WIRELESS G BROADBAND ROUTER USER MANUAL

MODEL 503693

INTELLINET™

NETWORK SOLUTIONS

INT-503693-UM-0608-01

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Wireless G Broadband Router, Model 503693.

The Wireless G Broadband Router allows you to conveniently share your network connection with multiple users on your network — with or without wires. It delivers 10/100 Mbps (auto-sensing) WAN and LAN connections, and is interoperable with 54 Mbps (802.11g) and 11 Mbps (802.11b) devices over a 2.4 GHz band wireless network. The WAN connection wizard makes installation a snap.

Keeping intruders out of your network can be a challenge, and this feature-rich wireless router is designed to make that challenge easier. It includes a true firewall that secures your network against hackers. With Network Address Translation (NAT) to shield your networked devices from intruders, Denial of Service (DoS) attack prevention to avert potential threats by scanning incoming traffic, and WEP, WPA and WPA2 encryption to conceal your information on the wireless LAN from eavesdroppers, you can rest assured that you've taken the necessary precautions to protect the data on your network.

The easy-to-follow instructions in this user manual help make setup and operation relatively simple, so you'll soon be enjoying the benefits of these additional features:

- Compatible with all common DSL and cable Internet service providers
- Easy wireless setup through integrated site survey function
- Supports Wi-Fi Protected Setup (WPS)
- Supports WMM function to meet the multi-media data bandwidth requirement
- Supports MAC filtering for wireless clients
- Supports Access Point mode and WDS (Wireless Distribution System) mode
- Integrated 10/100 Mbps LAN switch with Auto MDI/MDI-X support
- DHCP server assigns IP addresses for all LAN users
- Supports DDNS (dynamic DNS)
- 68 Mbps WAN-to-LAN throughput for wired networks
- Content control through URL, IP and Port filter
- Remote management function (enable/disable and management port)
- Easy installation and firmware updates through a Web-based user interface
- Lifetime Warranty

NOTE: For a quick install procedure, refer to the printed quick install guide enclosed with this product.

SAFETY & COMPLIANCE STATEMENTS

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of Federal Communications Commission (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 the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

CONTENTS

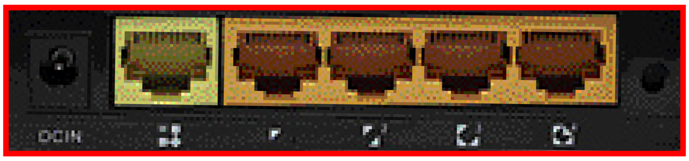
1 HARDWARE

1.1 Front Panel / LEDs

The front panel of the Wireless G Broadband Router features several LEDs for immediate indication of the device's operational status.

LED	Status	Description
PWR	On	Power is on.
	Off	Power is off.
CPU	On	The router is initializing.
	Flashing	The router is operating properly.
	Off	The router is experiencing a hardware error.
WL	Flashing	The wireless radio function is enabled.
	Off	The wireless radio function is disabled.
WAN	On	There is a device linked to the port, but no activity.
	Flashing	There is an active device linked to the port.
	Off	There is no device linked to the port.
1/2/3/4	On	There is a device linked to the port, but no activity.
	Flashing	There is an active device linked to the port.
	Off	There is no device linked to the port.

1.2 Rear Panel / Ports & Jacks



The rear panel of the Wireless G Broadband Router features these ports and jacks (left to right):

- Power adapter jack. ***NOTE:*** Only use the power adapter included with the Wireless G Broadband Router, as a different adapter could result in product damage.
- WAN RJ-45 port for connecting the router to a cable, DSL modem or Ethernet.
- Four LAN 10/100 Mbps RJ-45 ports for connecting the router to local PCs.
- Factory default reset button (recessed). ***NOTE:*** To reset to factory defaults, first turn the router on. Next, press in and hold the reset button for approximately 20 seconds. Then release the reset button and wait for the router to reboot.

1.3 System Requirements

Proper use of the Wireless G Broadband Router requires the following system components and connections:

- Broadband Internet access service (DSL/cable/Ethernet)
- DSL/cable modem that has an RJ-45 connector (not needed if you connect the router to the Ethernet)
- Each PC on the LAN needs a working Ethernet adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

Also, keep these guidelines in mind when positioning the router before installation and operation:

- Don't place it in direct sunlight or near a heater or heating vent.
- Keep at least 2 inches (5 cm) of space on all sides of the router.
- Keep the space well ventilated (especially if placed in a closet).
- Maintain the operating temperature and humidity as per specifications listed at the back of this user manual.

1.4 Connecting the Router

Before installing the router, connect your PC to the Internet through your broadband service. (If there is any problem, contact your ISP.) Then proceed through the following steps.

1. Turn off your PC(s), cable/DSL modem and the router.
2. Adjust the antenna. Normally, upright is a good place to start.
3. Connect the PC(s) and each switch/hub on your local area network to the LAN ports on the router.
4. Connect the DSL/cable modem to the WAN port on the router.
5. Connect the power adapter between the power socket on the router and an electrical outlet. The router will start to work automatically.
6. Turn on your PC(s) and the cable/DSL modem.

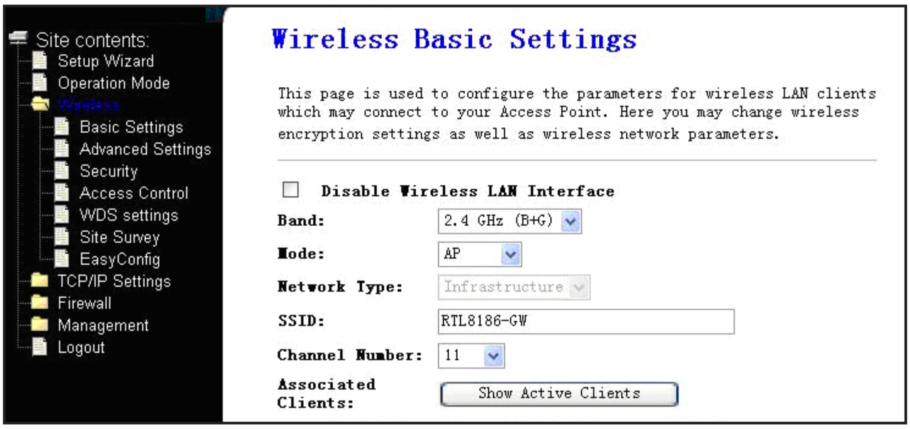
2 CONFIGURATION

2.1 Login

Connect to the Wireless G Broadband Router by entering http://192.168.1.254 in the address field of your Web browser. Once you've logged in, the browser will display the administrator menu on the left-hand side of the screen, with the five configuration options — Wireless (Settings), TCP/IP Settings, Firewall, Management and Logout — explained in detail in the following sections.

2.2 Wireless Settings

2.2.1 Basic Settings



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G)
Mode:	AP
Network Type:	Infrastructure
SSID:	RTL8186-GW
Channel Number:	11
Associated Clients:	Show Active Clients

Band — The three options in the drop-down menu are “2.4 GHz (G)” for 54 Mbps (802.11g); “2.4G Hz (B)” for 11 Mbps (802.11b); and “2.4 GHz (G+B),” which allows both 802.11g and 802.11b wireless stations to connect to the router.

Mode — The default is “AP”; options are “Client,” “WDS,” “AP+WDS.”

Network Type — The default is “Infrastructure”; when Mode is set to “Client,” this should be set to “Ad Hoc.”

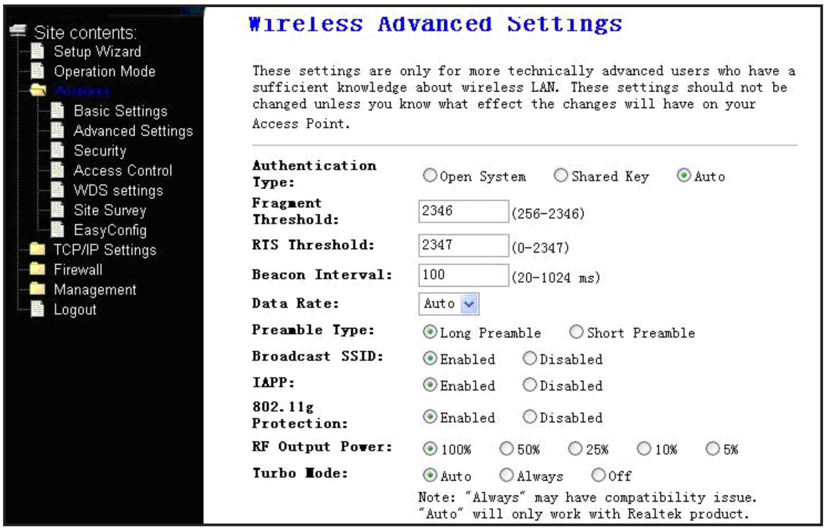
SSID — Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. ***NOTE:*** The default SSID is “Kingnet,” but it’s recommended that you change your network’s SSID to a different (case-sensitive) value.

Channel — It isn’t necessary to change the channel (1-13) unless you notice interference problems with another nearby access point.

Associated Clients — Click to show active clients.

2.2.2 Wireless Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge of wireless LAN. These settings should not be changed unless you know what effect the changes will have on your access point.



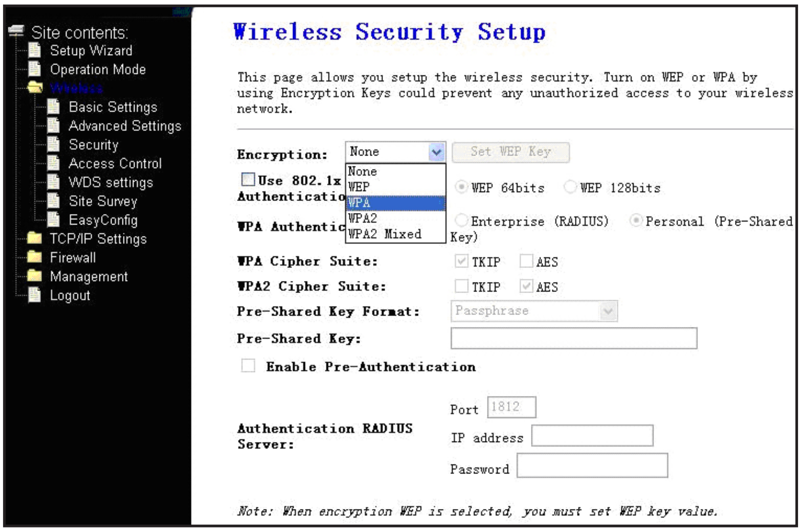
Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
IAPP:	● Enabled ○ Disabled
802.11g Protection:	● Enabled ○ Disabled
RF Output Power:	● 100% ○ 50% ○ 25% ○ 10% ○ 5%
Turbo Mode:	● Auto ○ Always ○ Off

Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

2.2.3 Wireless Security Setup



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: None (None / WEP / WPA / WPA2 / WPA2 Mixed) Set WEP Key

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

Encryption — Select “None,” “WEP,” “WPA,” WPA2” or “WPA2 Mixed.”

- WEP: Wired Equivalent Protocol.
- WPA: WI-FI Protected Access (WPA) is an intermediate solution for security issues. It uses Temporal Key Integrity Protocol (TKIP) to replace WEP.

WPA Authentication Mode — “Enterprise” uses an external authentication server (e.g., RADIUS) and EAP just as IEEE 802.1X does; “Personal” uses pre-shared keys without the need for additional servers. Both options will generate a master session key for the authenticator (AP) and supplicant (client station).

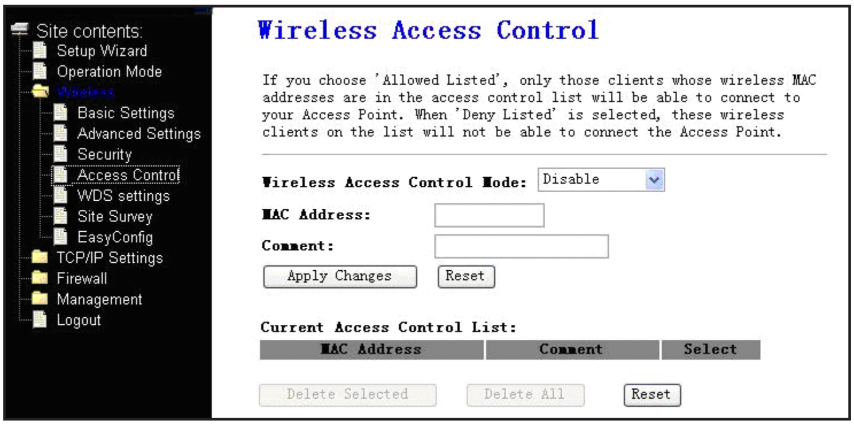
WPA Cipher Suite/WPA2 Cipher Suite — Choose either TKIP or AES.

Pre-Shared Key Format — Select passphrase or hex characters.

Pre-Shared Key — Enter up to 128 characters.

Authentication RADIUS Server — Enter a port, IP address and password.

2.2.4 Wireless Access Control



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

MAC Address:

Comment:

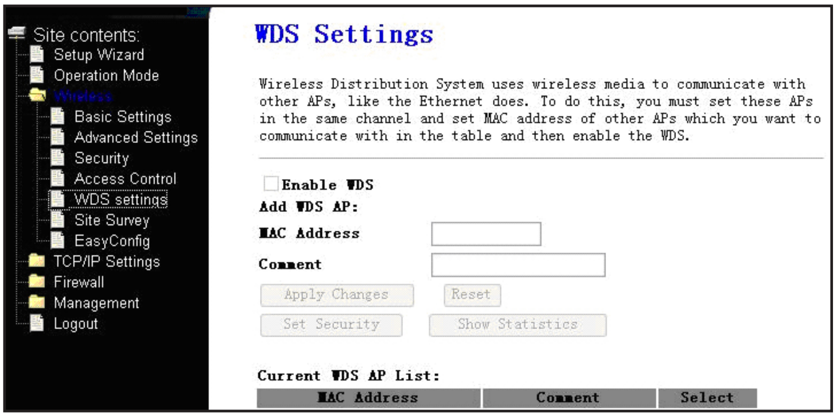
Current Access Control List:

MAC Address	Comment	Select

Wired Access Control Mode — If you choose “Allowed Listed” from the drop-down menu, only those clients whose wireless MAC addresses are on the access control list will be able to connect to your access point. When”Deny Listed” is selected, these wireless clients on the list will *not* be able to connect to the access point.

2.2.5 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, as the Ethernet does. To do this, you must set these APs in the same channel and set the MAC address of other APs you want to communicate with in the table and then enable the Wireless Distribution System.



WDS Settings

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.

□ Enable WDS

Add WDS AP:

MAC Address

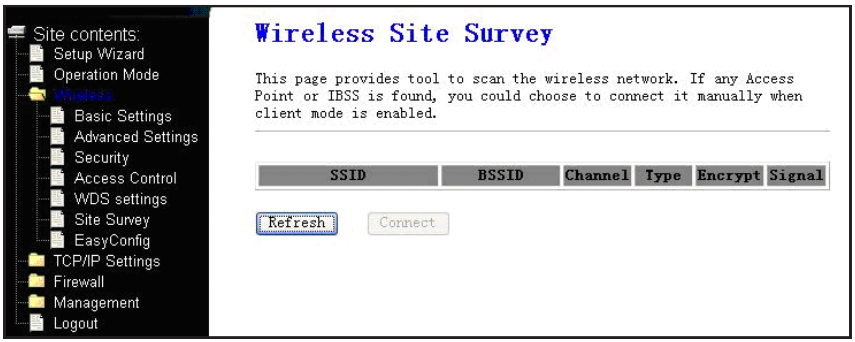
Comment

Current WDS AP List:

MAC Address	Comment	Select

2.2.6 Wireless Site Survey

This screen lets you scan the wireless network. If any access point or IBSS is found, you could choose to connect it manually when Client mode is enabled.



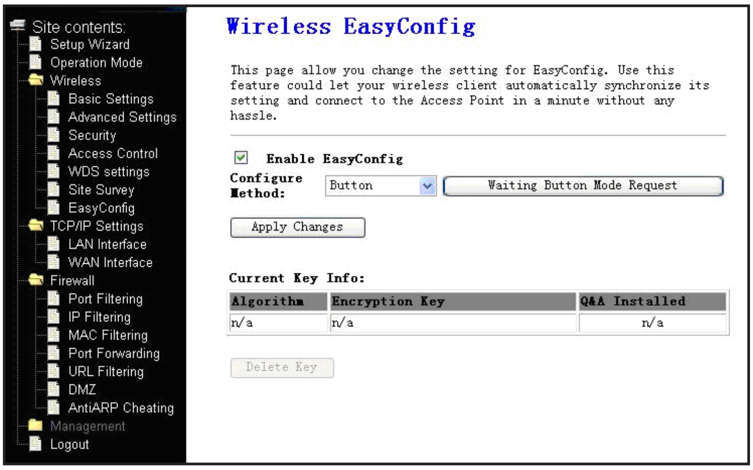
Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal

2.2.7 Wireless EasyConfig

This screen lets you change the setting for EasyConfig, a feature that allows your wireless client to automatically synchronize its setting and connect to the access point in a minute without any hassle.



Wireless EasyConfig

This page allow you change the setting for EasyConfig. Use this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

☑ Enable EasyConfig

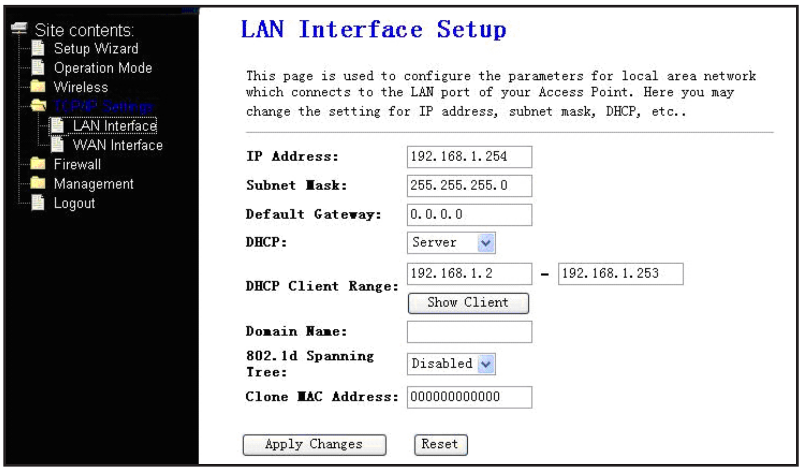
Configure Method: Button

Current Key Info:

Algorithm	Encryption Key	Q&A Installed
n/a	n/a	n/a

2.3 TCP/IP Settings

2.3.1 LAN Interface Setup



LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.1.2 – 192.168.1.253 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

IP Address — Enter the IP address of your router in dotted-decimal notation (factory default = 192.168.1.254).

Subnet Mask — This determines the size of the network, and would normally be set to 255.255.255.0.

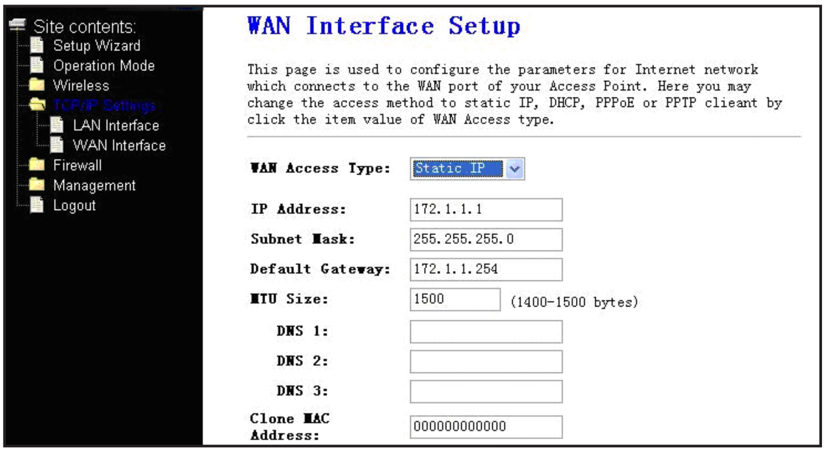
DHCP — Drop-down options are “None,” “Client” and “Serve.” The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs connected to the router on the LAN.

DHCP Client Range — Specify the first and final addresses in the IP address pool range.

802.1d Spanning Tree — Select “Enabled” or “Disabled.”

Clone MAC Address — Enter a MAC address, then click “Apply.”

2.3.2 WAN Interface Setup



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 or PPTP clieant by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254
MTU Size:	1500 (1400-1500 bytes)
DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

WAN Access Type — The drop-down menu lets you choose among “Static IP,” “DHCP,” “PPPoE” and “PPTP.” Each option displays a corresponding list of further options (IP address, subnet mask, server IP address, username and password can be obtained from your ISP, if necessary), including those below.

Connection Type — Select “Continuous,” “Connect on Demand” or “Manual.”

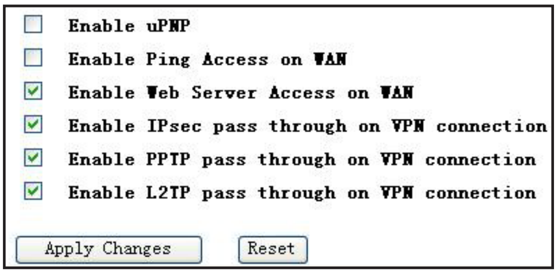
Idle Time — When the connection type is set to “Connect on Demand,” you can set the idle time.

MTU Size — The normal MTU (maximum transmission unit) value for most Ethernet networks is 1492 Bytes. For some ISPs, you need to reduce the MTU. This is rarely required, however, and shouldn’t be done unless you’re sure it’s necessary for your ISP connection.

DNS — Select “Attain DNS Automatically” or “Set DNS Manually.”

Clone MAC Address — Enter a MAC address, then click “Apply.”

Enable UpnP — The Universal Plug and Play (UPnP) feature lets devices access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.



☐ Enable uPNP

☐ Enable Ping Access on WAN

☑ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

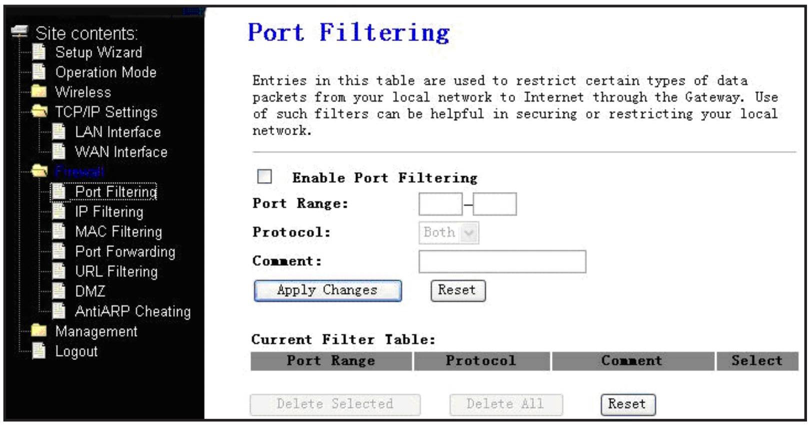
☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

2.4 Firewall

2.4.1 Port Filtering

Entries on this screen are used to restrict certain types of data packets from your local network to the Internet through the gateway. Using such filters can be helpful in securing/restricting your local network.



Port Filtering

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

☐ Enable Port Filtering

Port Range: -

Protocol: Both

Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select

Enable Port Filtering — Select to modify the port filter.

Port Range — Enter the filter port range; for example, 20-220.

Protocol — Select “TCP,” “UDP” or “Both.”

Current Filter Table — This displays the list of port filters.

2.4.2 IP Filtering

Similar to Port Filtering (above), with similar options.

Enable IP Filtering — Select to modify the IP filter.

Local IP Address — Enter the filter IP address(es); for example, 192.168.1.23.

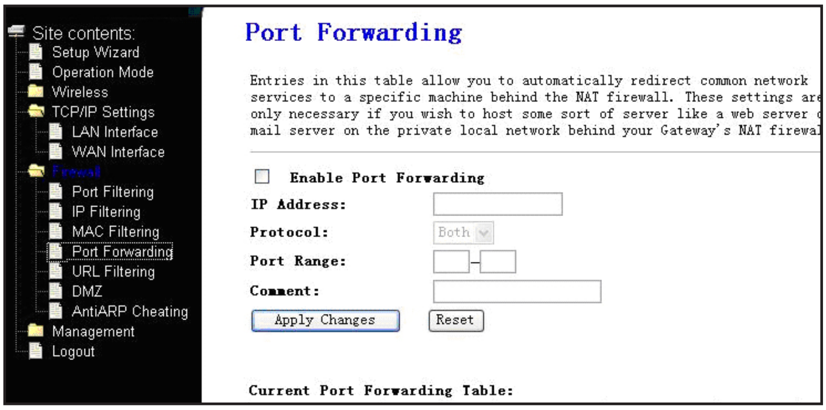
Protocol — Select “TCP,” “UDP” or “Both.”

Current Filter Table — This displays the list of IP filters.

2.4.3 MAC Filtering

Similar to Port and IP Filtering (above), with similar options.
Enable MAC Filtering — Select to modify the MAC filter.
MAC Address — Enter the MAC address; for example, 00:e0:4e:3f:2d:c5.
Protocol — Select “TCP,” “UDP” or “Both.”
Current Filter Table — This displays the list of MAC filters.

2.4.4 Port Forwarding



Port Forwarding

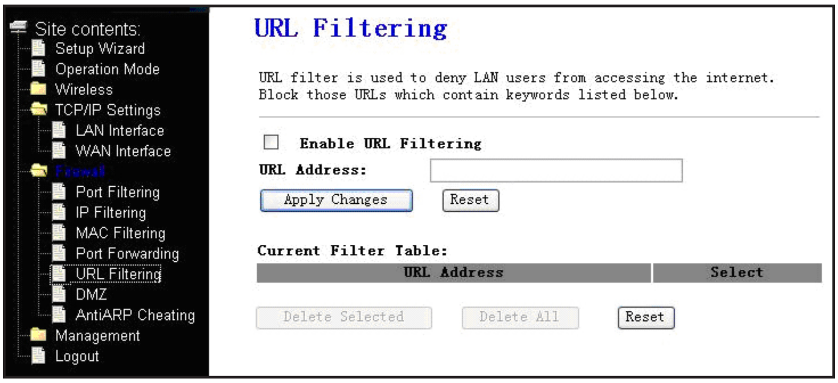
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server o mail server on the private local network behind your Gateway's NAT firewal

□ Enable Port Forwarding
IP Address:
Protocol: Both
Port Range: –
Comment:

Current Port Forwarding Table:

Entries on this screen allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server, like a Web server or mail server on the private local network behind your gateway’s NAT firewall.
Enable Port Forwarding — Select to enable the function.
IP Address — The IP address of the PC running the service application.
Protocol — Select “TCP,” “UDP” or “Both.”
Port Range — Enter the number(s) of the external port(s). Whether it’s a single service port or a range of service ports, the format is XXX – YYY, where XXX is the start port and YYY is the end port).
Current Port Forwarding Table — This displays the list of port forwarding services.

2.4.5 URL Filtering



URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

□ Enable URL Filtering
URL Address:

Current Filter Table:

URL Address	Select

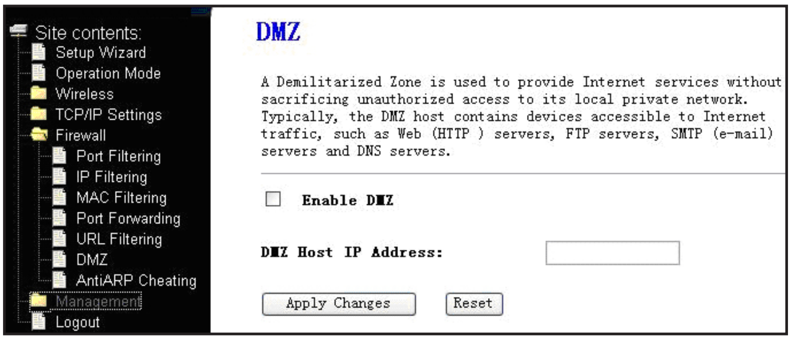
A URL filter is used to deny LAN users access to the Internet. Once selected, this filter function lets you use specific keywords to block associated URLs.
Enable URL Filtering — Select to enable the function.
URL Address — Enter a specific address to block; e.g., xxx.com.

2.4.6 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service, such as Internet gaming or videoconferencing. DMZ Host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ Enable — Select to enable the function.

DMZ Host IP Address — Enter an IP address; e.g., 192.168.1.34.



DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

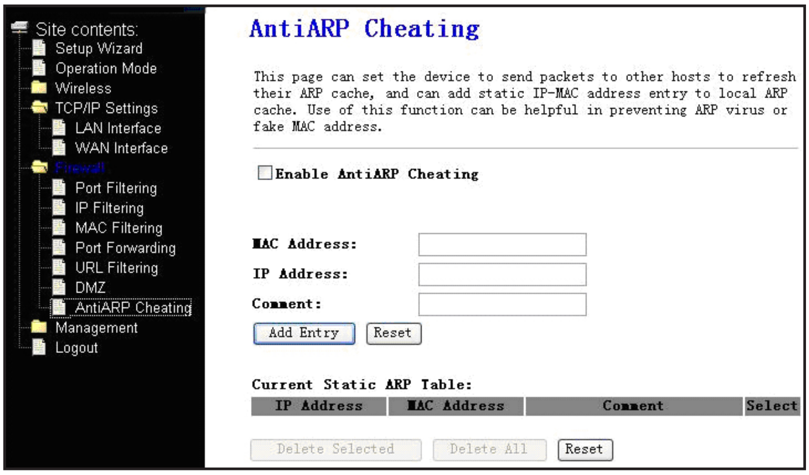
□ Enable DMZ

DMZ Host IP Address:

Apply Changes   Reset

2.4.7 Anti-ARP Cheating

On this screen, you can set the device to send packets to other hosts to refresh their ARP (address resolution protocol) cache. You can also add static IP-MAC address entries to local ARP caches. Use of this function can be helpful in preventing ARP viruses or fake MAC addresses.



AntiARP Cheating

This page can set the device to send packets to other hosts to refresh their ARP cache, and can add static IP-MAC address entry to local ARP cache. Use of this function can be helpful in preventing ARP virus or fake MAC address.

□ Enable AntiARP Cheating

MAC Address:

IP Address:

Comment:

Add Entry   Reset

Current Static ARP Table:

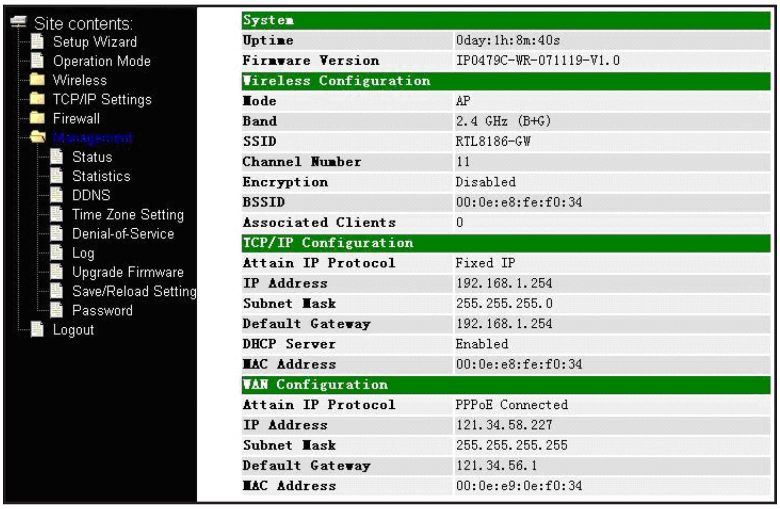
IP Address	MAC Address	Comment	Select

Delete Selected   Delete All   Reset

2.5 Management

2.5.1 Status

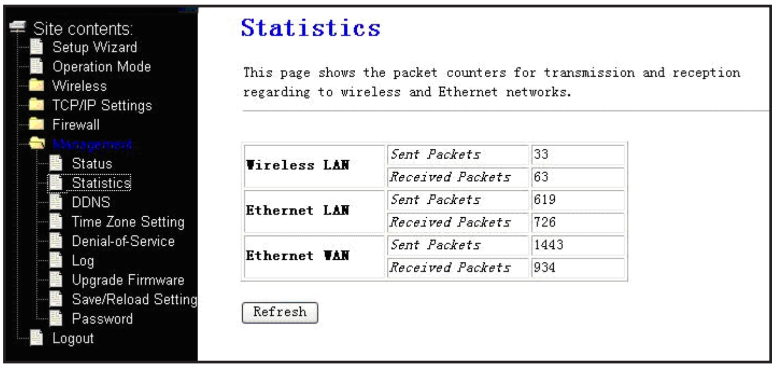
This screen shows the current status — and some basic settings of — the device, such as System Information, LAN Interface Information and WAN Interface Information.



System	
Uptime	0day:1h:8m:40s
Firmware Version	IP0479C-WR-071119-V1.0
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	RTL8186-GW
Channel Number	11
Encryption	Disabled
BSSID	00:0e:e8:fe:f0:34
Associated Clients	0
TCP/IP 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	00:0e:e8:fe:f0:34
WAN Configuration	
Attain IP Protocol	PPPoE Connected
IP Address	121.34.58.227
Subnet Mask	255.255.255.255
Default Gateway	121.34.56.1
MAC Address	00:0e:e9:0e:f0:34

2.5.2 Statistics

This screen displays the packet counters for transmission and reception as regards to wireless and Ethernet networks.

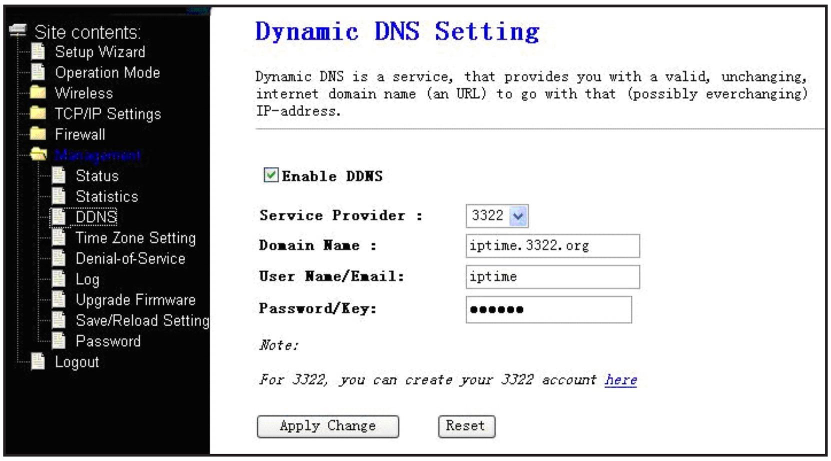


Statistics

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

Wireless LAN	*Sent Packets*	33
	Received Packets	63
Ethernet LAN	*Sent Packets*	619
	Received Packets	726
Ethernet WAN	*Sent Packets*	1443
	Received Packets	934

2.5.3 Dynamic DNS Settings



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☑ **Enable DDNS**

Service Provider : 3322

Domain Name : iptime.3322.org

User Name/Email: iptime

Password/Key: ●●●●●●

Note:

For 3322, you can create your 3322 account here

Dynamic DNS is a service that provides you with a valid, unchanging Internet domain name (URL) to go with your (possibly ever-changing) IP address. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own Web site, FTP server or other server behind the router. Before using this feature, you need to sign up with a DDNS service provider, such as www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS:

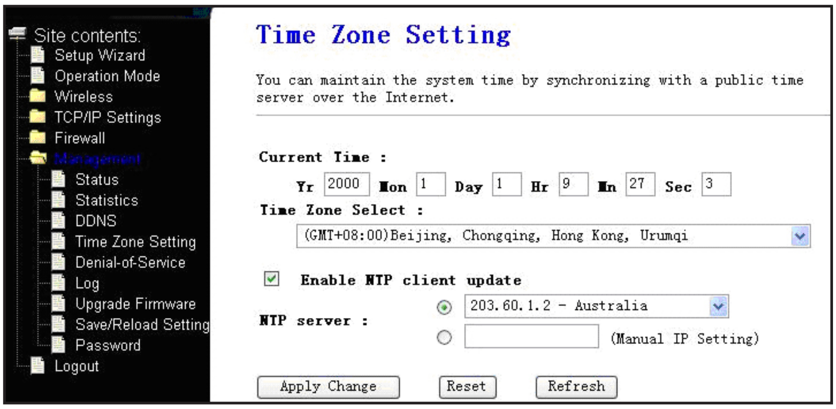
1. Enter your service provider.
2. Enter the username for your DDNS account.
3. Enter the password for your DDNS account.
4. Domain Name: The domain names are displayed here. Click “Apply Changes” to log out of the DDNS service.

2.5.4 Time Zone Settings

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time — Enter the date and time.

Time Zone Select — Select your local time zone from the drop-down list.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time :

Yr 2000 Mon 1 Day 1 Hr 9 Mn 27 Sec 3

Time Zone Select : (GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi

☑ Enable NTP client update

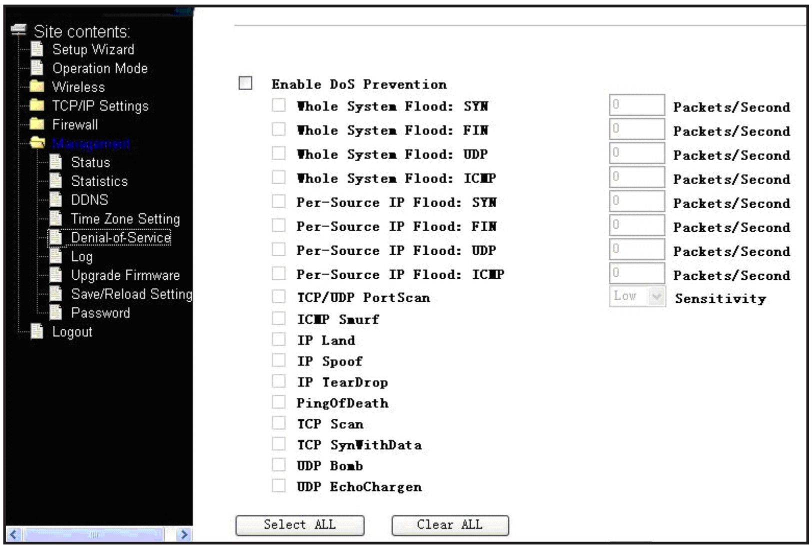
NTP server : ● 203.60.1.2 - Australia
○ (Manual IP Setting)

Enable NTP client update — Select to get the time from NTP (Network Time Protocol).

NTP server — Select a server from the drop-down menu.

Click “Apply Change” to get the time from the Internet (if connected).

2.5.5 Denial of Service



□ Enable DoS Prevention

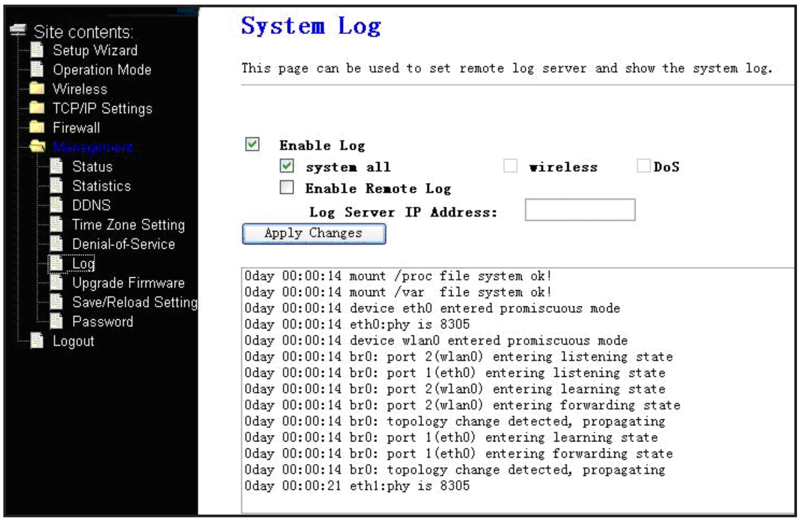
□ Whole System Flood: SYN	0	Packets/Second
□ Whole System Flood: FIN	0	Packets/Second
□ Whole System Flood: UDP	0	Packets/Second
□ Whole System Flood: ICMP	0	Packets/Second
□ Per-Source IP Flood: SYN	0	Packets/Second
□ Per-Source IP Flood: FIN	0	Packets/Second
□ Per-Source IP Flood: UDP	0	Packets/Second
□ Per-Source IP Flood: ICMP	0	Packets/Second
□ TCP/UDP PortScan	Low	Sensitivity
□ ICMP Smurf		
□ IP Land		
□ IP Spoof		
□ IP TearDrop		
□ PingOfDeath		
□ TCP Scan		
□ TCP SynWithData		
□ UDP Bomb		
□ UDP EchoChargen		

A denial-of-service (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Enable DOS Prevention — Select to modify the function.

Enable Source IP Blocking — Enter a source IP blocking time.

2.5.6 System Log



System Log

This page can be used to set remote log server and show the system log.

☑ Enable Log

☑ system all □ wireless □ DoS

□ Enable Remote Log

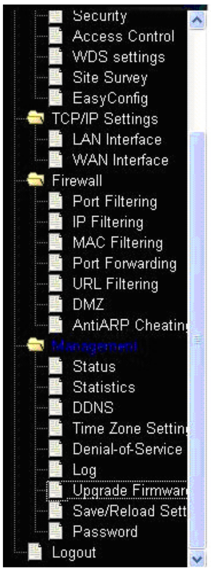
Log Server IP Address:

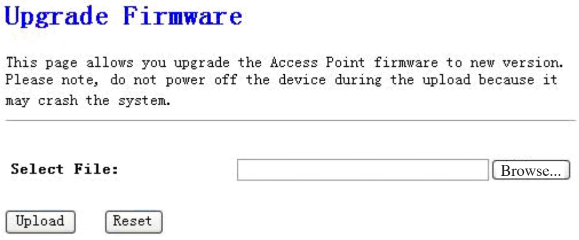
```
0day 00:00:14 mount /proc file system ok!
0day 00:00:14 mount /var  file system ok!
0day 00:00:14 device eth0 entered promiscuous mode
0day 00:00:14 eth0:phy is 8305
0day 00:00:14 device wlan0 entered promiscuous mode
0day 00:00:14 br0: port 2(wlan0) entering listening state
0day 00:00:14 br0: port 1(eth0) entering listening state
0day 00:00:14 br0: port 2(wlan0) entering learning state
0day 00:00:14 br0: port 2(wlan0) entering forwarding state
0day 00:00:14 br0: topology change detected, propagating
0day 00:00:14 br0: port 1(eth0) entering learning state
0day 00:00:14 br0: port 1(eth0) entering forwarding state
0day 00:00:14 br0: topology change detected, propagating
0day 00:00:21 eth1:phy is 8305
```

This screen displays the system log and can be used to set the remote log server.

