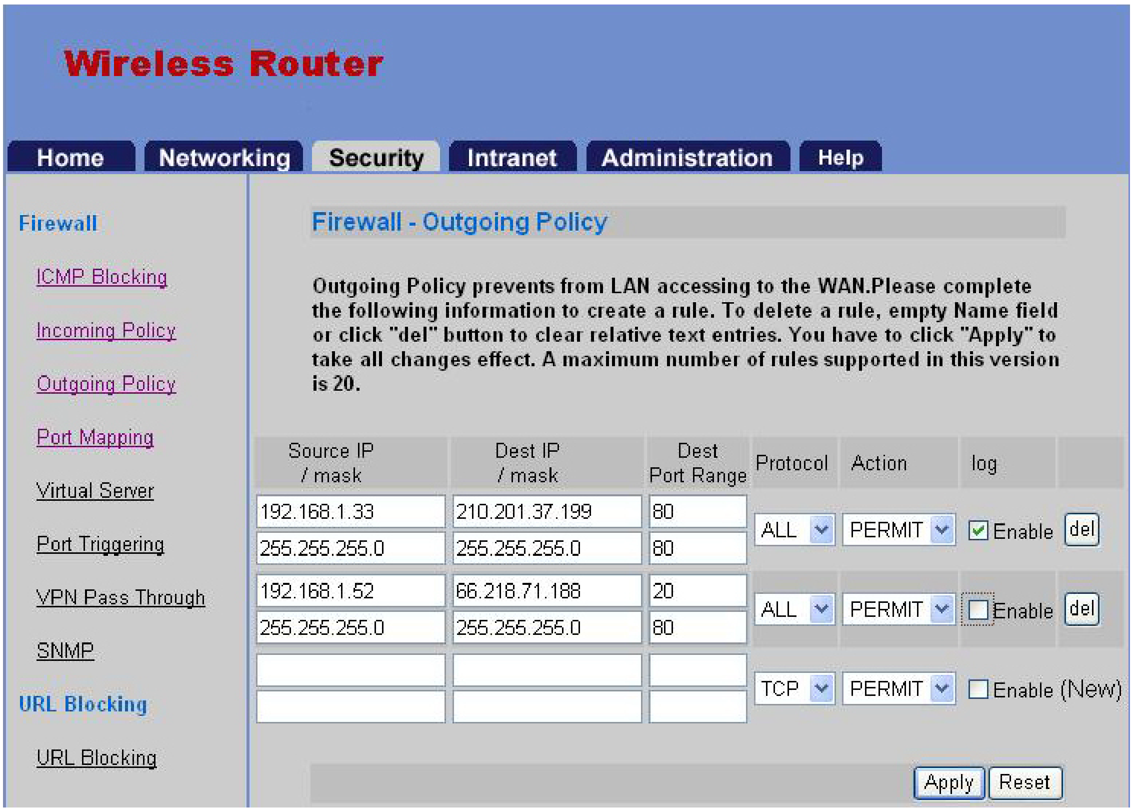
5.3.4. Blocking Individual (or Service Port) of LAN Clients from Accessing the Internet

1. Click on the Security tab.
2. Under the Firewall menu item, click on Outgoing Policy.
3. Enter the IP address and port number (or range) to be blocked onto the corresponding text box at the bottom of the list (marked New) according the following figure.
4. Click combo box and select protocol.
5. Click combo box and select PERMIT / DENY action.
6. Check Enable box to log the event.
7. Press Apply.



Firewall - Outgoing Policy

Outgoing Policy prevents from LAN accessing to the WAN.Please complete the following information to create a rule. To delete a rule, empty Name field or click "del" button to clear relative text entries. You have to click "Apply" to take all changes effect. A maximum number of rules supported in this version is 20.

Source IP / mask	Dest IP / mask	Dest Port Range	Protocol	Action	log	
192.168.1.33 255.255.255.0	210.201.37.199 255.255.255.0	80 80	ALL	PERMIT	☑ Enable	del
192.168.1.52 255.255.255.0	66.218.71.188 255.255.255.0	20 80	ALL	PERMIT	□ Enable	del
			TCP	PERMIT	□ Enable (New)	

This figure describes all the IP address coming from LAN port will be denied to access WAN services, but: Accessing to the port 80 (HTTP service) of WAN IP 210.201.37.199 from LAN IP 192.168.1.33(with port 80) will be allowed.

Accessing to the port 20~80 of WAN IP 66.218.71.198 from LAN IP 192.168.1.52 (with port 20~80) will be allowed.

Letting Stuff in

By default, IEEE 802.11g WLAN Router is deployed in firewall mode and will not allow outside computers to reach the LAN unless the connection is initiated by a LAN client. IEEE 802.11g WLAN Router empowers network administrators to allow WAN clients to access certain services provided by LAN clients. In other words, it is possible for WAN side computers to initiate connections provided the Network Administrator allows it. This is done through a technique called Port Mapping. When computers on the Internet communicate, they do so through IP addresses and special numbers called port addresses (or simply ports). The port determines which service is trying to connect to (e.g. port 80=HTTP/Web services).

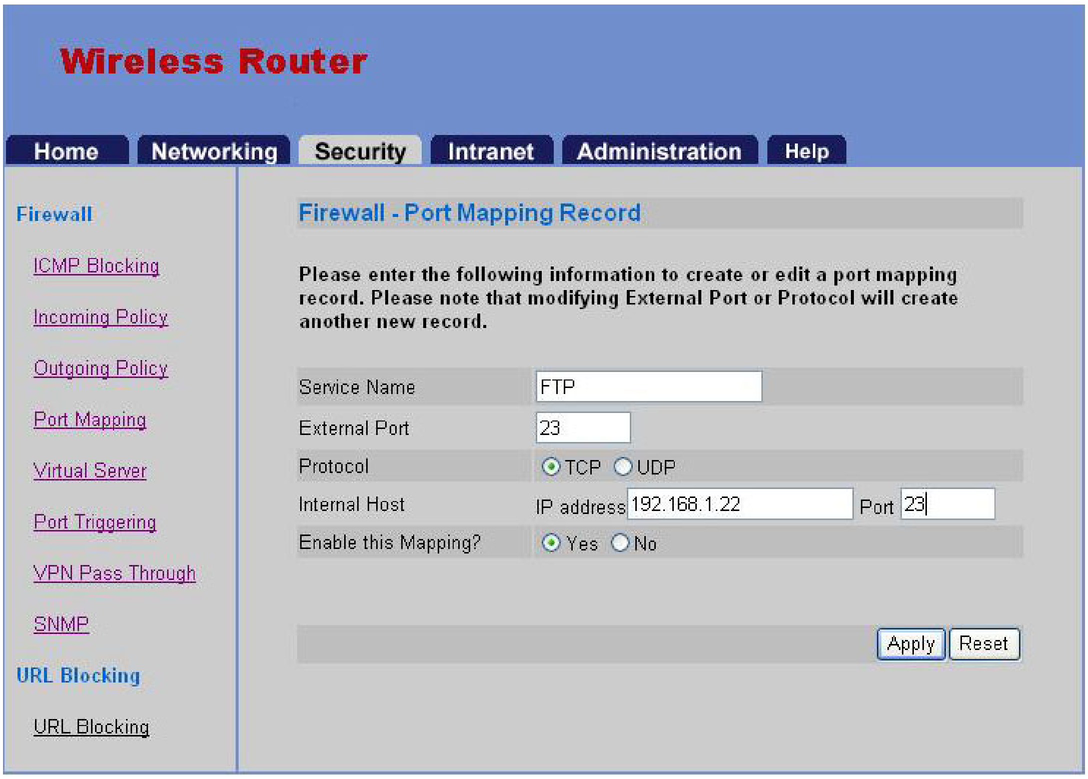
Each service also has what is known as a transmission protocol (either TCP or UDP). To properly use this feature, you would need the connection details for the service you wish to open to the Internet. Each WAN port/LAN IP/port group is called a rule. In addition, IEEE 802.11g WLAN Router rules can be further defined to allow or deny connections according to IP address using filters.

Port Mapping allows IEEE 802.11g WLAN Router to “pretend” to offer the service that an outside computer (WAN side) wishes to reach. Once the connection is made, all the requests between the outside and local (LAN side) computers are redirected by IEEE 802.11g WLAN Router to the proper destination. This process is completely transparent to the outside computers.

5.3.5. Mapping Internal Ports to the Outside

Add a record of Port Mapping

1. Click on Port Mapping under Firewall in the Security tab.
2. Click on Add.
3. Enter Service Name (ex: FTP), External Port (ex: 23).
4. Click on TCP.
5. Enter the last digit of IP address into Internal Host (ex: 192.168.1.22), port (ex:23).
6. Click on Enable.
7. Press Apply.



Firewall - Port Mapping Record

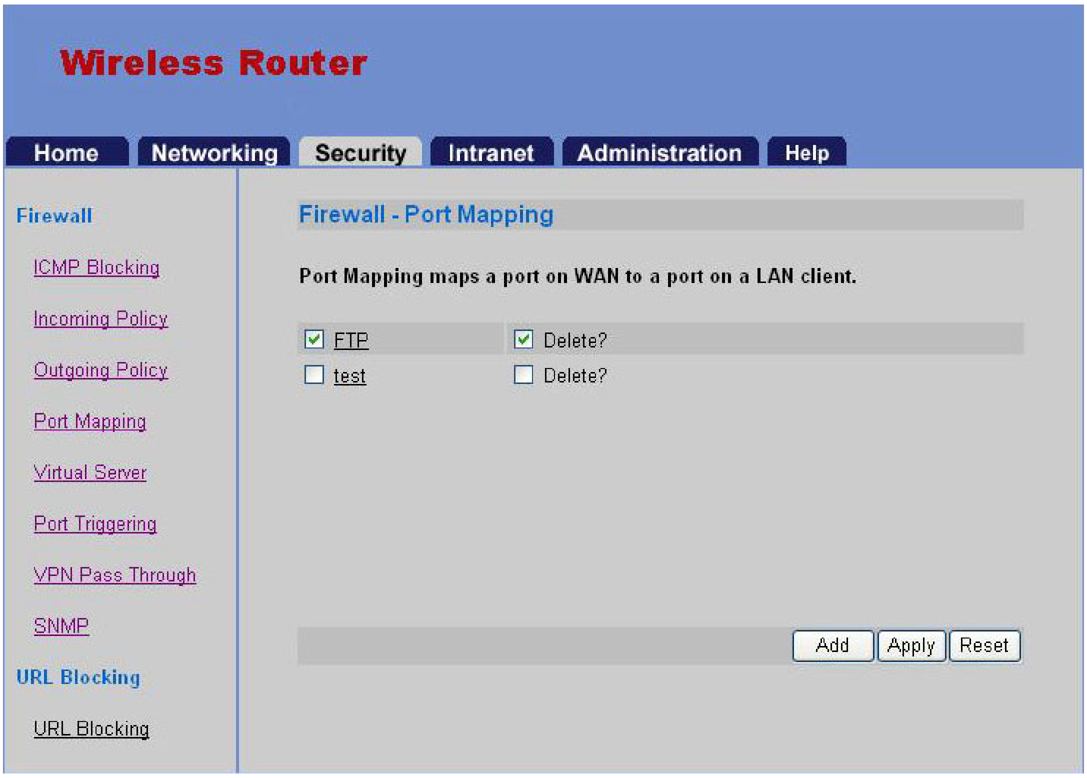
Please enter the following information to create or edit a port mapping record. Please note that modifying External Port or Protocol will create another new record.

Service Name	FTP
External Port	23
Protocol	● TCP ○ UDP
Internal Host	IP address 192.168.1.22 Port 23
Enable this Mapping?	● Yes ○ No

Any request from Internet for port 21 (FTP service port) to the IEEE 802.11g WLAN Router will be forwarded to LAN client 192.168.1.22

Deleting a record of Port Mapping

1. Click on Port Mapping under Firewall in the Security tab.
2. Click on Delete? beside record you want to delete and press Apply.



Firewall - Port Mapping

Port Mapping maps a port on WAN to a port on a LAN client.

☑ FTP ☑ Delete?

□ test □ Delete?

Enable a record of Port Mapping

1. Click on Port Mapping under Firewall in the Security tab.
2. Click on some records of Port Mapping and press Apply.

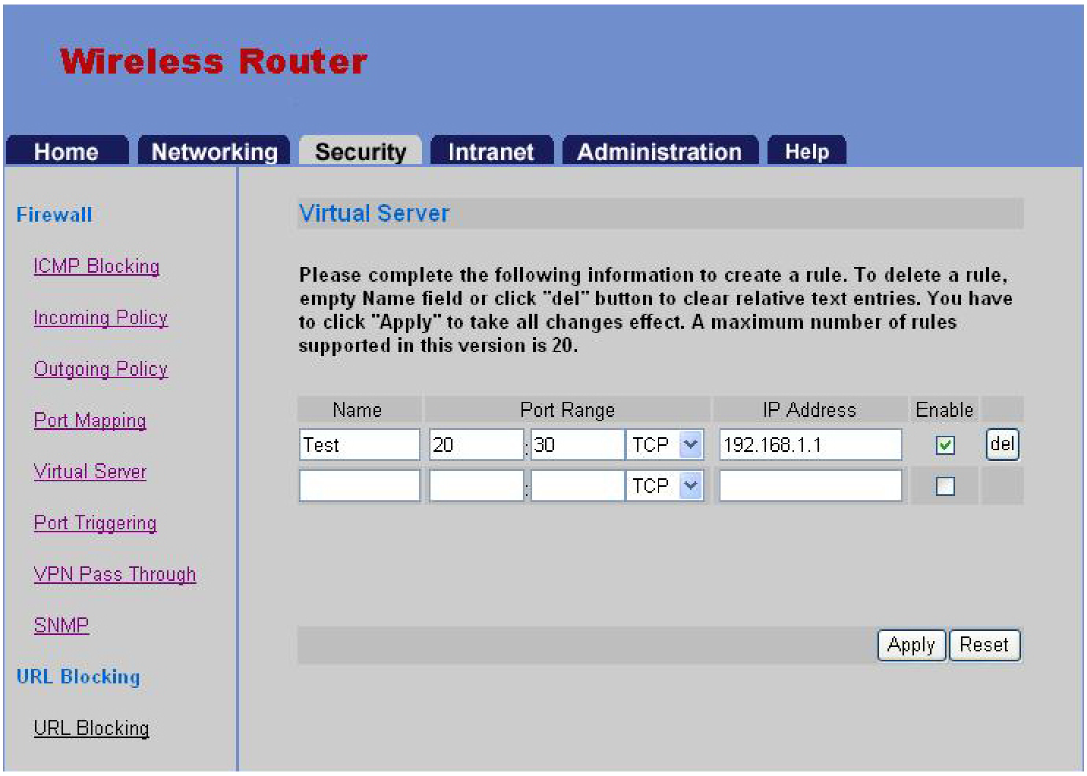
5.3.6. Configuring a Virtual Server

Adding a record to virtual server

1. Setup FTP server and Telnet Server in LAN port (ex: 192.168.1.1)
2. Click on Virtual Server under Firewall in the Security tab.
3. Enter Name (ex: Test)
4. Enter Port Range (ex: 20, 30).
5. Select TCP / UDP / ALL. (ex: TCP)
6. Enter IP address (ex: 192.168.1.1).
7. Click on Enable.
8. Press Apply.

Deleting a record from virtual server

1. Click on Virtual Server under Firewall in the Security tab.
2. Select the rule you want to delete
3. Press "del" button in the right of the rule
4. Press Apply.



Virtual Server

Please complete the following information to create a rule. To delete a rule, empty Name field or click "del" button to clear relative text entries. You have to click "Apply" to take all changes effect. A maximum number of rules supported in this version is 20.

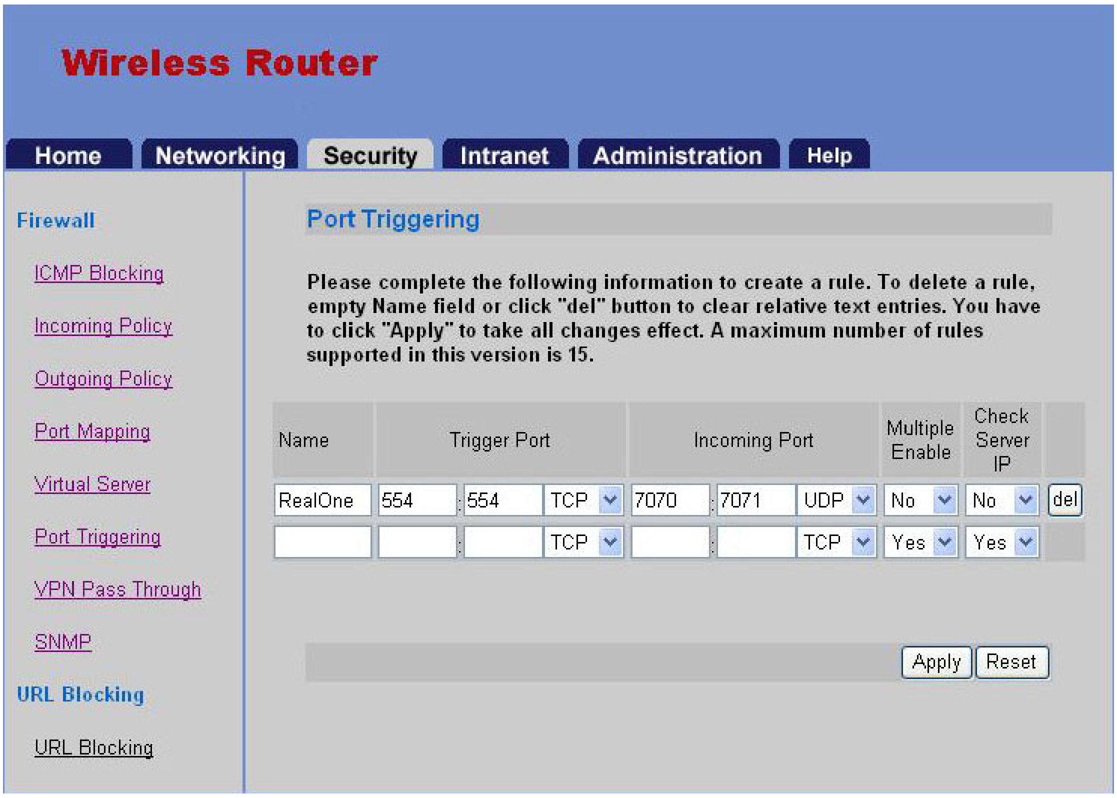
Name	Port Range			IP Address	Enable	
Test	20	30	TCP	192.168.1.1	☑	del
			TCP		□	

5.3.7. Port Triggering Configuration

Port trigger is a set of rules that are used to open ports in the firewall dynamically. Each rule is composed of a trigger condition and a port opening rule.

Add a Port Trigger rule for Realplayer

1. Click on Port trigger under Firewall in networking tab.
2. Add the following items in the port trigger page and press Apply.
3. Input the name. RealOne
4. Input the triggered port: 554-554
5. Select the triggered protocol: "TCP"
6. Input the opened port range: 7070-7071
7. Select the opened protocol: "UDP"
8. Select the server check: "No"



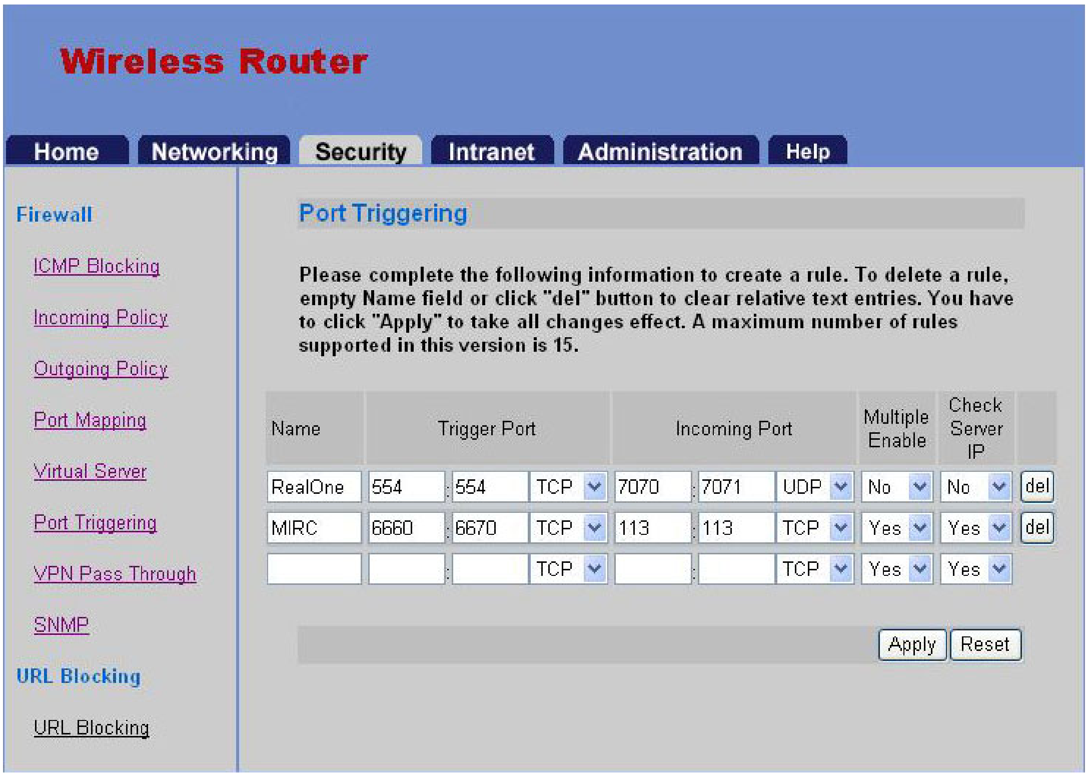
Port Triggering

Please complete the following information to create a rule. To delete a rule, empty Name field or click "del" button to clear relative text entries. You have to click "Apply" to take all changes effect. A maximum number of rules supported in this version is 15.

Name	Trigger Port			Incoming Port			Multiple Enable	Check Server IP
RealOne	554	554	TCP	7070	7071	UDP	No	No
			TCP			TCP	Yes	Yes

Add a Port Trigger rule for mIRC

1. Click on Port trigger under Firewall in Networking tab.
2. Add the following items in the port trigger page and press Apply.
3. Input the name. MIRC
4. Input the triggered port range: 6660:6670
5. Select the triggered protocol: "TCP"
6. Input the opened port range: 113-113
7. Select the opened protocol: "TCP"
8. Select the server check: "No"



Port Triggering

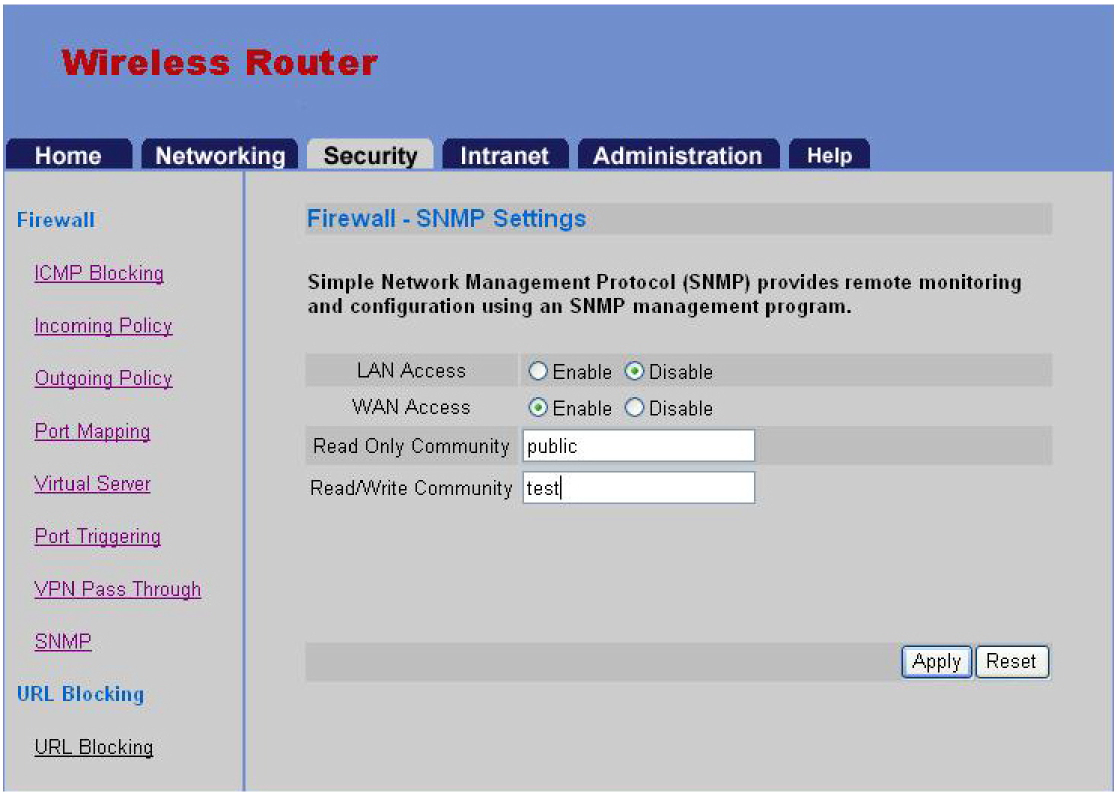
Please complete the following information to create a rule. To delete a rule, empty Name field or click "del" button to clear relative text entries. You have to click "Apply" to take all changes effect. A maximum number of rules supported in this version is 15.

Name	Trigger Port			Incoming Port			Multiple Enable	Check Server IP	
RealOne	554	554	TCP	7070	7071	UDP	No	No	del
MIRC	6660	6670	TCP	113	113	TCP	Yes	Yes	del
			TCP			TCP	Yes	Yes	

5.3.8. SNMP

IEEE 802.11g WLAN Router supports the Simple Network Management Protocol (SNMP). This protocol allows other SNMP aware systems to remotely monitor the behavior of your IEEE 802.11g WLAN Router. IEEE 802.11g WLAN Router complies with SNMP version 1 and version 2 type requests. SNMP compliant network management systems (NMS) can requests information from your IEEE 802.11g WLAN Router by providing the proper community strings.[1] Community strings act as passwords between SNMP aware devices (also called agents).

IEEE 802.11g WLAN Router distinguishes requests from the WAN and LAN sides. This allows the network administrator to prevent unwanted monitoring. By default, SNMP monitoring is allowed throughout the LAN, while disallowed through the WAN.



Firewall - SNMP Settings

Simple Network Management Protocol (SNMP) provides remote monitoring and configuration using an SNMP management program.

LAN Access ○ Enable ● Disable

WAN Access ● Enable ○ Disable

Read Only Community: public

Read/Write Community: test

Enable WAN Access

1. Click on SNMP under Firewall in the Security tab.
2. Click on Enable in the WAN Access item.
3. Modify Read Only Community, Read Write Community.
4. Press Apply.

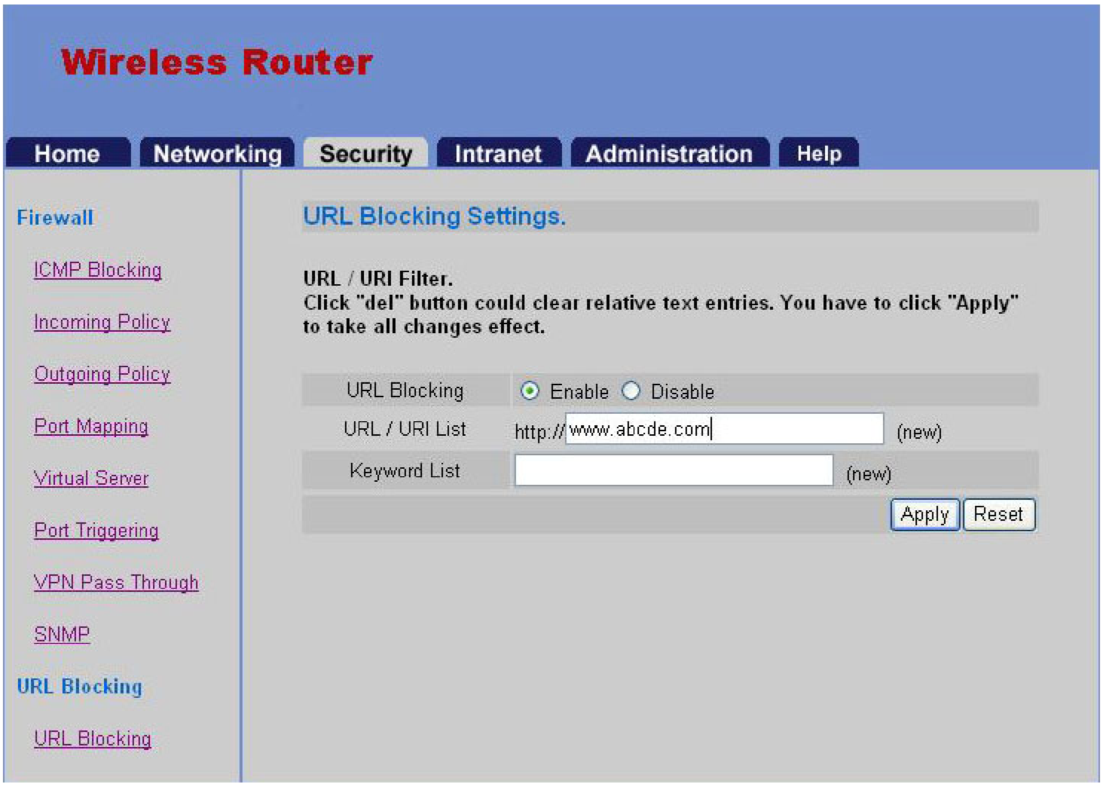
Enable LAN Access

1. Click on SNMP under Firewall in the Security tab.
2. Click on Enable in the LAN Access item.
3. Modify Read Only Community and Read Write Community.
4. Press Apply.

[1] Commnuity strings are the primary authentication mechanisms employed by SNMP V1 and SNMP V2. Read-Only SNMP support is available on all models. Read-Write SNMP support is available only on select models.

5.3.9. URL Blocking

Uniform Resource Locator (URL) blocking can be used by parents to limit access to certain Internet sites for their children. This feature is more effective than Internet IP Blocking as Internet sites might have multiple IP addresses and the user does not required to know the IP address to set a blocking rule. In addition, the user can set a keyword list that would block any URL that comprises the keyword. This way, the user can make the list short, making it easier to manage.



URL Blocking Settings.

URL / URI Filter.
Click "del" button could clear relative text entries. You have to click "Apply" to take all changes effect.

URL Blocking	● Enable ○ Disable
URL / URI List	http:// www.abcde.com (new)
Keyword List	(new)

Add a record on URL Blocking

1. Click on URL Blocking under URL Blocking in the Security tab.
2. Click on Enable in the URL Blocking item.
3. Enter URL/URI List, Keyword List and press Apply.

Delete a record on URL Blocking

1. Click on URL Blocking under URL Blocking in the Security tab.
2. Click on Enable in the URL Blocking tab.
3. Click on del beside URL/URI List you want to delete.
4. Click on del beside Keyword List you want to delete.
5. Press Apply.

5.4. INTRANET

Local Area Network Computing Internet style

The technology developed for the Internet has revolutionized so many aspects of modern day society. Applications of the Internet technology within a corporate environment present the same benefits and synergy at a much more personal scale.

Dubbed Intranets, local area networks that leverage technology developed for the World Wide Web provide a wealth of resources to the office. Like its global counter-part intranets offer the user with fast, reliable on-line services. Unlike its global counter-parts, intranets that are run behind properly configured firewalls are safe from malicious or unintentional intrusions that cause serious interruptions or intellectual property loss or damage.

Dynamic LAN Client Configuration

LAN side client computers can automatically obtain new IP addresses from IEEE 802.11g WLAN Router, through its built-in DHCP daemon. To achieve this each client computer should be set to acquire IP addresses via dynamic host configuration protocol (DHCP) or its predecessor the Bootstrap Protocol (BootP).

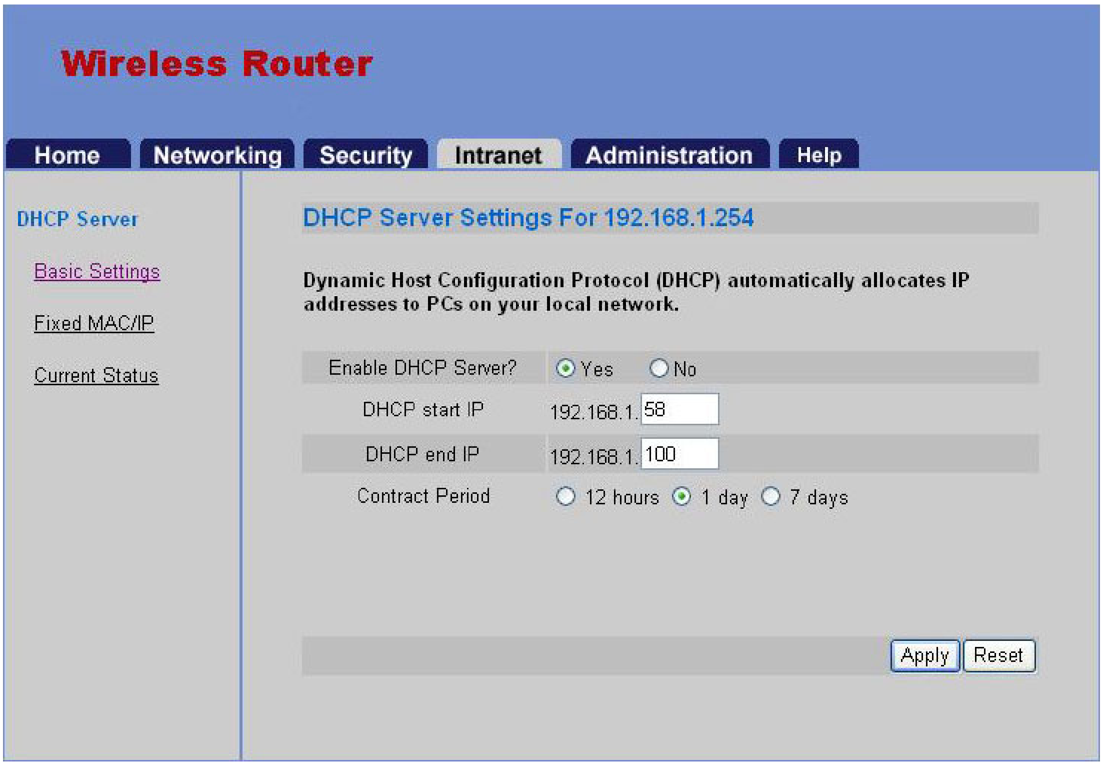
By default, IEEE 802.11g WLAN Router will assign up to 99 IP addresses within the range starting from 192.168.1.2 up to 192.168.1.100. Once assigned, a client computer would retain or lease the IP address for as long as 1 day (7 day max). Once the lease expires, the client computer can re-apply for a new IP address. It is possible that the DHCP daemon may assign a different IP address from what was just released. In order to guarantee that a LAN side computer gets the same IP address every time, see the section on permanent IP address assignment below.

Caution: There should be only one (1) DHCP daemon on your LAN. If you are already running another DHCP daemon or server, you should disable it before activating IEEE 802.11g WLAN Router DHCP daemon. Running more than one DHCP daemon on a LAN can have unpredictable (and sometimes difficult to fix) consequences.

5.4.1. DHCP Server Basic Settings

SET UP DHCP SERVER

1. Click on Basic Settings under DHCPD in the Intranet tab.
2. Click on Yes in Enable DHCP?
3. Enter the last digit of DHCP start IP and DHCP end IP.
4. Click on one of Contract Period.
5. Press Apply.



DHCP Server Settings For 192.168.1.254

Dynamic Host Configuration Protocol (DHCP) automatically allocates IP addresses to PCs on your local network.

Enable DHCP Server?	● Yes ○ No
DHCP start IP	192.168.1. 58
DHCP end IP	192.168.1. 100
Contract Period	○ 12 hours ● 1 day ○ 7 days

MODIFY DHCP IP RANGE OF DHCP SERVER

1. Click on Basic Settings under DHCPD in the Intranet tab.
2. Modify DHCP start IP and DHCP end IP and press Apply. (IP value must be between 1 and 254)

MODIFY CONTRACT PERIOD OF DHCP IP

1. Click on Basic Settings under DHCPD in the Intranet tab.
2. Click on other options in the Contract Period item.

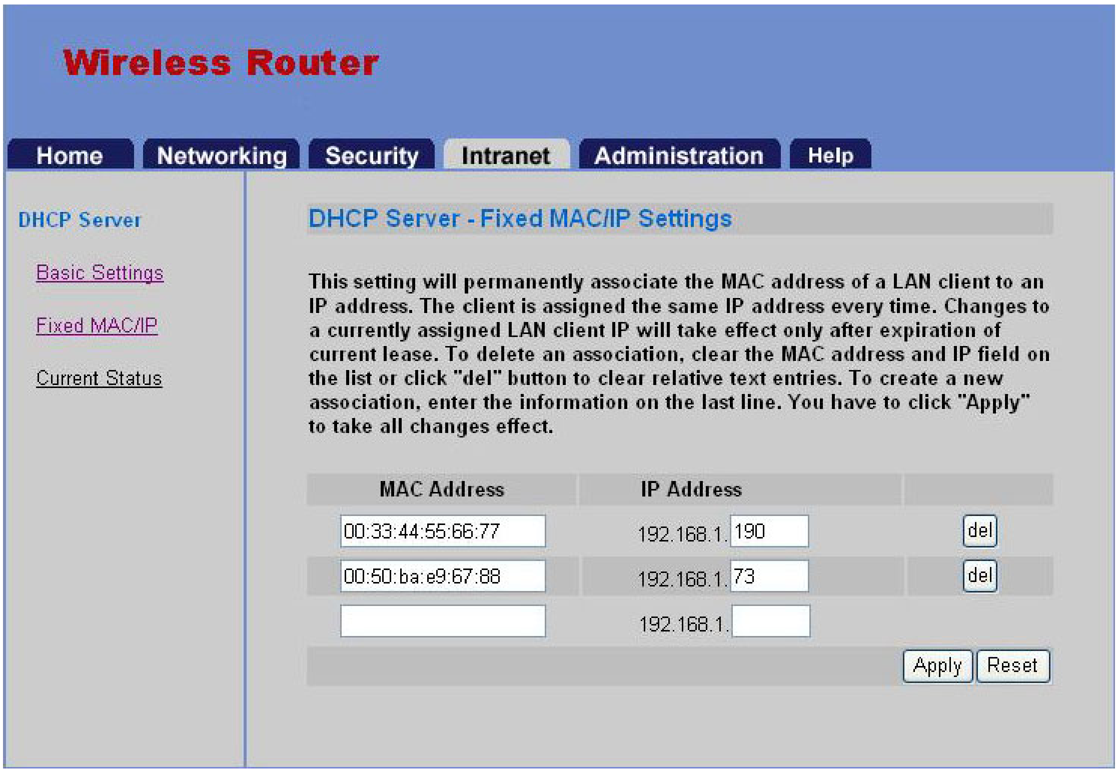
5.4.2. DHCPD Fixed MAC/IP

Adding a record of fixed MAC/IP

1. Click on Fixed MAC / IP under DHCPD in the Intranet tab.
2. Enter MAC Address, the last digit of IP address, and press Apply.

Deleting a record of fixed MAC / IP

1. Click on Fixed MAC / IP under DHCPD in the Intranet tab.
2. Click on del button beside record you want to delete.
3. Press Apply.



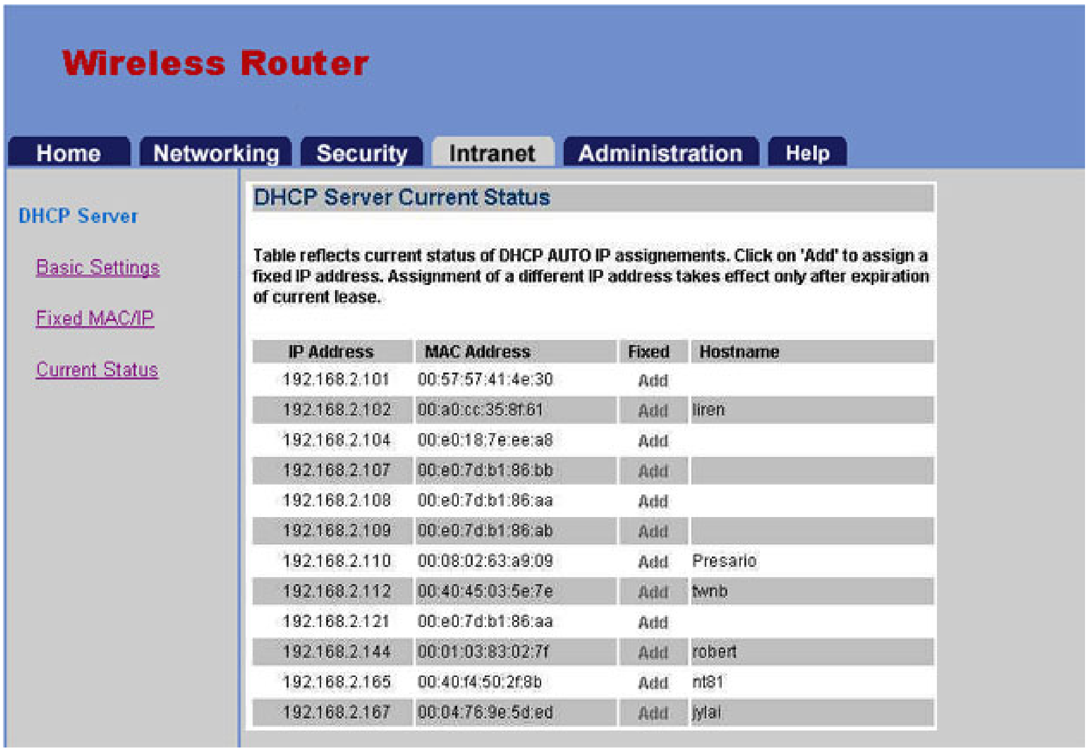
DHCP Server - Fixed MAC/IP Settings

This setting will permanently associate the MAC address of a LAN client to an IP address. The client is assigned the same IP address every time. Changes to a currently assigned LAN client IP will take effect only after expiration of current lease. To delete an association, clear the MAC address and IP field on the list or click "del" button to clear relative text entries. To create a new association, enter the information on the last line. You have to click "Apply" to take all changes effect.

MAC Address	IP Address	
00:33:44:55:66:77	192.168.1. 190	del
00:50:ba:e9:67:88	192.168.1. 73	del
	192.168.1.	

5.4.3. DHCP Server Status

1. Click on Current Status under DHCPD in the Intranet tab.



DHCP Server Current Status

Table reflects current status of DHCP AUTO IP assignements. Click on 'Add' to assign a fixed IP address. Assignment of a different IP address takes effect only after expiration of current lease.

IP Address	MAC Address	Fixed	Hostname
192.168.2.101	00:57:57:41:4e:30	Add	
192.168.2.102	00:a0:cc:35:8f:61	Add	liren
192.168.2.104	00:e0:18:7e:ee:a8	Add	
192.168.2.107	00:e0:7d:b1:86:bb	Add	
192.168.2.108	00:e0:7d:b1:86:aa	Add	
192.168.2.109	00:e0:7d:b1:86:ab	Add	
192.168.2.110	00:08:02:63:a9:09	Add	Presario
192.168.2.112	00:40:45:03:5e:7e	Add	twnb
192.168.2.121	00:e0:7d:b1:86:aa	Add	
192.168.2.144	00:01:03:83:02:7f	Add	robert
192.168.2.165	00:40:f4:50:2f:8b	Add	nt81
192.168.2.167	00:04:76:9e:5d:ed	Add	jylai

5.5. ADMINISTRATION

Access Control and Troubleshooting tools

IEEE 802.11g WLAN Router provides an extensive set of system tools that equip the novice network administrator to do advanced network trouble shooting. IEEE 802.11g WLAN Router also provides sophisticated control structures which can restrict access to its configuration.

Authentication

By now you have familiarized yourself with username/password authentication mechanism used by IEEE 802.11g WLAN Router. This is an industry standard method for authenticating the identity of the user who intends to use the system. Only authorized users should be entrusted with the valid username and password.

This feature allows the network administrator to manage the users who can change the IEEE 802.11g WLAN Router configuration or use the tools for trouble shooting. Users are also authenticated through the LAN clients they access IEEE 802.11g WLAN Router through. Users who attempt to access IEEE 802.11g WLAN Router through restricted workstations are denied access.

Besides, you can also choose a language setting. IEEE 802.11g WLAN Router currently supports English and Chinese (Big 5).

System Tools

IEEE 802.11g WLAN Router provides the following tools which aid in administration of the network.

System Status. This utility displays the current system status. It displays the current Network Status Current Routing Table, and DHCP clients information. The feature shows read-only system status and it will not allow you to modify the information. It provides a method of inspecting the health of your system.

Time Setup. This utility will setup your system time. You can either setup your system time manually or use Network Time Server to synchronize your system clock over the network. Router Service Time. This utility allows user to access Internet based on a predefined time frame.

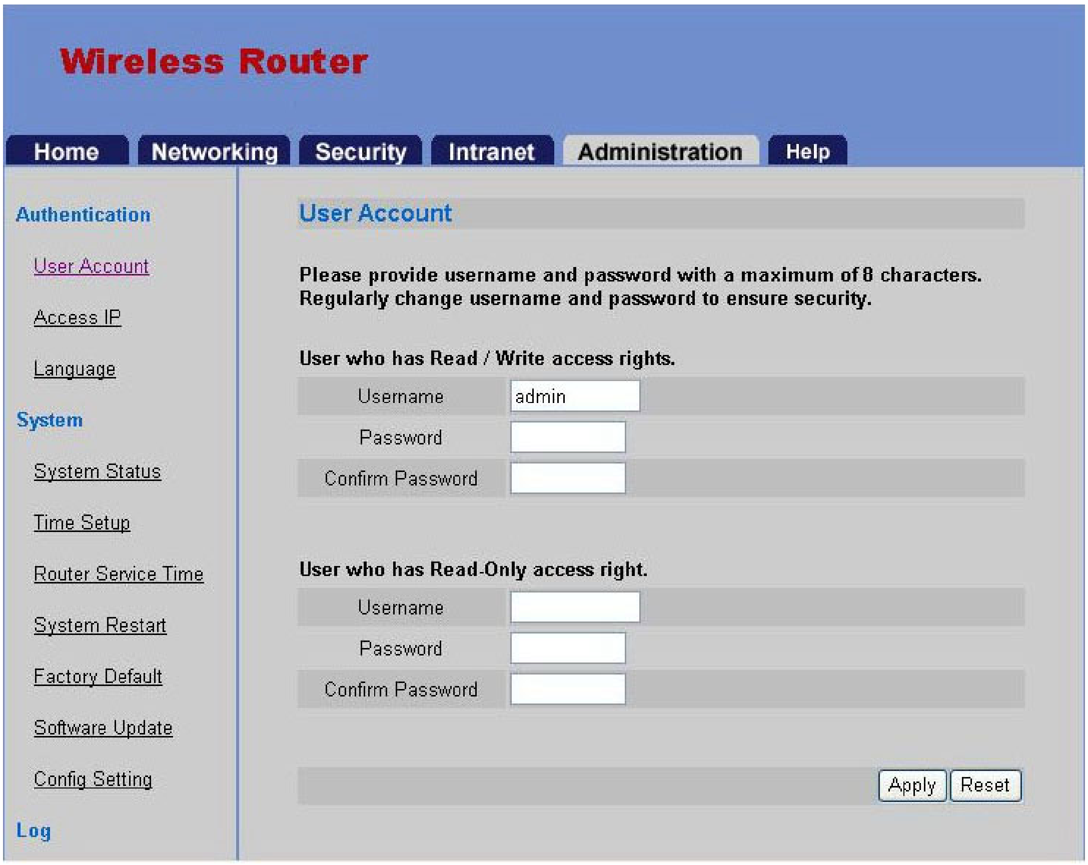
System Restart. This utility is used for restarting IEEE 802.11g WLAN Router. System restarts is needed in events of modified important system settings. Any saved changes of the system activities will be applied after the system rebooted.

Factory Default. This utility is used for clearing the configuration and resetting it back to original values (as it came out of the box)

Software Update. This utility allows the Network Administrator to connect to a server which provides software which can be used to upgrade IEEE 802.11g WLAN Router. The software update can also be done on local machine. Please check separate information sheet or vendor web site for more details.

Config Setting. This utility is used for backup your current IEEE 802.11g WLAN Router configurations in your PC. In the case you need to reset IEEE 802.11g WLAN Router back to factory default value, you can load the configuration you backup before.

5.5.1. User Account



User Account

Please provide username and password with a maximum of 8 characters.
Regularly change username and password to ensure security.

User who has Read / Write access rights.

Username	admin
Password	
Confirm Password	

User who has Read-Only access right.

Username	
Password	
Confirm Password	

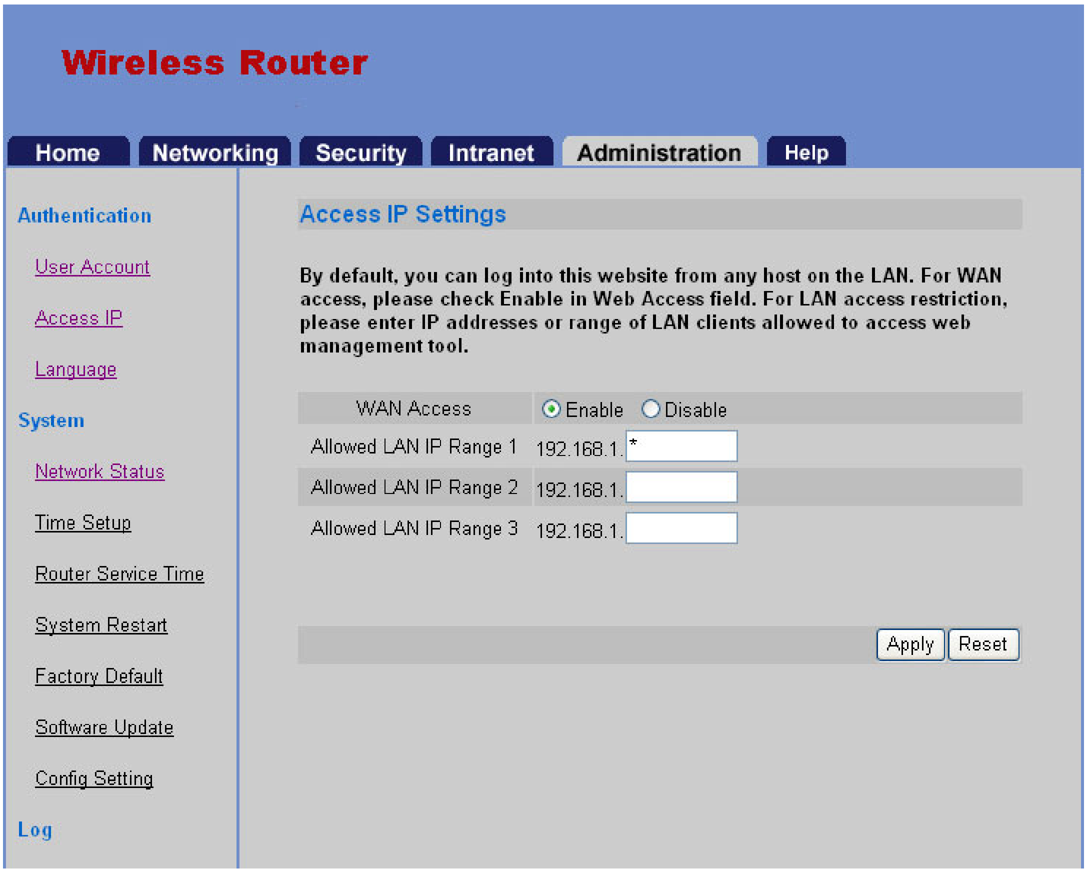
User who has Read / Write access right

1. Click on the Authentication tab and choose the User Account menu item.
2. Under the User who has Read/Write access right item, enter the user name in the Username text box.
3. Enter the password in the password text box.
4. Enter password again in the confirm password text box.

User who has Read-Only access right

1. Click on the Authentication tab. Choose the User Account menu item,
2. Under the User who has Read-Only access right item, enter the user name in the Username text box.
3. Enter the password in the password text box.
4. Enter password again in the confirm password text box.

