard. Setup is now completed.

For Windows XP

1. Select ***Start*** menu >***Control Panel > Network and Internet Connections***.
2. Select ***Set up or change your Internet Connection***.
3. Select the ***Connection*** tab, and click the ***Setup*** button.
4. Cancel the pop-up "***Location Information***" screen.
5. Click ***Next*** on the "***New Connection Wizard***" screen.
6. Select "***Connect to the Internet***" and click ***Next***.
7. Select "***Set up my connection manually***" and click ***Next***.
8. Check "***Connect using a broadband connection that is always on***" and click ***Next***.
9. Click ***Finish*** to close the New Connection Wizard. Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the Wireless Router, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

1. Start the AOL for Windows communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
2. Click the Setup button.
3. Select Create Location, and change the location name from "New Locality" to " Wireless Router ".
4. Click Edit Location. Select TCP/IP for the Network field. (Leave the Phone Number blank.)
5. Click Save, then OK.
6. Configuration is now complete.
7. Before clicking "Sign On", always ensure that you are using the " Wireless Router " location.

Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless Router. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the Wireless Router 's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the Wireless Router, it is only necessary to set the Wireless Router as the "Gateway".
Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Router.
- Ensure your DNS (Domain Name server) settings are correct.

To act as a DHCP Client (Recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel – Network.*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes:
   - Use the "Deactivate" and "Activate" buttons, if available.
   - OR, restart your system.

Other Unix Systems

To access the Internet via the Wireless Router:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Router.
- Ensure your DNS (Name Server) settings are correct.

Wireless Station Configuration

- This section applies to all wireless stations wishing to use the Wireless Router 's access point, regardless of the operating system that is used on the client.
- To use the Wireless Router, each wireless station must have compatible settings, as following:

Mode	The mode must be set to *Infrastructure*.
SSID (ESSID)	The network name must match the value used on the Wireless Router. ***Note! The SSID is case- sensitive.***
Disable	If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended.
WEP	By default, WEP on the Wireless Router is disabled. • If WEP remains disabled on the Wireless Router, all stations must have WEP disabled. • If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.
WPA **WPA2** **WPA-Mixed** **802.1x**	RADIUS Server: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP.

Note: By default, the Wireless Router will allow 802.11b, 802.11g and 802.11n connections.

Appendix A: Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Wireless Router and some possible solutions to them. If you follow the suggested steps and the Wireless Router still does not function properly, contact your dealer for further advice.

General Problems

Problem 1:	Can't connect to the Wireless Router to configure it.
Solution 1:	Check the following: • Check the Wireless Router is properly installed, LAN connections are OK, and it is powered ON. • Ensure that your PC and the Wireless Router are on the same network segment. • If your PC is set to "Obtain an IP Address automatically" (DHCP client), please restart it. • If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.254 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1:	When I enter a URL or IP address I get a time out error.
Solution 1:	A number of things could be causing this. Try the following troubleshooting steps. • Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address. • If the PCs are configured correctly, but still not working, check the Wireless Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)

	• If the Wireless Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.
Problem 2:	Some applications do not run properly when using the Wireless Router.
Solution 2:	The Wireless Router processes the data passing through it, so it is not transparent. Use the *Content Filter Settings* feature to allow the use of Internet applications, which do not function correctly. If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but: • It is a security risk, since the firewall is disabled. • Only one (1) PC can use this feature.

Wireless Access

Problem 1:	My PC can't locate the Wireless Router.
Solution 1:	Check the following: • Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*) • The SSID on your PC and the Wireless Router are the same. Remember that the SSID is case-sensitive. So, for example "**W**orkgroup" does NOT match "**w**orkgroup." • Both your PC and the Wireless Router must have the same setting for security. The default setting for the Wireless Router security is disabled, so your wireless station should also have security disabled. • If security is enabled on the Wireless Router, your PC must have security enabled, and the key must be matched. • To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Router. Remember that the connection range can be as little as 100 feet in poor environments.
Problem 2:	Wireless connection speed is very slow.
Solution 2:	The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following: • Wireless Router location Try adjusting the location and orientation of the Wireless Router. • Wireless Channel If interference is the problem, changing to another channel may show a marked improvement. • Radio Interference Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.

	• RF Shielding Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Router.

Appendix B: About Wireless LANs

BSS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).
Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)

Note to US model owner:
To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

Security

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.
If WEP is used, the Wireless Stations and the Access Point must have the same security settings for each of the following:

WEP	64 Bits, 128 Bits.
Key	For 64 Bits encryption, the Key value must match. For 128 Bits encryption, the Key value must match.
WEP Authentication	Open System or Shared Key.

WPA / WPA2

WPA/WPA2 (Wi-Fi Protected Access) is more secure than WEP. It uses a "Shared Key" which allows the encryption keys to be regenerated at a specified interval. There are several encryption options: **TKIP, AES, TKIP-AES** and additional setup for **RADIUS** is required in this method. The most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency.

If WPA or WPA2 is used, the Wireless Stations and the Access Point must have the same security settings.

802.1x

With **802.1x** authentication, a wireless PC can join any network and receive any messages that are not encrypted, however, additional setup for **RADIUS** to issue the WEP key dynamically will be required. RADIUS is an authentication, authorization, and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	The mode must be set to *Infrastructure*.
SSID (ESSID)	The network name must match the value used on the Wireless Router. ***Note! The SSID is case- sensitive.***
Disable	If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended.
WEP	By default, WEP on the Wireless Router is disabled. • If WEP remains disabled on the Wireless Router, all stations must have WEP disabled. • If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.
WPA **WPA2** **WPA-Mixed** **802.1x**	RADIUS Server: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP.