Wireless 802.11b/g VPN Router

User's Manual

FCC Certifications

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.

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. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

CE Mark Warning

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:
All trade names and trademarks are the properties of their respective companies.

Table of Contents

Unpacking Information

Thank you for purchasing the product. Before you start, please check all the contents of this package.

The product package should include the following:

1. **One Wireless VPN Router**
2. **One power adapter**
3. **One User Manual (CD)**
4. **One detachable antenna**

Introduction To Wireless Router

General Description

The Wireless Router built-in with 4-port 10/100Mbps Fast Ethernet Switch is the latest generation of Wireless router product for Home/Office and SOHO users. This full-feature and self-contained compact Wireless Router will be fully for broadband access in both of LAN and Wireless environment. This device has been specifically designed to provide LAN and Wireless users the most cost-effective method with multiple accesses to the Internet at the cost of a single public IP address（IP Sharing）and enjoy the true Plug-and-Play installation. Moreover, the built-in 4-port 10/100Mbps switch lets users plug the network cable into the device without buying additional switch.

This device is also an Access Point. It has a built-in wireless LAN. Users can connect to Internet using wireless network interfaces anywhere within the range of its radio transmission. It's ideal for SOHO users who require instant and convenient access to Internet without the restriction of connecting cables.

The friendly WEB-based graphics interface for setup makes any inexperienced users soon enter plug-and–play operation. Embedded DHCP server simplified IP address management and no MIS people needed for daily technical services. What is more, NAT/firewall is also implemented on this compact Router Box for protecting whole LAN from outside attack.

Key Features

The switch provides the following key features:

- Complies with IEEE 802.11b/g wireless standards
- Provides one 802.11b/g wireless Reverse SMA detachable antenna
- High speed transfer data rate up to 54Mbps
- Supports turbo mode for 72Mbps data transfer
- Supports wireless data encryption with 64/128-bit WEP, WPA (TKIP with IEEE 802.1x), WPA2 and AES functions
- Supports system log
- Supports authentication for wireless connectivity based on ESSID
- Provides MAC access control and hidden SSID function
- WDS supported with WEP, TKIP and AES encryption
- Channel : USA 11, Europe 13
- Supports NAT/NAPT IP Sharing
- Supports Static IP, PPPoE, PPTP, & DHCP client
- SPI Anti-DoS Firewall; Virtual DMZ; DNS relay; UPnP
- Support VPN
- Provides DHCP server
- Supports PSK, RSA authentication type for VPN.
- Supports VPN IKE Key management.
- Supports VPN pass through
- Supports ALG for FTP, NetMeeting, VPN pass-through, DDNS (DynDNS, TZO)
- Supports firmware upgrade function via Web
- Compliant with FCC Part 15.247 for US, ETS 300 328 for Europe
- Flash : 2MB NOR type, SDRAM : 16MB
- Certifications : FCC Class B, CE Mark

The Front Panel

The front panel of the Wireless Router is shown below.

System LEDs

System LED indicators locate on the front panel for showing the operating status of the whole device.

- PWR (Power) LED
  This indicator lights green when the Wireless Router is receiving power; otherwise, it is off.

- Status LED
  The LED will be dark for a few seconds when the system is started. After that, the LED will blink periodically to show the Wireless Router is working normally. If the LED stays green/dark that means the system failed, you need to contact your agent or try to reboot the system.

Port LEDs (Wireless)

- ACT LED
  I. When Wireless AP is ready for data transmitting and receiving, it is steady green.
  II. When the data is transmitting or receiving, it is blinking green.

Port LEDs (WAN)

Port LED (WAN) indicators locate on the front panel for showing the operating status of WAN port.

- Act/Link LED
  The LED stays light (green) means the port has good linkage to its associated devices.
  The LED will blink green when there is traffic transverse the port.

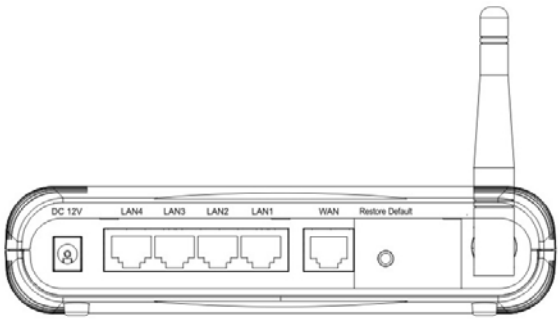
Port LEDs (LAN)

Port LEDs (LAN) indicators locate on the front panel for showing the operating status of 10/100Mbps Fast Ethernet switching ports.

- Act/Link LED
  Every port has a Act/Link LED. Steady green (link state) indicates that the port has good linkage to its associated devices. Flashing green indicates that the port is receiving or transmitting data between its associated devices.

The Rear Panel

The rear panel of the Wireless Router is shown below



Power Connection

Plug the circle end of the power adapter firmly into the rear panel of the Wireless Router, and the other end put into an electric service outlet then the system is ready.

Placement (Optional)

There are three ways to place the Router. The first way is to place the Router horizontally on a surface. The second way is to attach the router to the wall. The third way is to stand the Router vertically on a surface. These options are explained in further detail below.

Desktop Option

1. The Router has one plastic stand that can be divided into two parts.
2. Combine one part of stand with the side of router.
3. Do the same with the second part.
4. Place the Router

Wall-mount option

Before attach this router on the wall, you have to finish the desktop option steps first.

1. Select a location with access for cables and a power outlet.
2. Unplug the unit. Place it upside down on a flat surface and mark the two holes for anchors.
3. Installing the Wall mount anchor (plastic) into the wall with tools such as drill or hammer.
4. Insert the provided screws in each hole of the stand parts.
5. Attaches the unit to the anchors on the wall.

Stand Option

1. The Router includes two stand parts.
2. Combine two parts into one stand. Combine it with the side of router near the power port. Push the stand up to snap it into place.
3. Place the Router.

Restore Default Button

1. Push the button for more than 5 seconds and then release it, the system will return to factory default setting. In the meantime, system rewrites flash to default value and Status LED halts for a while. Approximately 60 seconds later, the Status LED blinks green periodically, now the whole system parameters have returned to factory default value. If the process has been interrupted by any reason (power off…), the system will fail. Before performing the process, ensure a safe operating environment please！
2. To reboot the Router, Press the button for 2-5 seconds and then release it, and all the setting won't be erased. Wait for the Router to complete the reboot, and then you can start to use it.

Warning： Incomplete factory setting recovery procedure will cause the Wireless Router malfunction！If you are unfortunately in this situation, do not try to repair it by yourself. Consult your local distributor for help！

Installing And Using Wireless Router

This Chapter provides a step-by-step guide to the installation and configuration of the Wireless Router. We suggest you go over the whole chapter and then do more advanced operation.

Network configuration setup

Steps to build up the network:

- Connect the ADSL or Cable modem to the Ethernet WAN port on the back of the Wireless Router by using the UTP cable.
- Connect the phone line from the wall socket to the line-in port on the ADSL modem, or the coaxial cable to the line-in port on the Cable modem.
- Plug-in the power adapter to the modem and turn on the power. Install the Ethernet card into the computer by referring to the User Guide that came with the card.
- Connect the computer to the Wireless Router by using standard twisted-pair Ethernet cable from the computer's Ethernet card to an 10/100Mbps Ethernet port on the back of the Wireless Router.
- Plug-in the power adapter to the Router and the other side to the wall outlet.

Computer configuration setup

In order to communicate with this Wireless Router, you have to configure the IP addresses of your computer to be compatible with the device. The router supports DHCP server and it is enabled as default. Users that configure your IP address as **"Obtain an IP address automatically"** may skip the following IP configuration instruction.

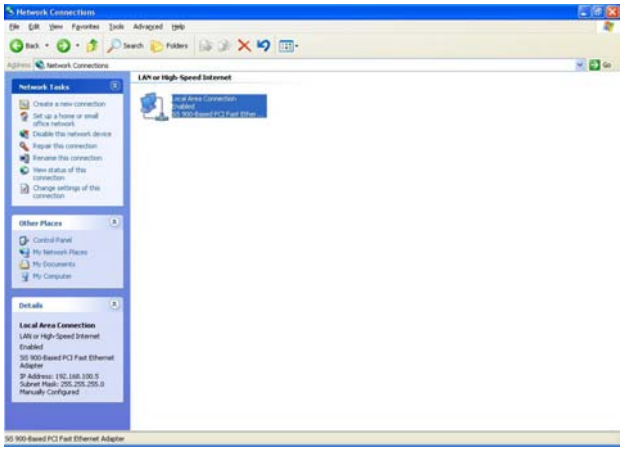
Note:

1. The default network setting of the device:
   IP address: 192.168.1.1
   Subnet Mask: 255.255.255.0
   DHCP Server: enabled

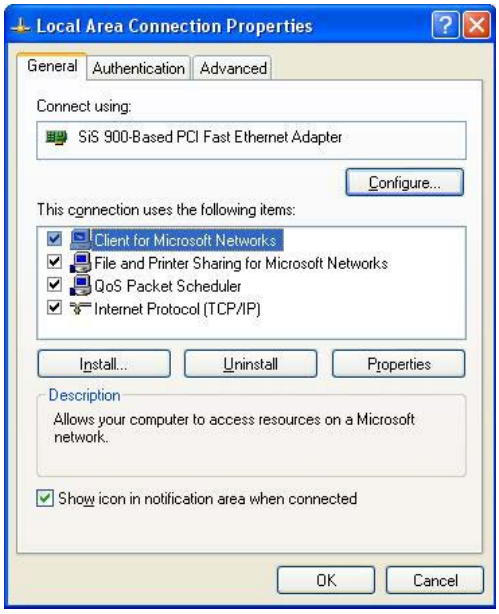
2. In the following TCP/IP configuration guide, the IP address "192.168.1.2 " is assumed to be your IP address if you want to specify IP addresses manually. Please **DO NOT** choose 192.168.1.1 for the IP address (192.168.1.1) has been set as the default IP for this device.
3. The following TCP/IP configuration guide uses windows XP as the presumed operation system.

Procedures to configure IP addresses for your computer

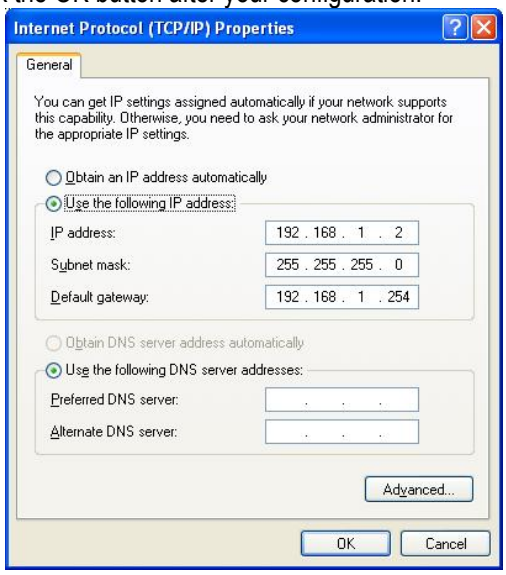
1. If you are in Classic Start menu view, click **Start→Settings→Control Panel→Network Connections**.
   If you are in Start menu view, click **Start→Control Panel→ Network Connections.**
2. Double click "**Local Area Connection**"



3. Choose **Internet Protocol (TCP/IP)** and click **Properties.**



4. You may choose “Obtain an IP address automatically”(recommend) to get IP address automatically or choose “Use the following IP address” to specify IP addresses manually. Please click the OK button after your configuration.



Management

Wireless Router configuration setup

In order to make the whole network operate successfully, it is necessary to configure the Wireless Router through your computer has a WEB browser installed. Please follow up the steps listed below.

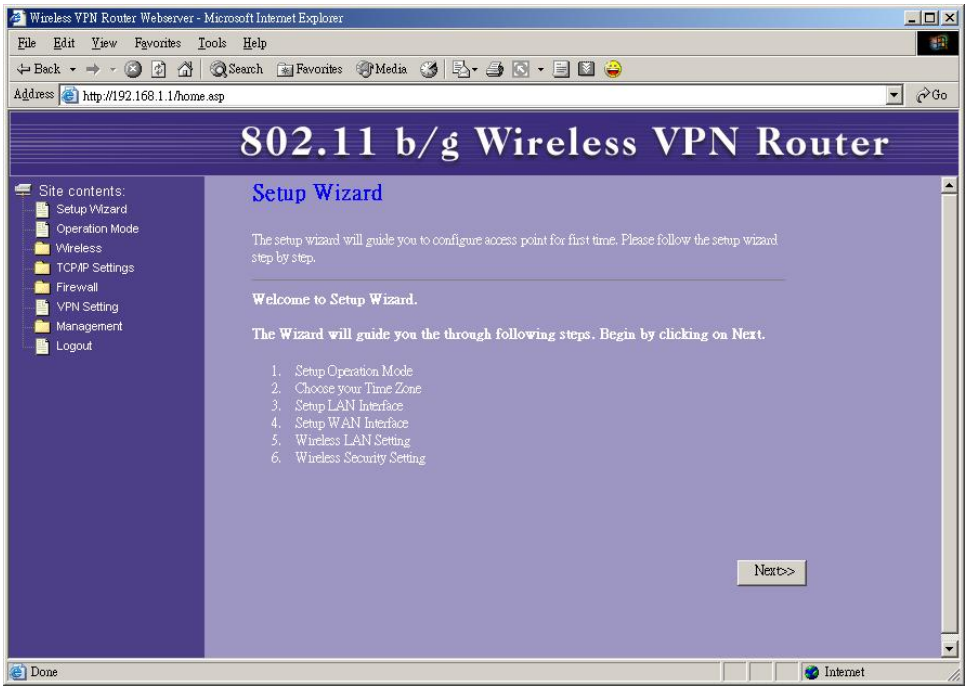
1. Double click the Internet WEB browser icon on your desktop screen (Netscape Communicator 4.0 and Internet Explorer 3.0 or update version)

2. Type 192.168.1.1 into the URL WEB address location and press Enter.

3. The Username and Password Required window appears.
   - Enter **admin** in the User Name location (default value).
   - Enter **admin** in the Password location (default value).
   - Click **"OK"** button

4. The Graphic User Interaface

After the password authorization, the Setup Wizard shows up as the home page of the Graphic User interface. You may click on each folder on left column of each page to get access to each configuration page.

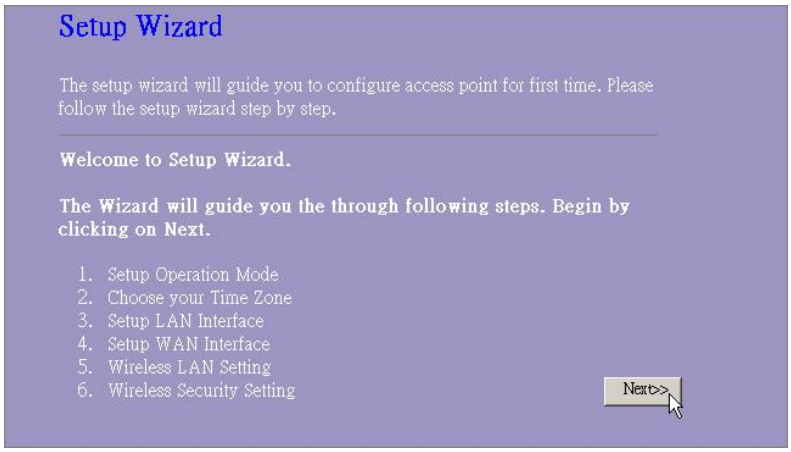


Setup Wizard

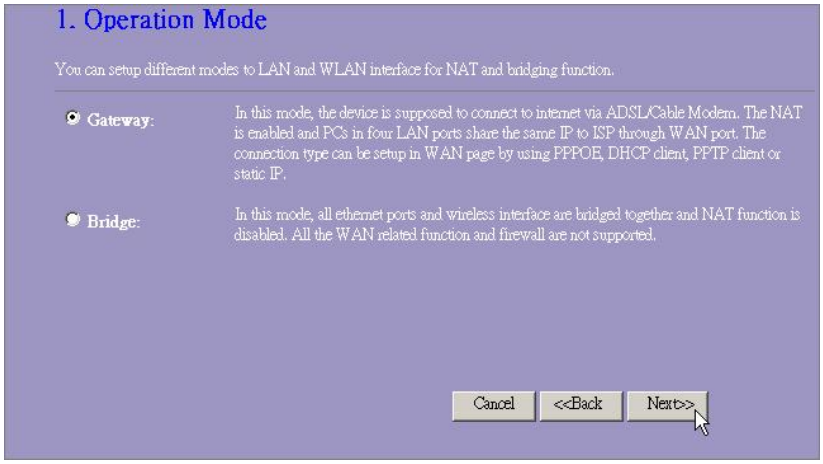
If you are using the router for the first time, you may follow the procedures of the setup wizard to do a step-by-step configuration.

Note: The following instruction does an overall introduction to the Setup Wizard. For detail information to each item, please refer to instruction of each page.

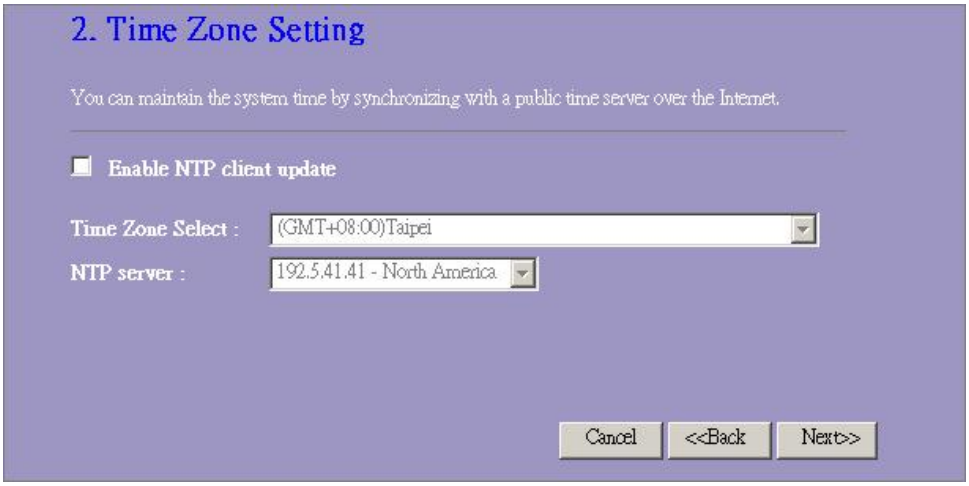
1. To start the Setup Wizard, click the “Next” button to proceed.



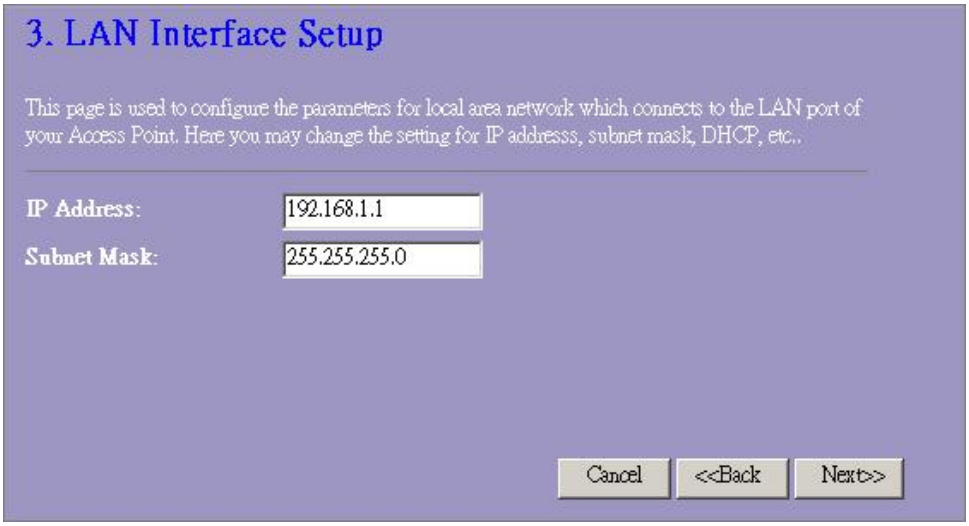
2. Select your demanding operation mode and click “Next”.