5.5.2. Access IP



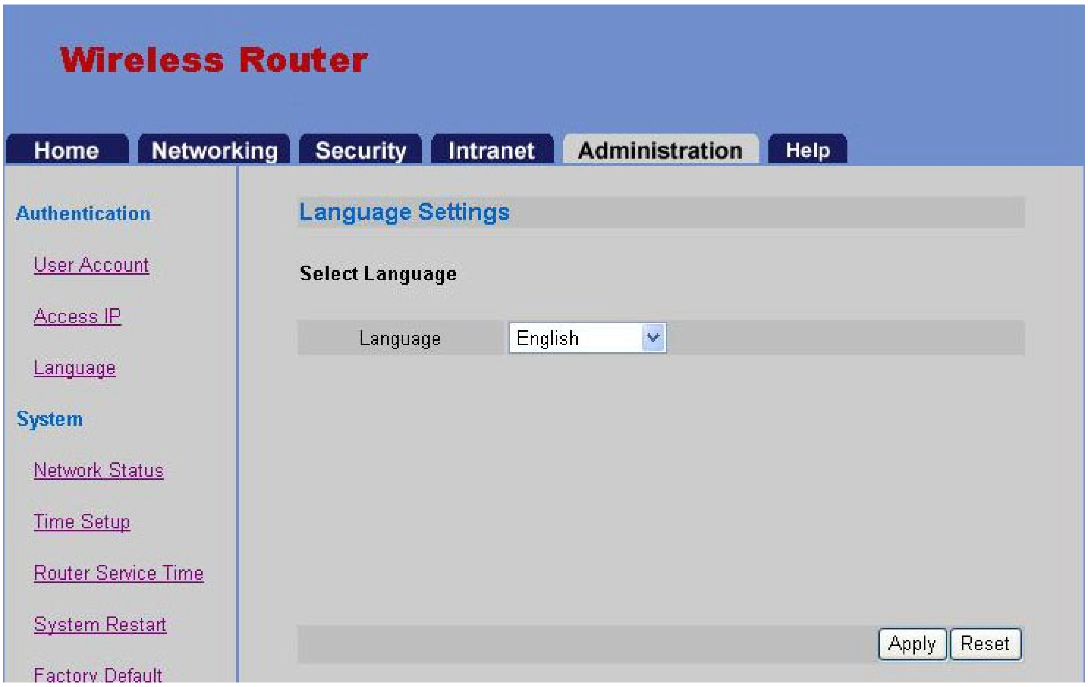
Access IP Settings

By default, you can log into this website from any host on the LAN. For WAN access, please check Enable in Web Access field. For LAN access restriction, please enter IP addresses or range of LAN clients allowed to access web management tool.

WAN Access	● Enable ○ Disable
Allowed LAN IP Range 1	192.168.1. *
Allowed LAN IP Range 2	192.168.1.
Allowed LAN IP Range 3	192.168.1.

1. Click on the Authentication tab. Choose the Access IP menu item.
2. Select Enable / Disable on WAN access.
3. Enter up to three sets of LAN IP address (or Ranges) into appropriate text box.
4. Click on Apply button.

5.5.3. Language



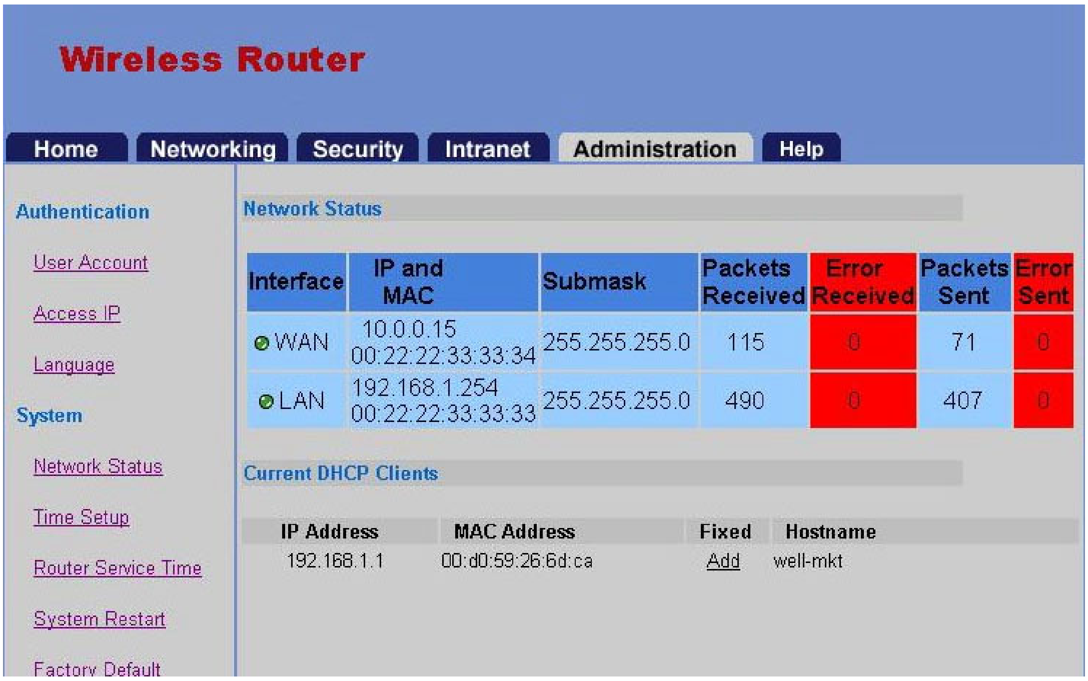
Language Settings

Select Language

Language English

1. Click on the Administration tab.
2. Under the Authentication menu item, click on Language.
3. Select your language in the Language box.
4. Clicks Apply to set your language.

5.5.4. System Status



Network Status

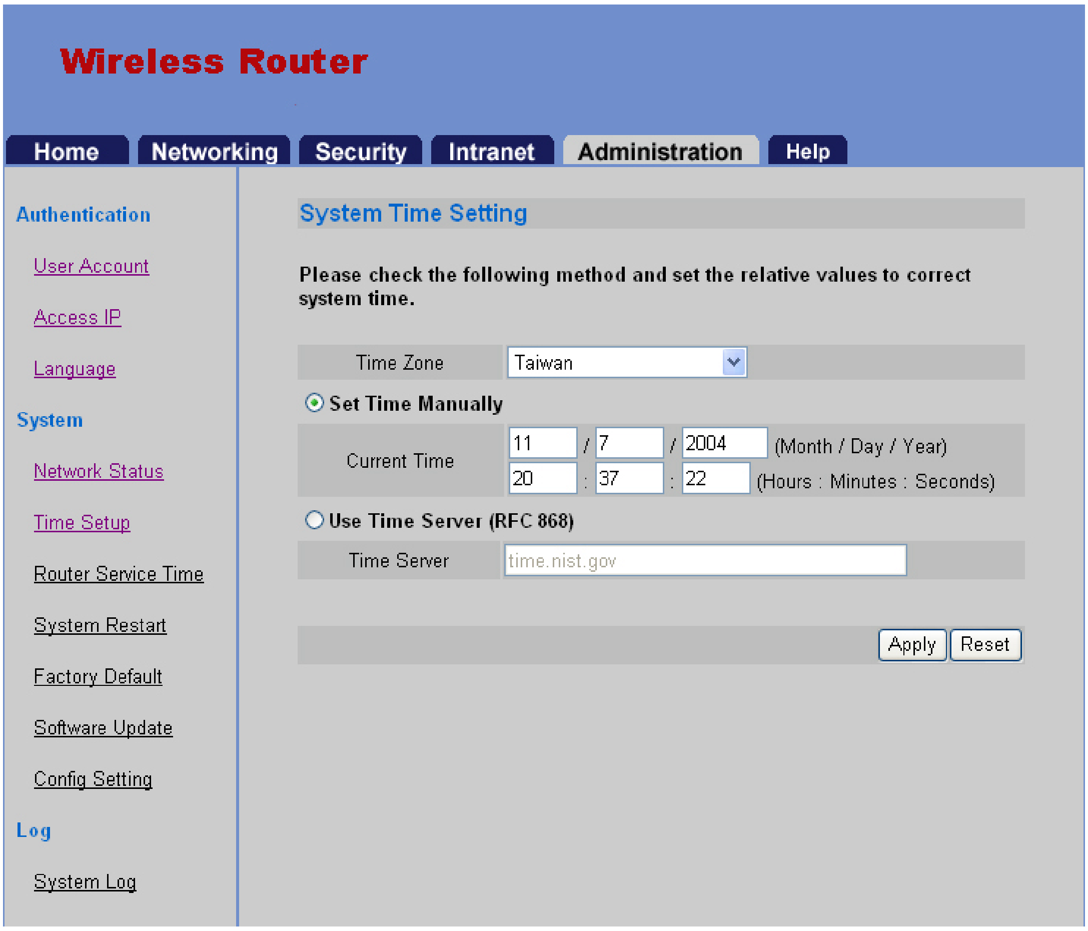
Interface	IP and MAC	Submask	Packets Received	Error Received	Packets Sent	Error Sent
● WAN	10.0.0.15 00:22:22:33:33:34	255.255.255.0	115	0	71	0
● LAN	192.168.1.254 00:22:22:33:33:33	255.255.255.0	490	0	407	0

Current DHCP Clients

IP Address	MAC Address	Fixed	Hostname
192.168.1.1	00:d0:59:26:6d:ca	Add	well-mkt

1. Click on the Administration tab.
2. Under the Authentication menu item, click on System status.

5.5.5. Time Setup



System Time Setting

Please check the following method and set the relative values to correct system time.