2.5.7 Upgrade Firmware

This screen lets you upgrade the AP firmware. ***NOTE:*** Do not power off the device during the upload, as doing so may crash the system.





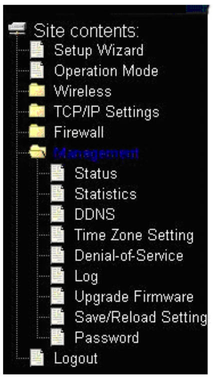
Upgrade Firmware

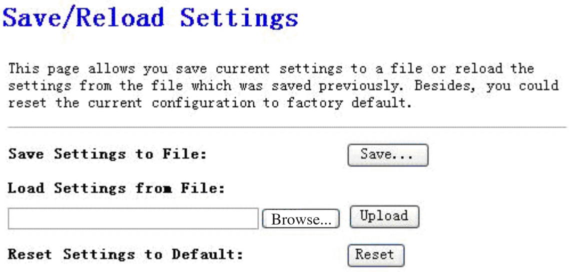
This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

2.5.8 Save/Reload Settings

This screen lets you save current settings to a file or reload the settings from the file which was saved previously. You can also reset the current configuration to factory default settings.





Save/Reload Settings

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

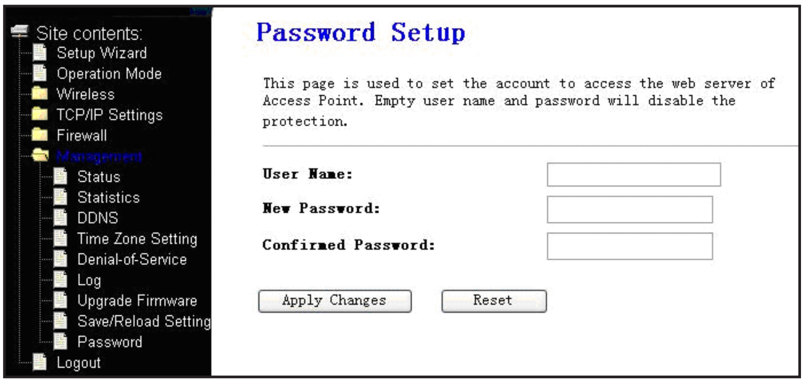
Save Settings to File:

Load Settings from File:

Reset Settings to Default:

2.5.9 Password Setup

On this screen, you can set up the account to access the Web server of the access point. ***NOTE:*** Empty fields for "User Name" or "Password" disables the protection.



Password Setup

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

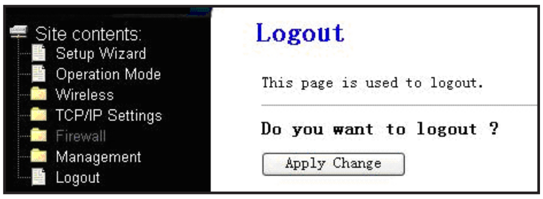
User Name:

New Password:

Confirmed Password:

2.6 Logout

This screen is used to log out.



Logout

This page is used to logout.

Do you want to logout ?

3 SPECIFICATIONS

Standards

- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.1x (Wireless User Authentication)
- IEEE 802.11b (11 Mbps Wireless LAN)
- IEEE 802.11g (54 Mbps Wireless LAN)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3u (100Base-TX Fast Ethernet)

General

- LAN ports: 4 RJ-45 10/100 Mbps data ports
- LAN ports with Auto MDI/ MDI-X
- LAN to WAN throughput: 68 Mbps
- Certifications: FCC Class B, CE Mark, RoHS

Router

- Chipset: Realtek RTL8186
- Supported WAN connection types:
  - Dynamic IP (DHCP for cable service)
  - Static IP
  - PPPoE (for DSL)
- Protocols:
  - CSMA/CA
  - CSMA/CD
  - TCP/IP
  - UDP
  - ICMP
  - PPPoE
  - NTP
  - NAT
  - DHCP
  - DNS
- NAT: Port forwarding
- Firewall:
  - Port filter
  - IP filter
  - Access control based on . MAC address
  - URL filter
  - DMZ (demilitarized zone)
  - Anti-ARP Cheating
- Supports:
  - UPnP (Universal Plug and Play)
  - DHCP (client/server)
  - PPPoE (DSL), DHCP (cable) and static IP
  - VPN PPTP, L2TP and IPsec pass-through

Wireless

- Chipset: RTL8225
- Wireless frequency range: 2.412 - 2.484 GHz
- Modulation technologies:
  - 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
  - 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- Number of channels: 11
- Data rates:
  - IEEE 802.11b (11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps)
  - IEEE 802.11g (54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps)
- Output power:
  - OFDM: 15 dBm +/- 1 dBm (54 Mbps, 50 mW max.)
  - CCK: 15 dBm +/- 1 dBm (11 Mbps, 50 mW max.)
- Max. coverage distance: 100 m / 300 ft. (indoor), 300 m / 900 ft. (outdoor)
- Wireless security:
  - WEP encryption (64/128 bit)
  - WPA (TKIP and AES)
  - WPA2 (TKIP and AES)
  - Client access control thru MAC filter
- Antenna: single dipole, 2 dBi gain

LEDs

- Power
- CPU (operational status)
- WL (Wireless)
- WAN Link/Act
- LAN 1-4 Link/Act

Environmental

- Dimensions: 169 (W) x 108 (L) x 180 (H) mm (6.6 x 4.3 x 7.0 in.)
- Weight: 0.8 kg (1.8 lbs.)
- Operating temperature: 0 – 55°C (32 – 122°F)
- Operating humidity: 10 – 95% RH, non-condensing
- Storage temperature: 0 – 60°C (0 – 149°F)

Power

- External power adapter: 9.0 V DC, 0.8 A
- Power consumption: 6.3 Watts max.

Package Contents

- Wireless G Broadband Router
- User manual
- Power cord
- Ethernet Cat5 RJ-45 cable, 0.8 m (2.6 ft.)

INTELLINET™

NETWORK SOLUTIONS

BRINGING NETWORKS TO LIFE

INTELLINET NETWORK SOLUTIONS™ offers a complete line
of active and passive networking products.
Ask your local computer dealer for more information or visit
www.intellinet-network.com.