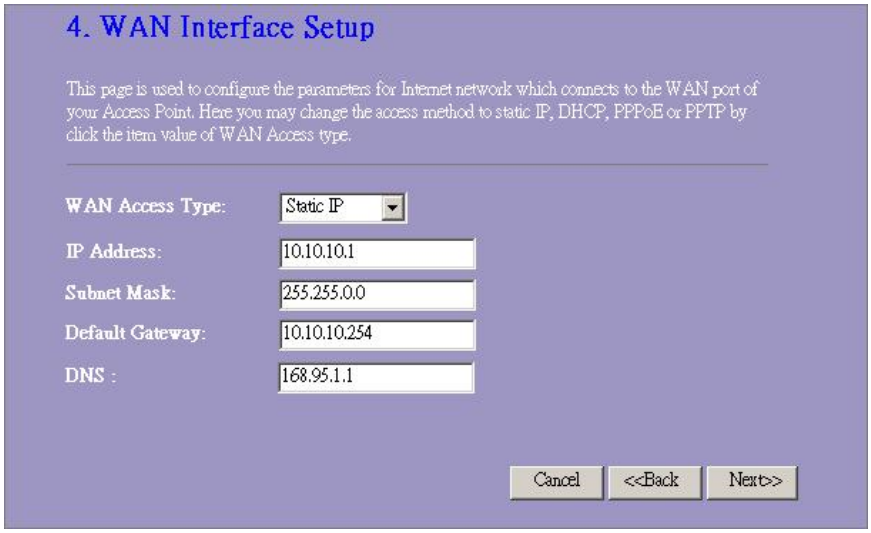
3. Mark the check box to enable synchronizing time by NTP server. Select the religion you live and a NTP server by clicking the drop list then click “Next”.



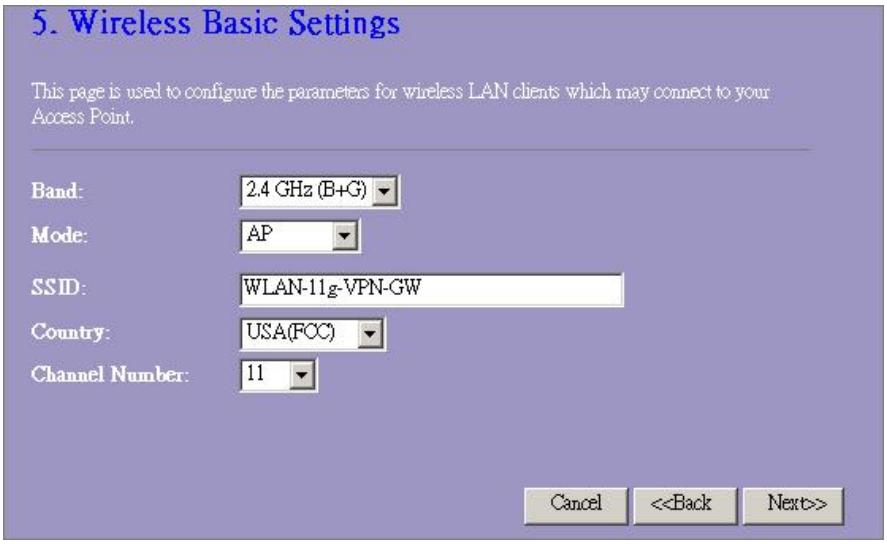
4. Specify an IP address and subnet mask for connecting to the router in LAN.



5. Select a WAN access type for the router to connect to Internet. Fill in the parameters that required in each blank, and then click the “Next” button. You may get those parameters from your ISP.



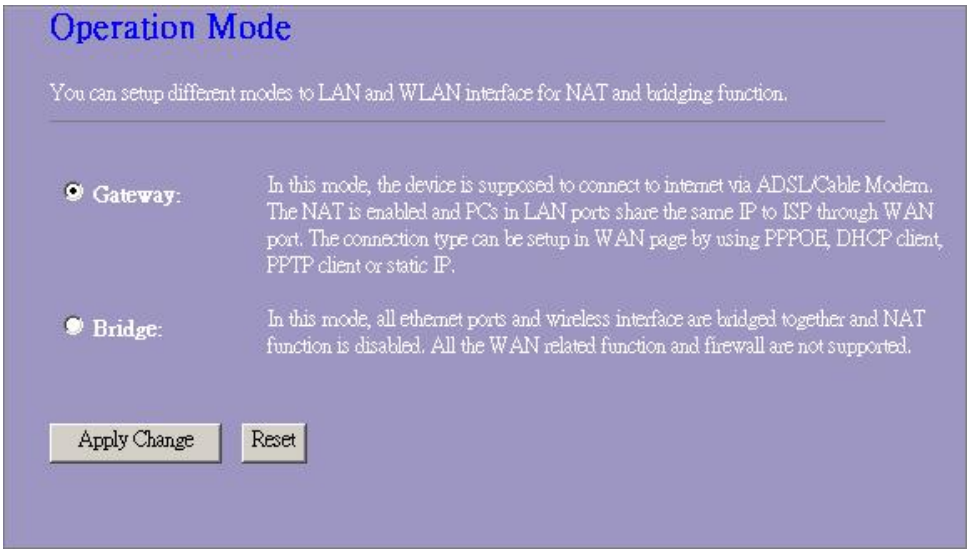
6. Select the wireless parameters that are used for associating with this router and click **“Next”**



7. Click the drop list to select the encryption type for your wireless network. Fill in the parameters for the encryption type you select and click finish to complete configuration.

Operation Mode

To select an operation mode for this router, click on the mode that you want to perform and click the Apply Change button to execute.

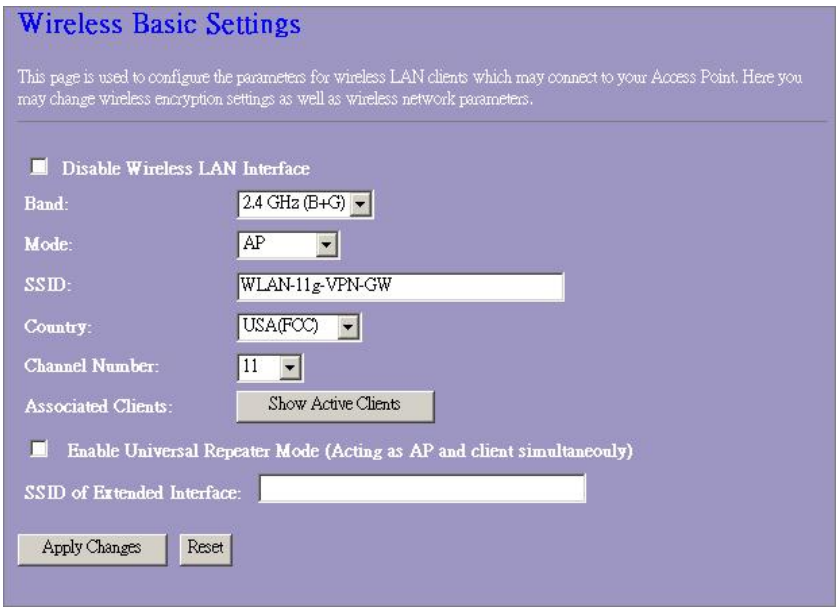


Wireless

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE802.11b/g wireless network adaptor connect to your Intranet. It supports WEP encryption and MAC address filter to enhance the security of your wireless network.

Basic Settings

You can set up the configuration of your Wireless and monitor the Wireless Clients associate with your AP.



Configuration

Disable Wireless LAN Interface	To Disable interface of Wireless LAN
Band	To select a band for this device to match 802.11b, 802.11g or both.
Mode	Configure this device as AP, WDS or both.
SSID	The name of the wireless network
Country	Select the region you live.
Channel Number	The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

Associated Clients	Click "Show Active Clients" button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.
Enable Universal Repeater Mode	Mark this checkbox to enable Universal Repeater Mode which acts this device as an AP and client simultaneously.
SSID of Extended Interface	While you enable the Universal Repeater Mode, you have to specify an SSID for the extended interface.

Click **<Apply changes>** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

- **Active Wireless Client Table**

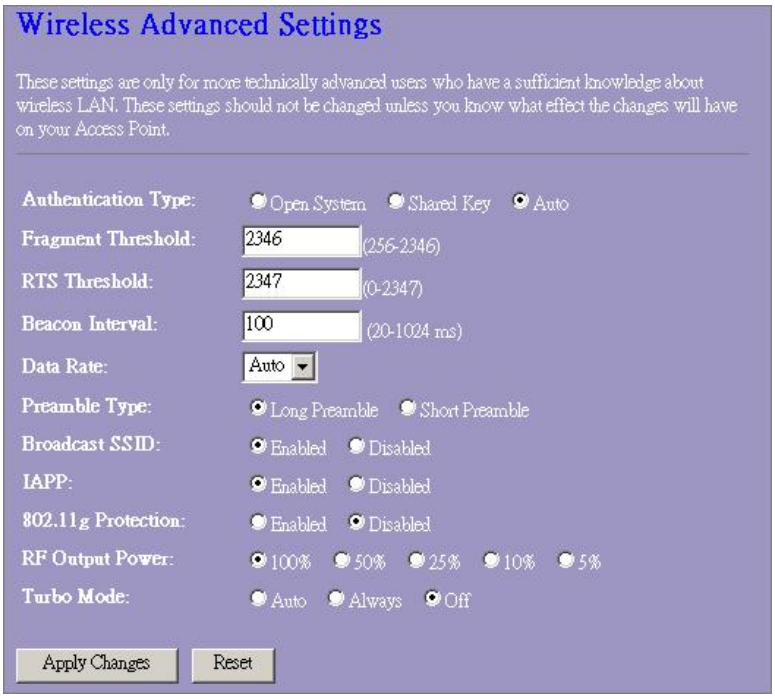
  This is the window that pops up after clicking the **"Show Active Clients"** button.

MAC Address	MAC address of this active wireless station.
Tx Packet	The number of transmitted packets that are sent out from this active wireless station.
Rx Packet	The number of received packets that are received by

	this active wireless station.
TX Rate	The transmission rate
Power Saving	Shows if the wireless client is in Power Saving mode
Expired Time	This is the time in second before dissociation. If the wireless keeps idle longer than the expired time, this wireless router will dissociate it. The wireless client station has to associate again when it is active.
Refresh	Refresh the "Active Wireless Client Table".
Close	Close the "Active Wireless Client Table".

Advanced Settings

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Data Rate, Preamble Type, Broadcast SSID, IAPP and 802.11g Protection. We recommend not changing these parameters unless you know what changes will be there on this router.



Configuration

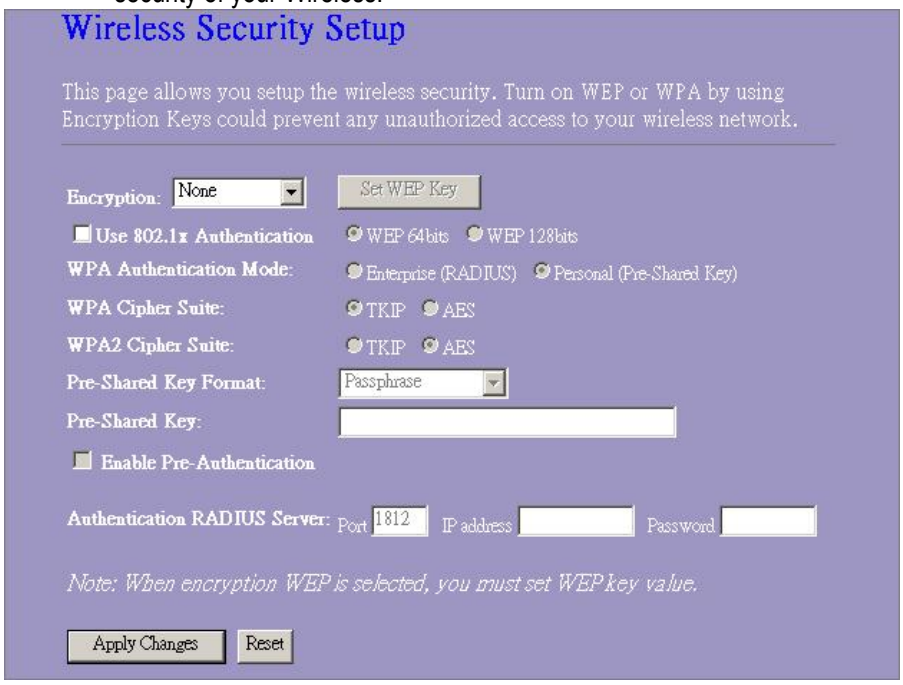
Authentication Type	**Open System mode**	Wireless AP can associate with this wireless router without WEP encryption.
	Shared Key mode	You should also setup WEP key in the "Security" page and wireless AP associating with this wireless router should use WEP encryption in the authentication phase.
	Auto	The wireless client can associate with this wireless router by using any one of these two Modes.
Fragment	To specifies the maximum size of packet during the data	

Threshold	transition. The lower values you set, the worst performance it will be.
RTS Threshold	If the packet size is smaller the RTS threshold, the wireless router will not send this packet by using the RTS/CTS mechanism.
Beacon Interval	The period of time how long a beacon is broadcasted.
Data Rate	The "Data Rate" is the data packets limitation this wireless router can transmit. The wireless router will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	It defines the length of CRC block in the frames during the wireless communication. "Short Preamble" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability
Broadcast SSID	If you enable "Broadcast SSID", every wireless station located within the coverage of this wireless router can discover this wireless router easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast SSID" can provide better security.
IAPP	To enables multiple AP to communicate and pass information regarding the location of associated Stations.
802.11g Protection	Some 802.11g wireless adapters support 802.11g protection, which allows the adapters searches for 802.11g singles only. Select the “Disabled” to disable supporting 802.11g protection or select “enable” to support this function.
RF Output Power	Select the RF (Radio Frequency) power. The RF output power has positive correlation with signal strength.
Turbo Mode	Some of our wireless adapters supports turbo mode, which provides a better connection quality. Select “Always” to support turbo mode or select “off” to turn it off . Select “Auto” turns it on or off automatically.

Click the **<Apply Changes>** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

Security

At the page, you can set up the WEP, WPA Encryption to ensure the security of your Wireless.



Configuration

Encryption	To enable WEP, WPA, WPA2 and WPA2 Mixed encryption modes, select the option in the drop list. If you select none, any data will be transmitted without Encryption and any station can access the router.
Use 802.1x Authentication	To enable the 802.1x, Click the check box of the item.
WPA Authentication Mode	There are two items, “Enterprise (WPA-Radius)” and “Personal (Pre-Shared Key)”. You can select the mode by clicking the item.
WPA Cipher Suite	Select the WPA Cipher Suite to be TKIP or AES

WPA2 Cipher Suite	Select the WPA2 Cipher Suite to be TKIP or AES
Pre-Shared key Format	To decide the format, select what you need in the drop list.
Pre-shared Key	Enter the Pre-shared Key according to the pre-shared key format you select.
Enable Pre-Authentication	You can mark this checkbox to enable Pre-authentication after selecting Enterprise (RADIUS) WPA 2 authentication mode
Authentication RADIUS Sever	If you use RADIUS Sever to ensure your security, you have to set up the parameters in the item. To set up the Port, IP address and Password of your RADIUS, Enter the Port Number, IP and Password.

Click **<Apply Change>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

Access Control

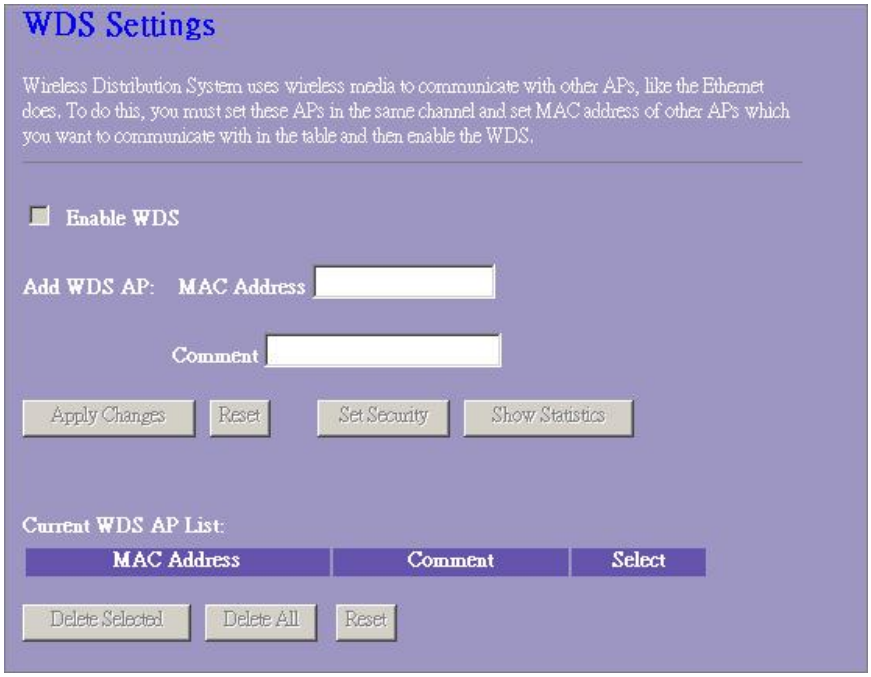
To restrict the Number of Access authentication of Stations, Set up the control list in this page.

Configuration

Wireless Access Control Mode	Click on the drop list to choose the access control mode. You may select “Allow listed” to allow those allowed MAC addresses or select “Deny Listed” to ban those MAC addresses from accessing to this device.
MAC Address & Comment	To set up the Value of MAC Address & Comment; enter the MAC Address and Comment of station and click Apply Changes to save.
Current Access Control list	To Delete the station on the list, Click the check box in the select item and click the “Delete Selected”. If you want to delete all stations on the list, click “Delete All” to remove all of them.

Click <Apply Change> button to save the above configurations. You can now configure other advance sections or start using the router.

WDS Setting



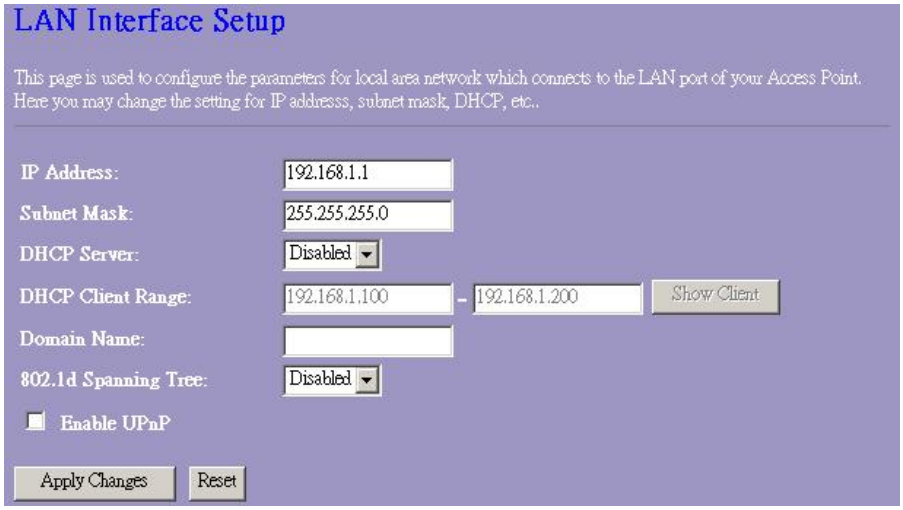
Wireless Distribution System allows the router to communicate with other APs wirelessly. To make it work, you must ensure that these APs and the Router are in the same Channel and add these APs MAC Address and Comment values into the WDS list. Don't Forget to Enable the WDS by click the check box of "Enable WDS" and press "Apply Changes" button to save.

To Delete the AP on the list, Click the check box in the select item and click the "Delete Selected". If you want to delete all APs on the list, click "Delete All" to remove all of them.

TCP/IP Setting

LAN Interface Setup

To set up the configuration of LAN interface, Private IP of you router LAN Port and Subnet mask for your LAN segment.



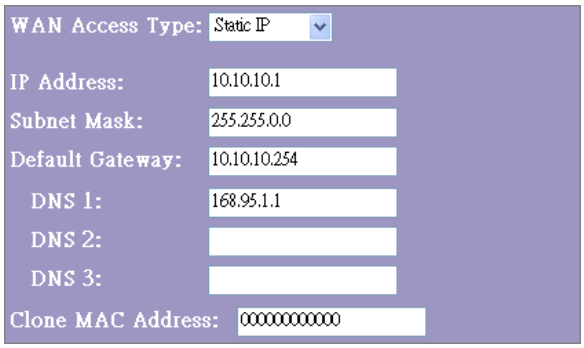
Configuration

IP address	The IP of your Router LAN port (Default 192.168.1.1)
Subnet Mask	Subnet Mask of you LAN (Default 255.255.255.0)
DHCP Server	To give your LAN Client an IP, you have to enable “DHCP Server”. If not, manual setting up your client IP is necessary when you want to use the router as your client’s default gateway.
DHCP Client Range	Specify the DHCP Client IP address range. You can also click the “Show Client” button to listed those connected DHCP clients.
Domain Name	Specify a domain name of the device.
802.1d Spanning tree	To prevent from network loops and preserve the quality of bridged network
Enable UPnP	Mark this checkbox to allow this router to be recognized by UPnP.

WAN Interface Setup

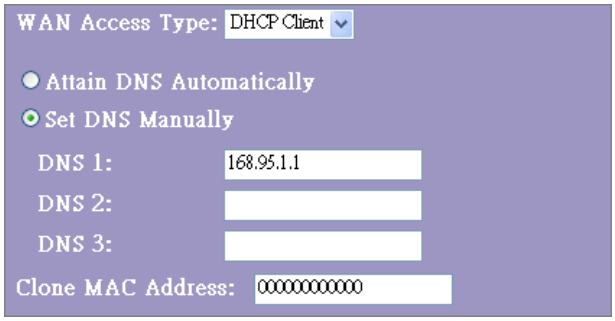
This page allows users to configure those parameters for connecting to Internet. You may select the WAN Access Type from the drop list and configure parameters for each mode.

Static IP Mode



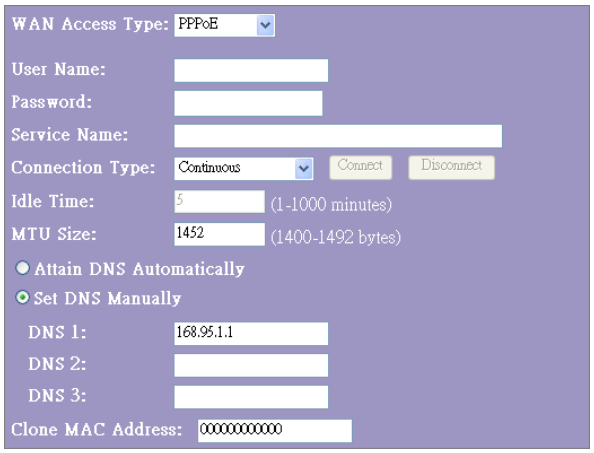
IP Address, Subnet Mask and Default Gateway	Fill in the IP address, Subnet Mask and Default Gateway that provided by your ISP.
DNS 1, 2 and 3	To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

DHCP Client Mode



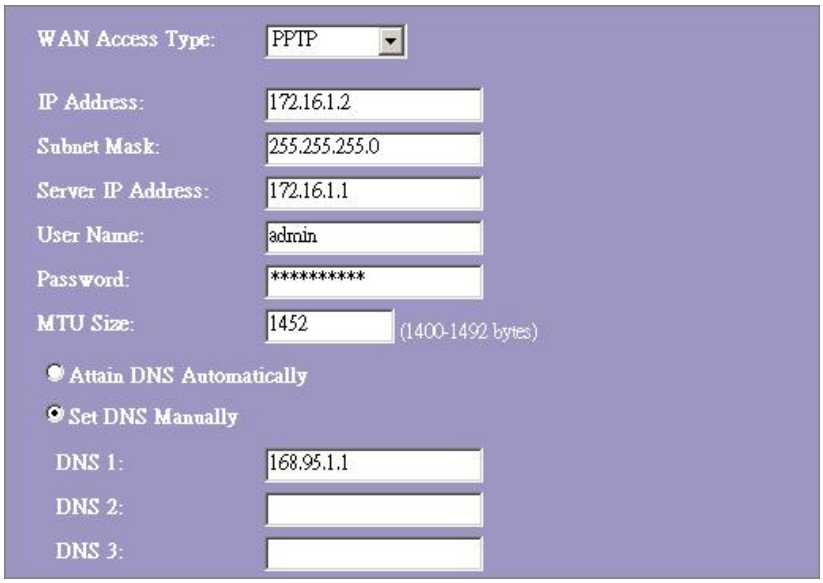
Attain DNS automatically:	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically"
Set DNS Manually	To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

PPPoE Mode



User Name, password and service name	Fill in the User Name, password and service name that provided by your ISP.
Connection Type	**"Continuous"** is for Always keep connection
	"Connect on demand" is for bill by connection time. You can set up the Idle time for the value specifies the number of time that elapses before the system automatically disconnects the PPPoE session.
	"Manual" To connect to ISP, click "Connect" manually from the WEB user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.
Idle Time:	The value specifies the number of idle time that elapses before the system automatically disconnects the PPPoE session.
MTU Size	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter your MTU number in the text-box to set the limitation.
Attain DNS automatically:	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically
Set DNS Manually	To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

PPTP Mode



IP Address, Subnet Mask, Server IP Address, User Name and Password	Fill in the IP address, Subnet Mask, Server IP Address, User Name and password that provided by your ISP.
MTU Size	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter your MTU number in the text-box to set the limitation.
Attain DNS automatically:	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically"
Set DNS Manually	To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

Common configurations for WAN interface

There are some settings are able to be configured on each WAN access types:

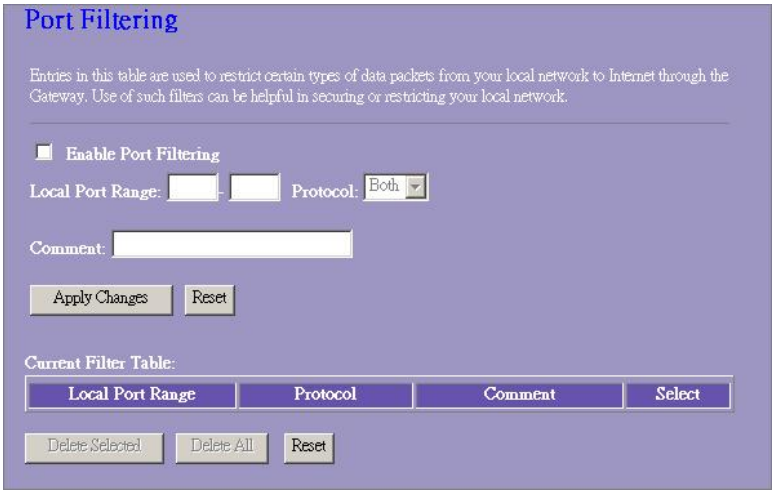
Enable Ping Access on WAN	Allow users on WAN to ping this device.
Enable Web Server Access on WAN from port	To Enable the user to access this Router through Internet, Enter the specific IP and the port number
Enable IPsec pass through on VPN connection	Mark the check box to enable IPsec pass through on VPN connection and clear the checkbox to disable.
Enable PPTP pass through on VPN connection	Mark the check box to enable PPTP pass through on VPN connection and clear the checkbox to disable.
Enable L2TP pass through on VPN connection	Mark the check box to enable L2TP pass through on VPN connection and clear the checkbox to disable.
Clone MAC Address	When ISP use MAC address authentication (with DHCP), then the MAC address of the Ethernet card attached to your Cable modem must be registered with the ISP before connecting to the WAN (Internet). If the Ethernet card is changed, the new MAC address must be registered with the ISP. MAC cloning feature allows the MAC address reported by WAN side network interface card to be set to the MAC address already registered with the ISP eliminating the need to register the new MAC address with the ISP. This feature does not change the actual MAC address on the NIC, but instead changes the MAC address reported by Wireless Router to client requests. To Change the MAC address, enter it in the text box.

Firewall Configuration

Port Filtering

The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users.

Port Filtering To restrict certain type of data packets from your LAN to Internet through the Router, add them on the Current Filtering Table.



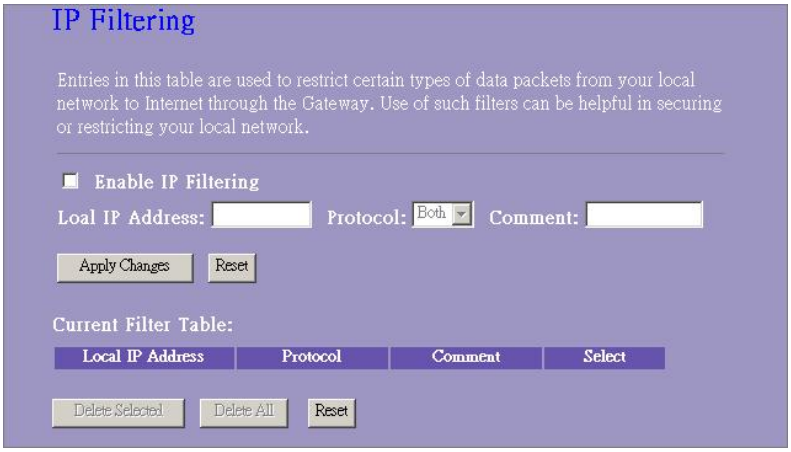
Configuration

STEPS	1.	Click the check box of “Enable Port Filtering” to enable the function.
	2.	Enter the Port range (EX 25-110), Protocol (UDP/TCP), and comment (EX. E-Mail)
	3.	To Delete the Port range on the list, Click the check box in the select item and click the “Delete Selected”. If you want to delete all entries on the list, click “Delete All” to remove all of them.

Click <Apply Change> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

IP filtering

The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet.



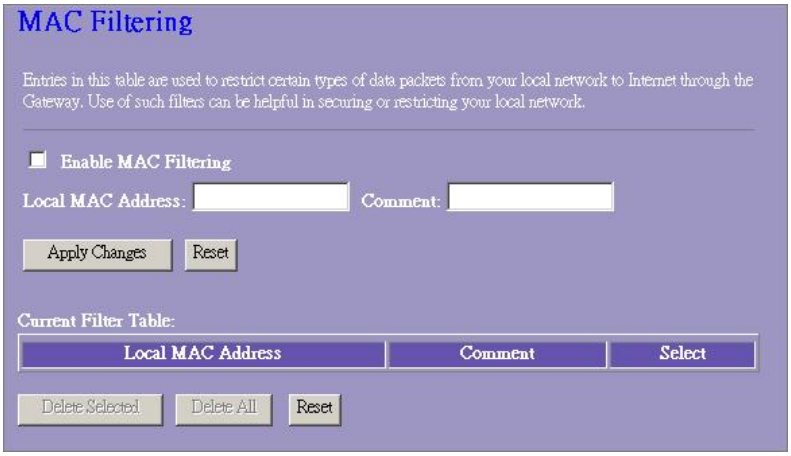
Configuration

STEPS	1.	Click the check box of “Enable IP Filtering” to enable the function.
	2.	Enter the specific Local IP address (EX 10.10.3.9), Protocol (UDP/TCP), and comment (EX. Peter)
	3.	To Delete the IP address on the list, Click the check box in the select item and click the “Delete Selected”. If you want to delete all entries on the list, click “Delete All” to remove all of them.

Click <Apply Change> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

MAC filtering

The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the MAC addresses to block specific internal users from accessing the Internet.



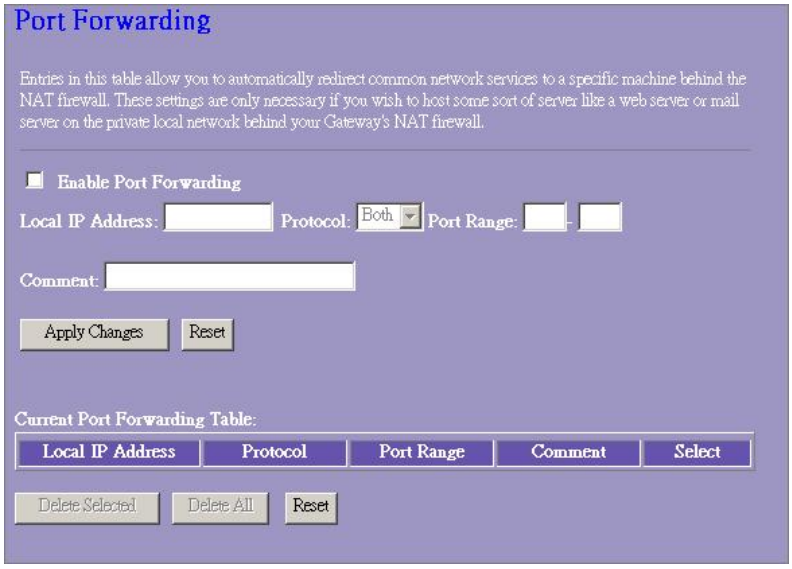
Configuration

STEPS	1.	Click the check box of “Enable MAC Filtering” to enable the function.
	2.	Enter the specific MAC address (EX 00:0e:b6:a8:72), and comment (EX. Peter)
	3.	To Delete the MAC address on the list, Click the check box in the select item and click the “Delete Selected”. If you want to delete all Entries on the list, click “Delete All” to remove all of them.

Click <Apply Change> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

Port forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.



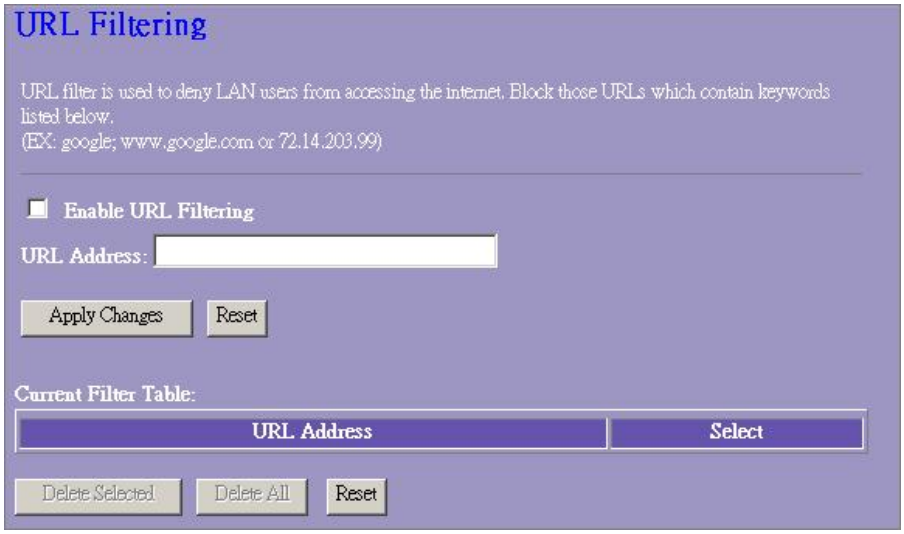
Configuration

STEPS	1.	Click the check box of “Enable port forwarding” to enable the function.
	2.	Enter the specific IP address (EX 10.10.10.10), Protocol (UDP/TCP), Port range (EX 25-110), and comment (EX. E-Mail)
	3.	To Delete the IP address on the table, Click the check box in the select item and click the “Delete Selected”. If you want to delete all Entries on the table, click “Delete All” to remove all of them.

Click <Apply Change> at the bottom of the screen to save the above configurations.

URL Filtering

The URL Filter allows users to prevent certain URL from accessing by users in LAN. This filter will block those URLs that contain certain keywords.



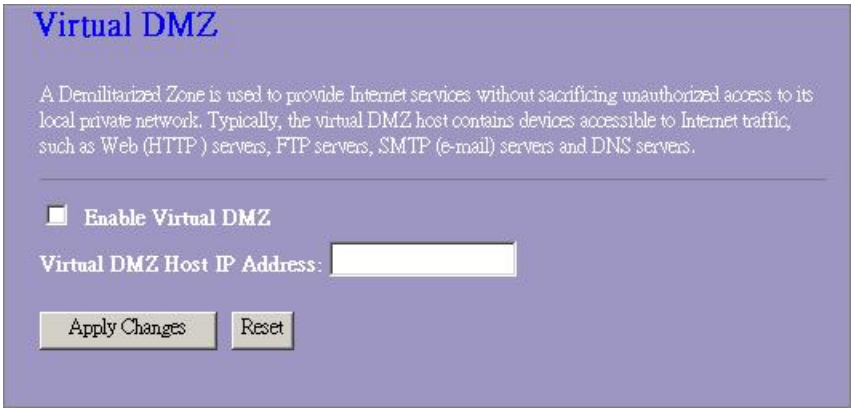
Configuration

STEPS	1.	Click the check box of “Enable URL Filtering” to enable the function.
	2.	Enter the URL that is going to be banned.
	3.	To Delete the URL on the table, Click the check box in the select item and click the “Delete Selected”. If you want to delete all URLs on the table, click “Delete All” to remove all of them.

Click <Apply Change> at the bottom of the screen to save the above configurations.

Virtual DMZ

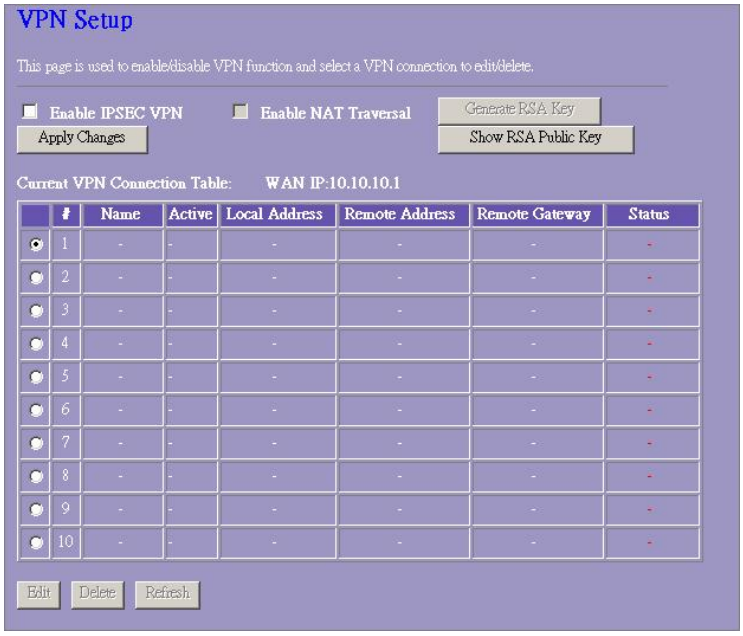
The virtual DMZ is used to enable protocols, which need to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this page.



To configure it, enter the Host IP (private IP address) and Click "Apply changes" to enact the setting.

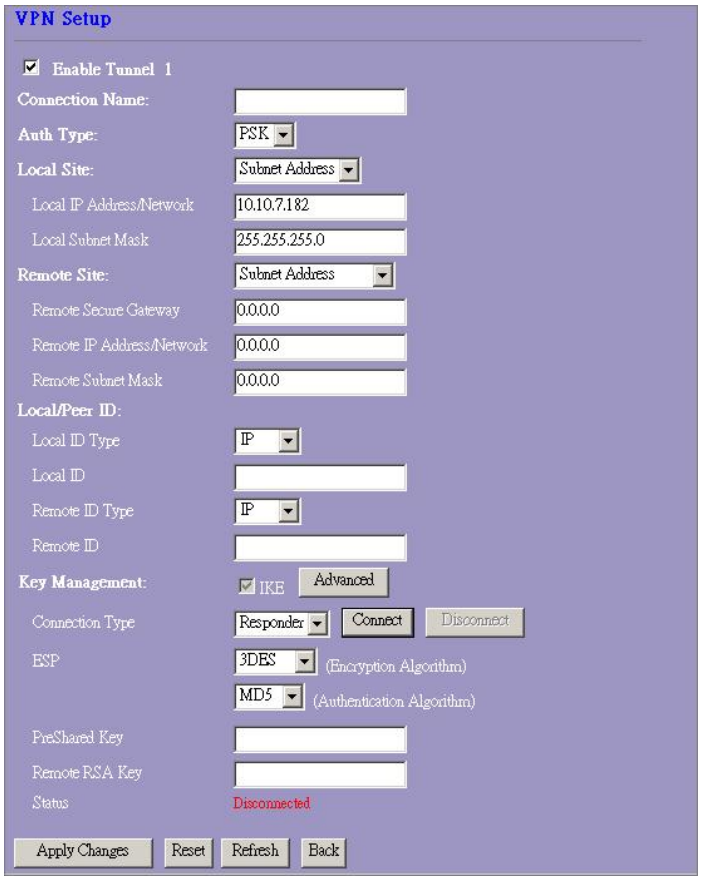
VPN Setting

VPN (Virtual Private Network) construct a virtual tunnel to a remote network, which prevents the connection from peeping and inspection. The data is encrypted with the encryption algorithm that you specified. To start configuring VPN, please mark the **"Enable IPSPEC VPN"** check box before any configuration.



Enable IPSEC VPN	Mark this check box to enable VPN function of the device.
Enable NAT Traversal	Click this check box to perform NAT traversal.
Generate\ Show RSA Key	Click the two buttons to generate a RSA key and show the RSA key that you generate. The RSA key is an encryption type for securing your VPN.
Current VPN table	The established VPN tunnels list.
Edit, Delete and Refresh	You may select on one VPN connection and click the "Edit" button to configure it or click "Delete" to remove it. The "Refresh" button reload

VPN parameters configuration



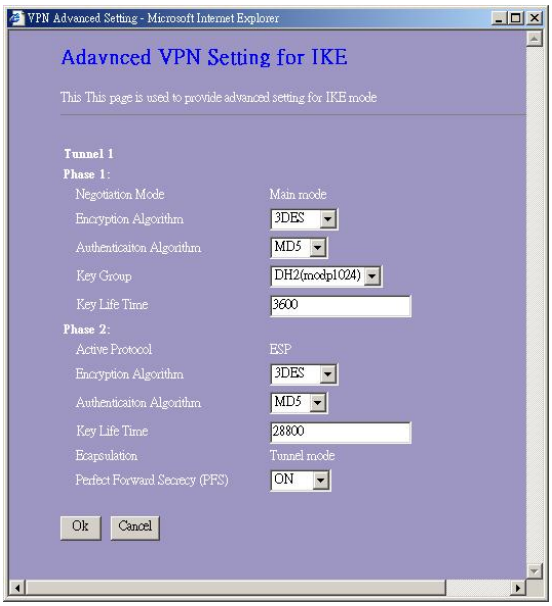
After clicking the “Edit” button, you may configure this VPN tunnel.

Enable Tunnel 1	Mark this checkbox to enable this VPN tunnel and clear it to uncheck it.
Connection Name	Specify a name for this connection.
Auth Type	Select an authentication method for this VPN form the drop list.
Local Site	Specify the local network information.
Remote Site	Specify the remote network information.
Local /Peer ID	Select an information type for identification.

Key Management	**IKE:** Mark this check box to enable IKE. IKE (Internet Key Exchange) is a key exchange and authentication protocol used by IPsec. You may also click the **"Advanced"** button to do more advanced configuration for IKE. **Connection Type:** Select a connection to be a initiator in this VPN or a responder. **ESP:** Select the encryption and authentication algorithm form the drop list. **Pre-Shared Key:** Specify a pre-shared key for this VPN after selecting "PSK" in the "Auth Type" drop list. **Remote RSA Key:** Specify a RSA key for this VPN after selecting "RSA" in the "Auth Type" drop list. **Status:** Shows if this tunnel is connected or disconnected.

Advanced VPN Setting for IKE

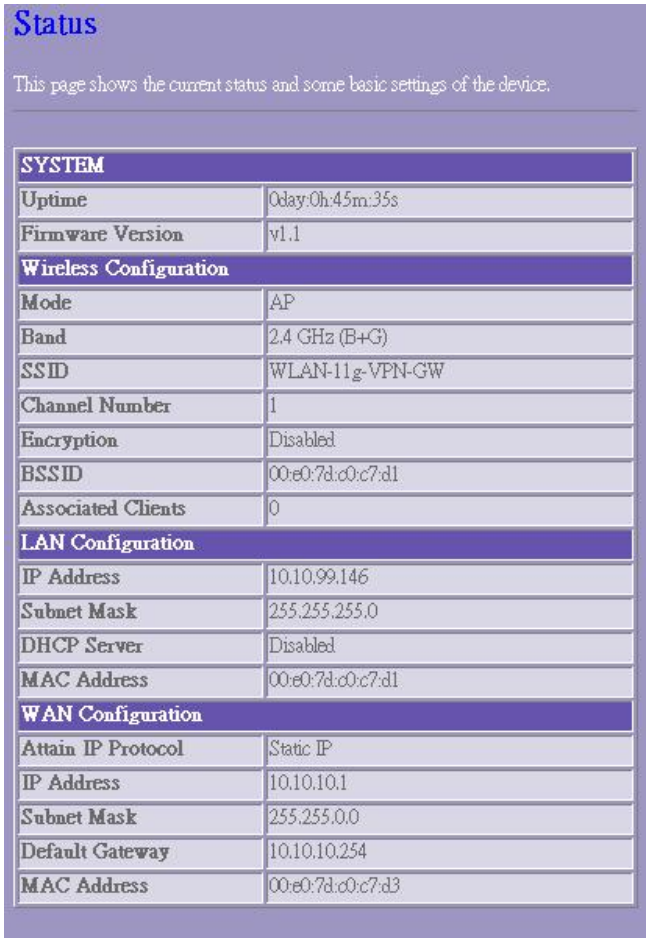
This window allows users to configure advanced VPN settings for IKE. Please select encryption algorithm, authentication algorithm and key group from the drop list. Specify a key refreshing time.



Management

Status

In the home page of the Wireless Router, the left navigation bar shows the options to configure the system. In the right navigation screen is the summary of system status for viewing the configurations.



Status

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

SYSTEM	
Uptime	0day:0h:45m:35s
Firmware Version	v1.1
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	WLAN-11g-VPN-GW
Channel Number	1
Encryption	Disabled
BSSID	00:e0:7d:c0:c7:d1
Associated Clients	0
LAN Configuration	
IP Address	10.10.99.146
Subnet Mask	255.255.255.0
DHCP Server	Disabled
MAC Address	00:e0:7d:c0:c7:d1
WAN Configuration	
Attain IP Protocol	Static IP
IP Address	10.10.10.1
Subnet Mask	255.255.0.0
Default Gateway	10.10.10.254
MAC Address	00:e0:7d:c0:c7:d3

- *System*

Uptime	The period that you power the device on.
Firmware Version	The version of the firmware applied on this device.

- Wireless Configuration

Mode	The operation mode of the wireless router
Band	The performing band of this wireless router
SSID	The name of this wireless network
Channel Number	The channel used by the wireless LAN. All devices in the same wireless LAN should user the same channel
Encryption	The security encryption status of this wireless network
BSSID	The Basic Service Set Identity of this router.(This parameter is the same as the MAC address of LAN port)
Associated Clients	The number of associated clients.

- LAN Configuration

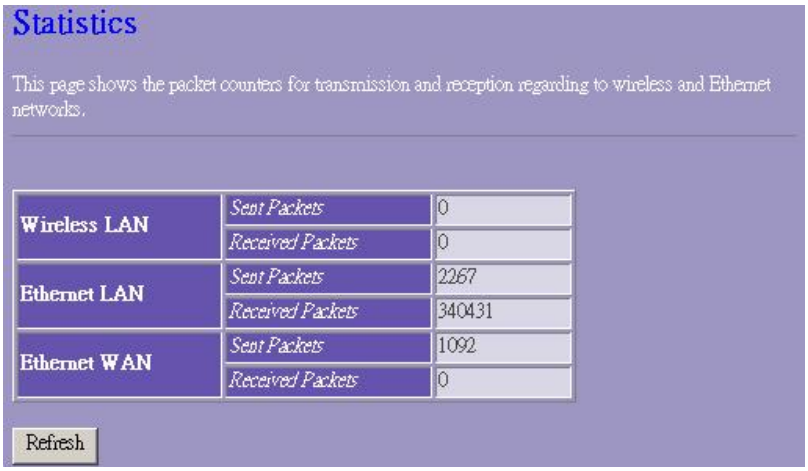
IP Address	IP Address of router
Subnet Mask	Subnet Mask of the router
DHCP Server	Enabled or Disable of DHCP
MAC Address	MAC Address of LAN-port

- WAN Configuration

Attain IP Protocol	Static IP address
IP Address	IP address of WAN-port
Subnet Mask	Subnet Mask of WAN-port
Default Gateway	Default Gateway of WAN-port
MAC Address	MAC Address of WAN-port

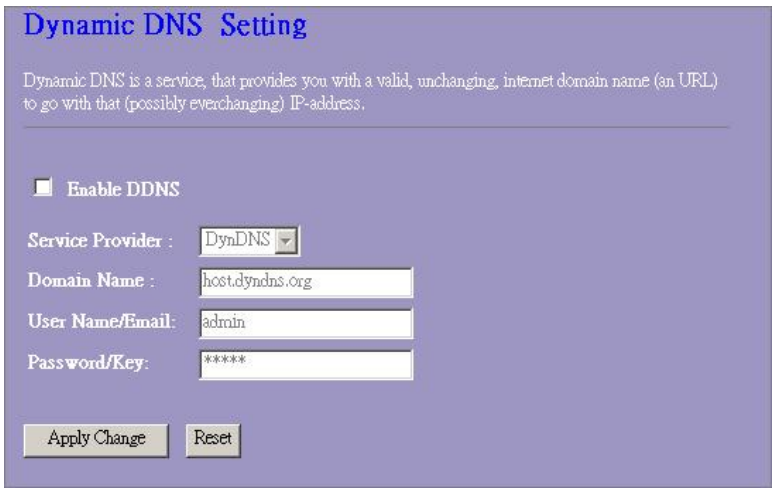
Statistics

On this page, you can monitor the sent & received packets counters of wireless, Ethernet LAN, and Ethernet WAN. To see the latest report, click refresh button.



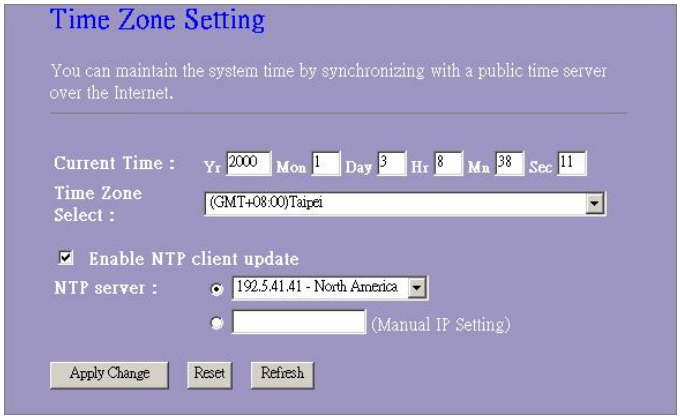
DDNS

This page allows users to connect to DDNS. To enable DDNS, Mark the "Enable DDNS" checkbox. Select the service provider from the drop list. Fill in domain name, username, and password. Click the "Apply Change" button after configuration.



Time Zone Setting

This page allows users to configure the time of the router. To specify manually, fill in the blanks in “Current Time” and click the “Apply Change” button. To synchronize time from a timeserver, please mark the “Enable NTP client update” checkbox, select a NTP server from the drop list or manually enter a NTP server. Click the “Apply Change” button after your configuration.

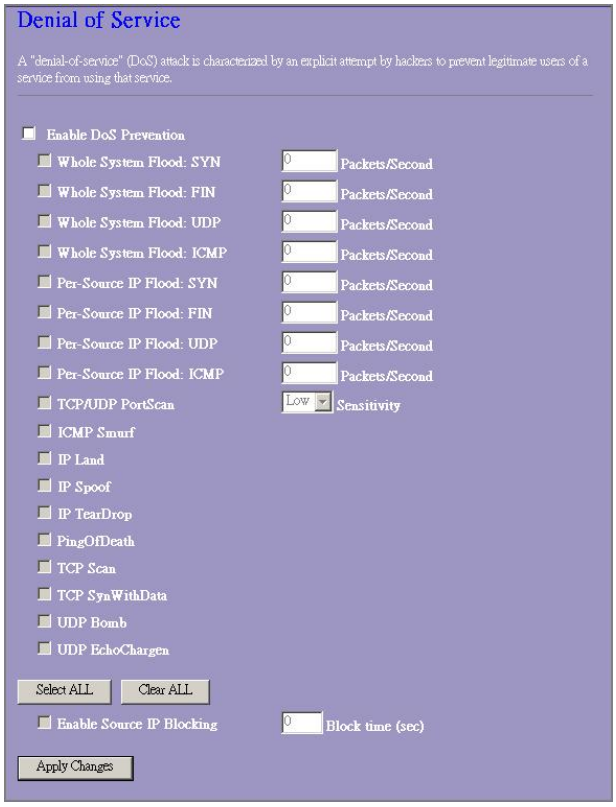


Denial of Service

Denial of Service(DoS) allows users to prevent certain packets from accessing this router. This helps to improve the security and against the assault from hackers.

To perform Denial of Service:

1. Mark the **"Enable DoS prevention"** checkbox.
2. Some packets allow users to specify a packet flow limit. Please fill in an allowed packet amount per second in those blanks first.
3. Select those packet types that you are going to block by marking the check boxes. You may also click the **"Select All"** button to select all packet types or click **" Clear All**" button to remove all selected packets.
4. Click the **"Apply Changes"** button to execute.



System Log

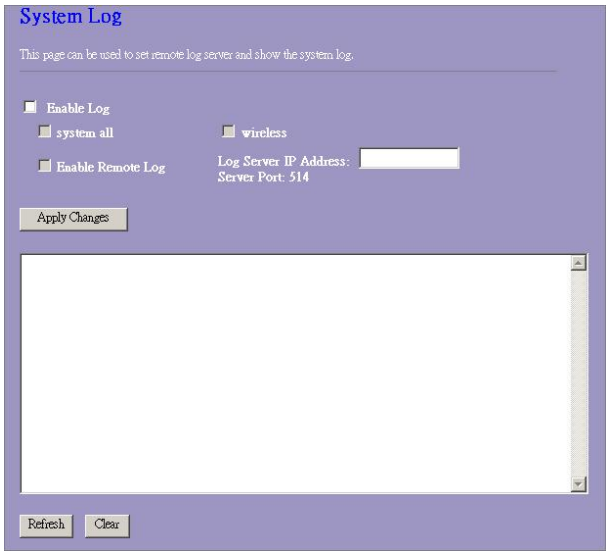
This System Log page shows the information of the current activities on the router.

To enable system log function:

1. Mark the “Enable Log” checkbox.
2. To see all information of the system, select the “system all” checkbox.
3. To see wireless information only, select the “wireless” checkbox.

   To sent the log information to a certain note, select the “Enable Remote Log” checkbox and fill in the IP address in the “Log Server IP Address” box.
4. Click the “Apply Changes” button to activate

You could also click the “Refresh” button to refresh the log information or click the “clear” button to clean the log table.



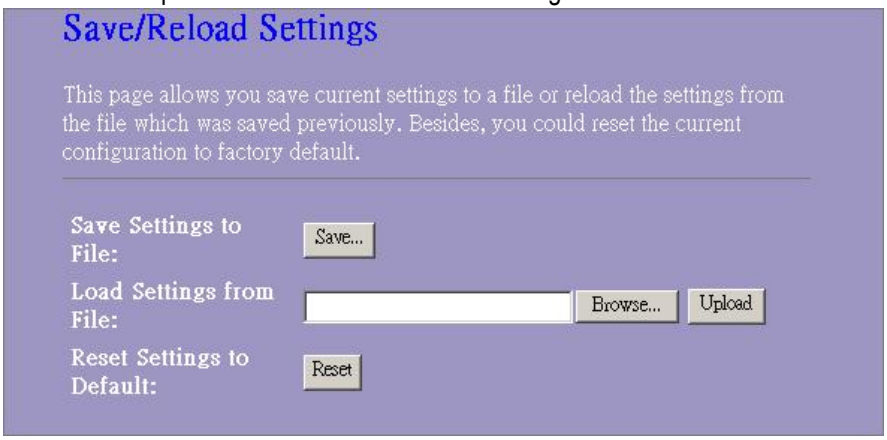
Upgrade Firmware

To Upgrade Firmware,

STEPS	1.	Click “browse…” button to select the firmware you want to upgrade.
	2.	Click Upload to start the upgrade process. Please don’t close the WEB-browser and wait for process to complete. When Upgrade is completed, you can start to use the router.

Save and Reload Settings

To save setting to file, click “Save...” button.
To load setting from file,
1. Click “Browse…” on the to select the file
2. Click upload to start the process and wait for it to complete
To reset setting to Default, click reset to start the process and it will be completed till the status LED start blinking.



Password

To set up the Administrator Account information, enter the Username, New password, and reenter the password on the text box. Don’t forget to click the “Apply Changes” to save the configuration.

Product Specifications

Standard	IEEE802.3, 10BASE-T IEEE802.3u, 100BASE-TX IEEE802.3x full duplex operation and flow control IEEE802.11b wireless LAN infrastructure IEEE802.11g wireless LAN infrastructure
Interface	1 * WAN port 4 * 10/100 RJ-45 Fast Ethernet switching ports Antenna: 802.11b/g wireless reverse SMA detachable
WAN Connection	Ethernet 10/100 Mbps
Cable Connections	RJ-45 (10BASE-T): Category 3,4,5 UTP RJ-45 (100BASE-TX): Category 5 UTP
Network Data Rate	802.11b: 1, 2, 5.5 and 11Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps
Transmission Mode	Auto-Negotiation (Full-duplex, Half-duplex)
LED indications	System: Power, Status Port (WAN): ACT/LINK Port (LAN): ACT/LINK Port(Wireless): ACT
Security	64/128-bit WEP, WPA(TKIP with IEEE 802.1x), WPA2, AES
Receiver Sensitivity	54Mbps OFDM, 10%PER, -71dBm 11Mbps CCK, 10%PER, -81dBm 1Mbps BPSK, 10%PER, -92dBm
Memory	Flash : 2MB NOR type, SDRAM : 16MB
Transmit Power	16dBm~18dBm
Range Coverage	Indoor 35~100 meters Outdoor 100~300meters.
Emission	FCC CLASS B, CE, VCCI Class B
Operating Temperature	0^0 ~ 40^0C (32^0 ~ 104^0F)
Operating Humidity	10% - 90%
Power Supply	External Power Adapter, 12VDC/ 1A