Time Zone: Taiwan

● Set Time Manually

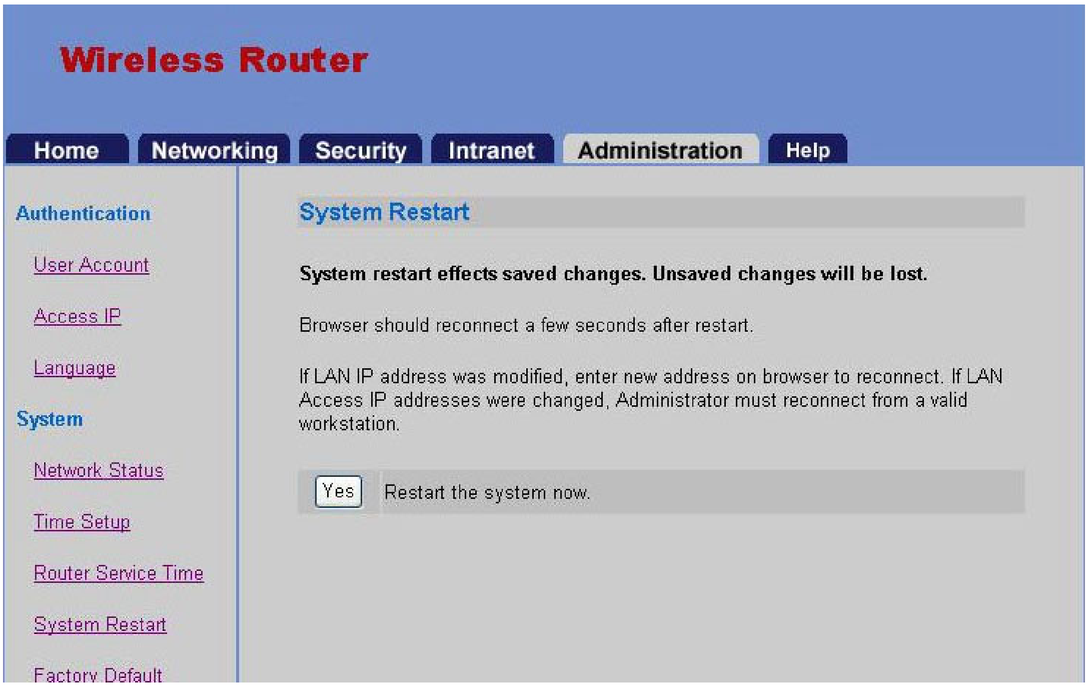
Current Time: 11 / 7 / 2004 (Month / Day / Year)
20 : 37 : 22 (Hours : Minutes : Seconds)

○ Use Time Server (RFC 868)

Time Server: time.nist.gov

1. Click on the Administration tab.
2. Under the System menu item, click on Time Setup.
3. Select your time zone in the Time Zone selection box.
4. Choose either Set Time Manually or Use Time Server.
5. If you choose the setup time manually, enter current time by specifying Month, Day, Hours, Minutes, and Seconds in the appropriate fields.
6. If you choose to use Time Server, specifying the Time server.
7. Click on Apply button to setup time.

5.5.6. System Restart



System Restart

System restart effects saved changes. Unsaved changes will be lost.

Browser should reconnect a few seconds after restart.

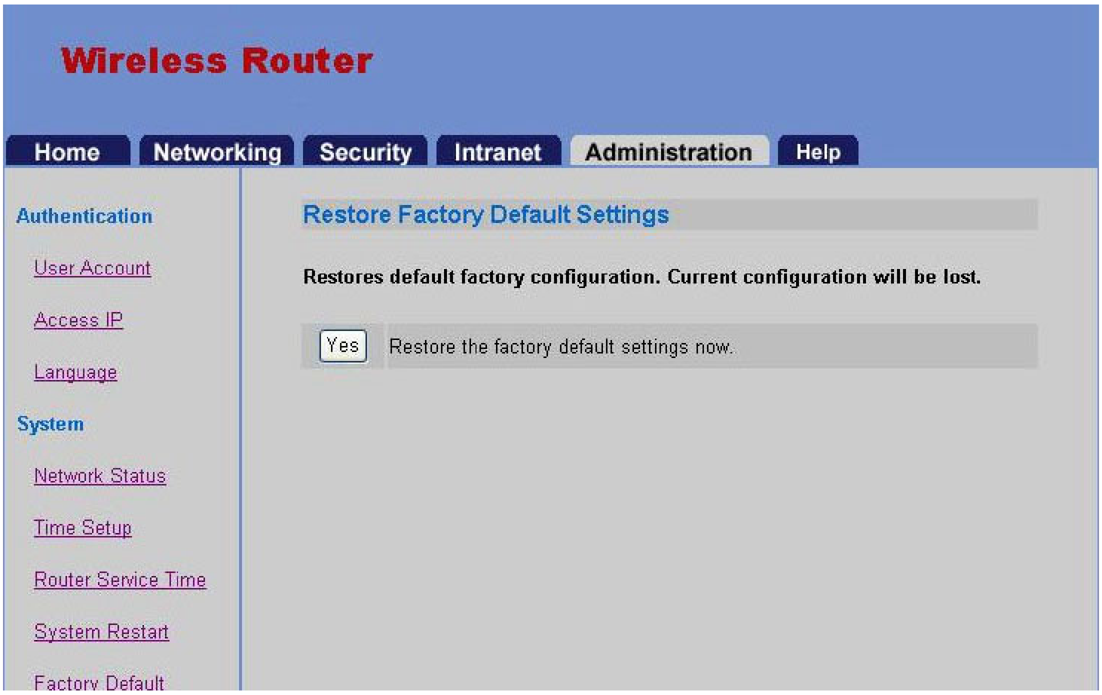
If LAN IP address was modified, enter new address on browser to reconnect. If LAN Access IP addresses were changed, Administrator must reconnect from a valid workstation.

Yes Restart the system now.

1. Click on the Administration tab.
2. Under the System menu item, click on System Restart.
3. Press Yes button to restart the system.

5.5.7. Factory Default

1. Click on the Administration tab.
2. Under the system menu item, click on Factory Default.
3. Press Yes button to restart the system with factory default.

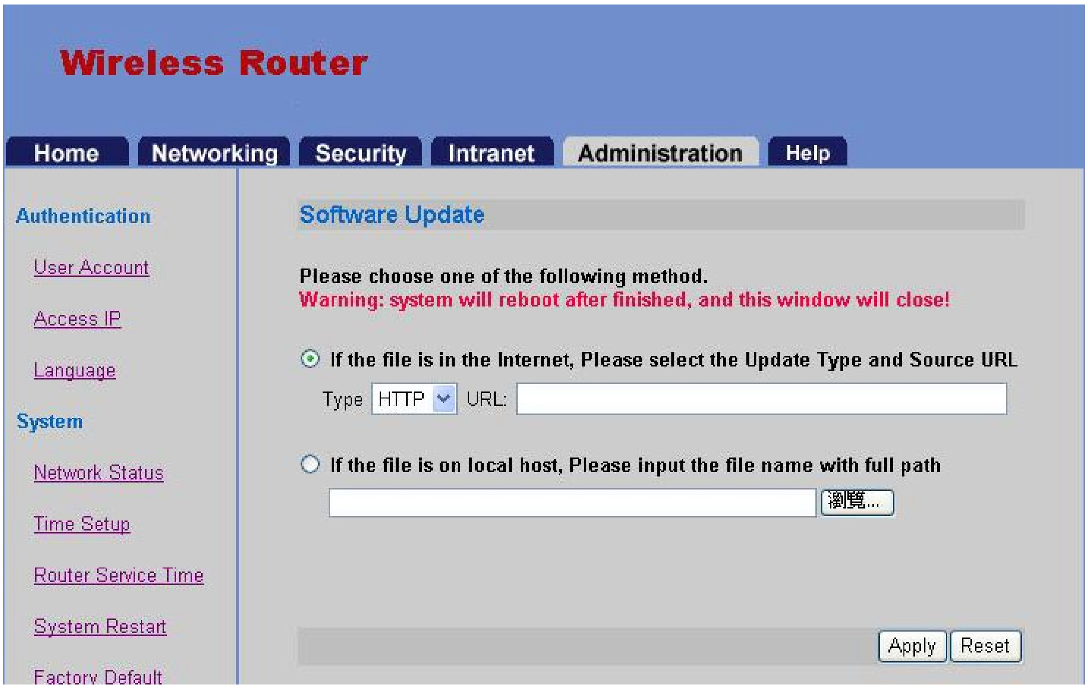


Restore Factory Default Settings

Restores default factory configuration. Current configuration will be lost.

Restore the factory default settings now.

5.5.8. Software Update



Please choose one of the following method.
Warning: system will reboot after finished, and this window will close!

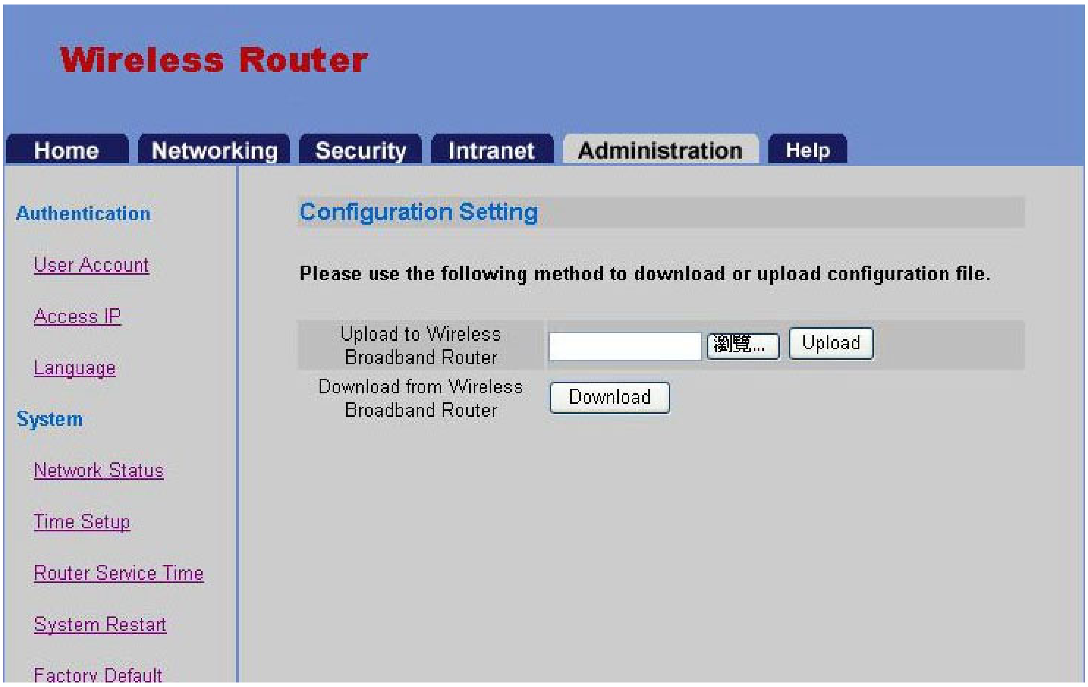
● If the file is in the Internet, Please select the Update Type and Source URL

Type HTTP URL:

○ If the file is on local host, Please input the file name with full path

1. Click on the Administration tab.
2. Under the System menu item, click on Software Update.
3. Choose either the software update file is in the internet or on the local host.
4. If the file is in the internet, type in the URL.
5. If the file is on local host, type in the name file with full path or click on Browse button to search the file on local host.
6. Click Apply button to start update.

5.5.9. Config Setting



Configuration Setting

Please use the following method to download or upload configuration file.

Upload to Wireless Broadband Router

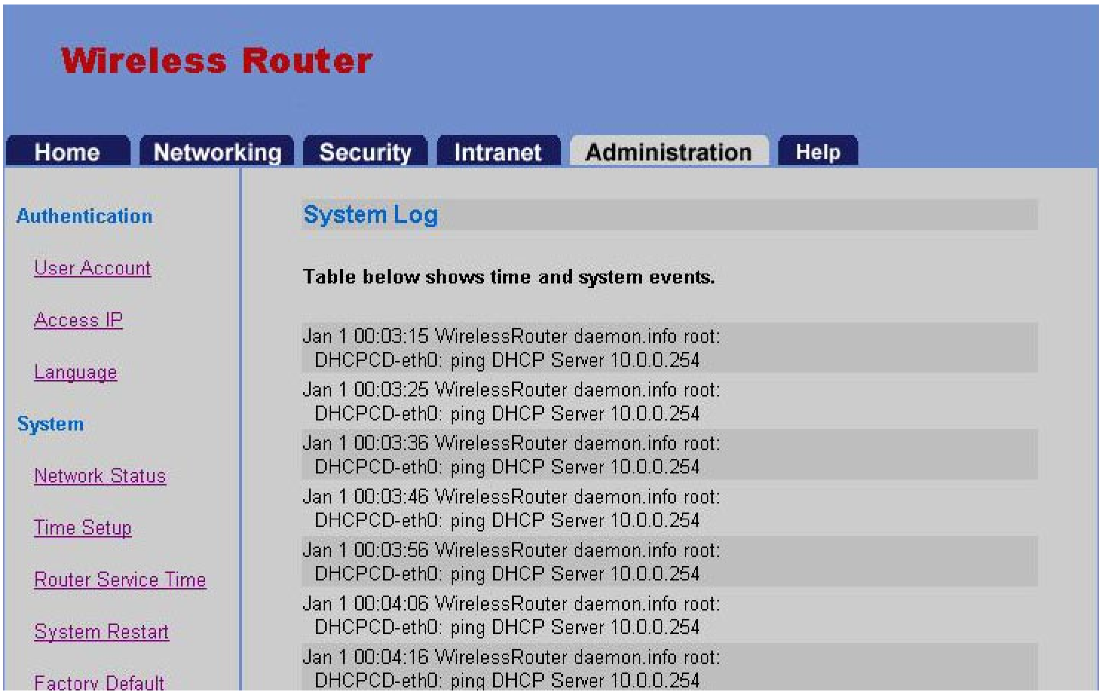
Download from Wireless Broadband Router

1. Click on the Administration tab.
2. Under the System menu item, click on Config Setting.
3. Select following method to Download or Upload configuration file.
4. If you select Download, you can either enter the path and filename in then text box or press browser button to assign path and filename. Press Download button to start.
5. If you select Upload, then press Upload button to save.

5.5.10. System Log

IEEE 802.11g WLAN Router provides a system log of all system activities up to 50 entries. Old entries will be purged automatically to ensure a healthy system. However, if you want to keep a full system log, you can setup a remote system log daemon (remote syslogd) to record all system events remotely.

This feature can also be very helpful to monitor the system activities at distant.



System Log

Table below shows time and system events.

```
Jan 1 00:03:15 WirelessRouter daemon.info root:
  DHCPCD-eth0: ping DHCP Server 10.0.0.254
Jan 1 00:03:25 WirelessRouter daemon.info root:
  DHCPCD-eth0: ping DHCP Server 10.0.0.254
Jan 1 00:03:36 WirelessRouter daemon.info root:
  DHCPCD-eth0: ping DHCP Server 10.0.0.254
Jan 1 00:03:46 WirelessRouter daemon.info root:
  DHCPCD-eth0: ping DHCP Server 10.0.0.254
Jan 1 00:03:56 WirelessRouter daemon.info root:
  DHCPCD-eth0: ping DHCP Server 10.0.0.254
Jan 1 00:04:06 WirelessRouter daemon.info root:
  DHCPCD-eth0: ping DHCP Server 10.0.0.254
Jan 1 00:04:16 WirelessRouter daemon.info root:
  DHCPCD-eth0: ping DHCP Server 10.0.0.254
```

1. Change some settings of IEEE 802.11g WLAN Router.
2. Click on the Administration tab.
3. Under the Log menu item, click on System Log.

6. Terminology

Boot
It is the process when the PC starts executing instructions.

Browser
It is an application program that helps users to view and interact with the information of the World Wide Web.

BSS (**B**asic **S**ervice **S**et)
A group of wireless Network PC Card users and an Access Point.

Cable Modem
It is a device that connects a PC to the Internet via the cable television network. It features asymmetric transmission rates: around 36 Mbps downstream from the Internet to the PC, and from 200 Kbps to 2 Mbps upstream from the PC to the Internet.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol)
It is a protocol that automates the assignment and acquirement of IP addresses between a server and a client in a network.

DMZ (De-**M**ilitarized **Z**one**)**
It allows LAN clients behind a NAT Router to be totally exposed and accessible to the WAN side in order to run special applications or set up a server.

DNS (**D**omain **N**ame **S**ystem)
Domain Name System explains where Internet domain names are located. In addition, it translates Internet domain names into Internet Protocol (IP) addresses. A domain name must be meaningful, so you can remember it easily for the access of websites.

Domain
It is a subnet work composed of a group of clients and servers.
DoS (**D**enial **o**f **S**ervice)
Denial of Service attacks network devices and try to disable the devices.

Dynamic IP Address
Dynamic IP Address is automatically assigned to a client in a TCP/IP network by a DHCP server in the network.

Encryption
A security method that applies a specific algorithm to data in order to alter the data appearance and prevent other devices from reading the information.

ESS (**E**xtended **S**ervice **S**et)
An ESS is composed of two or more BSS, and the users can roam in an ESS.

Ethernet
It is a common LAN protocol defined as the 802.3 standard by IEEE (Institute of Electrical and Electronics Engineers). All clients in the network share the total bandwidth. It could be 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 1000 Mbps (Gigabit Ethernet).

FTP (**F**ile **T**ransfer **P**rotocol)
File Transfer Protocol enables you to transfer files in a bi-directional method over a TCP/IP network.

Firewall
It is a mechanism that protects a network from attacks from the other networks. Also, it can provide the Internet access control list that restricts clients?connection to other networks.

Firmware
It is programming that is inserted into programmable read-only memory and becomes a permanent part of a computing or network device.

Hardware
It is the physical part of PCs and network device.

HTTP (**H**yper **T**ext **T**ransport **P**rotocol) **(WEB)**
It is the protocol used to transmit and receive data over the World Wide Web. It can establish connection with a Web server and transmit HTML pages to the client browser. For instance, when you enter a domain name on your browser, you are actually sending an HTTP request to a Web server for Web page information. After the Web server receives your HTTP request, it will send the Web page to you by displaying it via the browser.

ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol)
It is a kind of TCP/IP protocol that sends the error message, the control message, and the information messages to a network device. For instance, a router uses ICMP to notify the sender that its destination node is not available. A ping utility can send ICMP echo request to verify the existence of an IP address, too.

IP (**I**nternet **P**rotocol)
It is the Network Layer protocol in the TCP/IP communication and provides the basic packet delivery for TCP/IP networks. It contains a network address and allows messages to be routed to a different network or subnet.

IP Address
It is a 32-binary digit number that provides the source or destination information on the Internet.

ISP (**I**nternet **S**ervice **P**rovider)
It is a company that provides individuals and companies the access to the Internet.

LAN (**L**ocal **A**rea **N**etwork)
It consists a group of PCs and network devices that communicate with each other over a network and share the resources of a single processor or server within a small geographic area.

MAC Address (**M**edia **A**ccess **C**ontrol **A**ddress)
It is a unique number assigned to any Ethernet network device by the device manufacture. It enables the network to identify the device at the hardware level.

NAT (**N**etwork Address **T**ranslation) (IP Sharing)
Network Address Translation can translate the source IP address of a LAN client to the IP address of a WAN client before forwarding a packet from the LAN to the WAN. When the packet returns, NAT translates the destination address from a WAN client to the address of a LAN client before forwarding the packet back to the LAN client. When only one WAN IP address is available, NAT can translate the only WAN IP address into multiple LAN IP addresses for the LAN clients. Therefore the LAN clients "Share" the only one WAN IP address, and it is called "IP Sharing".

Port
It is a pathway of network device, such as a switch or a router. It can make connection between the LAN and the WAN via the network device.

Port Number
In a TCP/IP network, a port number is assigned to an application program running in the PC. The port number is included in the transmitted packets and will link the data to the correct service. Well-known ports include port 21 for FTP and port 80 for HTTP.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet)
It enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet and is commonly implemented by xDSL box Internet Service Provider for Dial-Up
Internet connections.

PPTP (**P**oint to **P**oint **T**unneling **P**rotocol)
It is a standard VPN protocol that secures a private network with encryption and authentication of User ID and Password.

Router
It is a network device that divides a large network into small sub-networks, and that transmits packets with a routing table.

Server
A server is the PC that enables its clients to access files stored in it, to make printing, and to communicate within the same Ethernet network.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol)
It is a standard e-mail protocol that defines the message format and manages the e-mail transmission between e-mail servers.

Software
It is a series of instructions that tells the PC how to process the data.

Static IP Address
Static IP is also a WAN access type provided by some Internet Service Providers. You need to enter the information of IP address, Subnet Mask, Default Gateway, Primary DNS, and Secondary DNS IP Address.

Subnet Mask
It is a method used to split IP networks into a series of subnets.

Switch
It is a network device that transmits packets between nodes on the same network.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol)
It is a group of network standards that enable PCs of different operating systems to communicate with each other across the network.

Telnet
Telnet is a terminal emulation protocol used commonly on the Internet and TCP/IP network. It enables you to log on to a remote PC and to run a program on the remote PC with an established account and password.

Virtual DMZ
Port forwarding all ports (1-65535) to a dedicated host in LAN.

Virtual Server (Port Forwarding)
A NAT Router can function as a Virtual Server that can forward the service packet specified with a port number to the LAN host specified by the LAN IP address. In other words, the Gateway can open the port for the service with specified port number and then “forward” the port to a LAN host. Therefore it is called “Port Forwarding”, too.

VPN (**V**irtual **P**rivate **N**etwork)
It is a network security mechanism that secures the network data transmission via tunneling, encryption, and authentication etc.

WAN (**W**ide **A**rea **N**etwork)
It is a kind of network that covers a wide geographic area like a country.

WEP (**W**ired **E**quivalent **P**rivacy)
A data privacy mechanism based on a 64-bit, or 128-bit shared key algorithm, as described in the IEEE 802.11standard.

Wireless LAN
It is a network technology that uses the air to transmit data between wireless clients and Access Points.