MG7315

8x4 DOCSIS 3.0 Cable Modem plus N450 Router User Manual

VER: 1.0

Contents

1 Safety Precautions

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.
- The screen of the coaxial cable is intended to be connected to earth in the building installation.

2 Overview

The MG7315 is targeted towards DOCSIS3.0 cable modem and gateway. With eight downstream channels and four upstream channels, it supports up to 400Mbs/160Mbs.The MG7315 incorporates a variety of industry standard peripheral interfaces including dual IEEE802.3 10/100/1000Mbps interface, one with integrated GPHY. The MG7315 supports WLAN access. It complies with IEEE 802.11,802.11b/g and 802.11n specifications, WEP, WPA, and WPA2 security specifications. The WLAN of the MG7315 supports 3T3R.

2.1 Application

- Home gateway
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

2.2 Features

- User-friendly GUI for web configuration
- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- WLAN with high-speed data transfer rates of up to 450 Mbps, compatible with IEEE 802.11b/g/n, 2.4GHz compliant equipment
- IP routing and bridging
- Network/port address translation (NAT/PAT)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)

- File server for network attached storage (NAS) devices
- Web filtering
- Remote update
- System statistics and monitoring

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- DOCSIS3.0
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

3 Hardware Description and Hardware Installation

3.1 Hardware Description

3.1.1 Front Panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on and the device operates normally.
		Off	The device is powered off.
D/S	Green	On	CM has locked D/S frequency
		Blink	CM scan D/S frequency
		Off	Device is powered off.
	Blue	On	CM has locked D/S channel bonding
		Blink	CM is on D/S channel bonding
		Off	Device is powered off.
U/S	Green	On	CM has locked U/S frequency
		Blink	CM is range and scan U/S frequency
		Off	Device is powered off or CM scan D/S frequency.
	Blue	On	CM has locked U/S channel bonding
		Blink	CM is on U/S channel bonding
		Off	Device is powered off or CM scan D/S frequency.
Internet	Green	off	Not connect
		On	CM online
		Blink	Catching the wan man address
Ethernet	Green	On	The Ethernet interface is connected.

Indicator	Color	Status	Description
1/2/3/4		Blink	Data is being transmitted through the Ethernet interface.
		Off	The Ethernet interface is disconnected.
WLAN	Green	On	WLAN is enabled.
		Blink	Data is being transmitted through the wireless interface.
		Off	WLAN is disabled.
WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
		Blink	Negotiation is in progress under Wi-Fi Protected Setup.
		Off	Wi-Fi Protected Setup is disabled.

3.1.2 Rear Panel

The following table describes the interfaces or the buttons on the rear panel.

Interface	Description
Antenna	The antenna interface, for connecting the antennas.
Cable	RF cable port, for connecting HFC cable.
Reset	Press the button for at least 10 second and then release it. System restores the factory default settings.
Eth 4~1	RJ-45 port, for connecting the router to a PC or another network device.
Power	Power interface, for connecting the power adapter.

⚠ **Warning:**

*Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the **Reset** button gently for 10 second with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.*

3.2 Hardware Installation

3.2.1 Connecting the Device

Please follow the steps below to connect the device.

Step1 Connect the **Cable** port of the CM/RG with HFC cable.

Step2 Connect the **Eth** port of the CM/RG to the network card of the PC via an Ethernet cable.

Step3 Plug one end of the power adapter to the wall outlet and connect the other end to the **Power** port of the CM/RG.

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. MG7315 provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows 7.

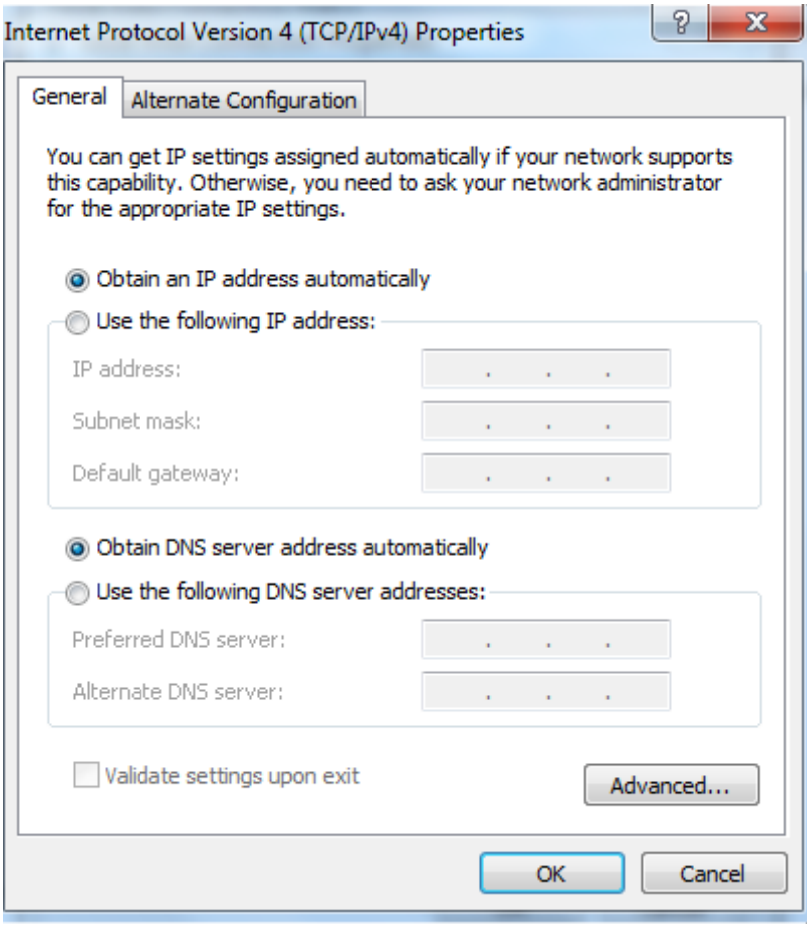

Figure 1 IP and DNS configuration

TCP/IP configuration steps for Windows XP are as follows:

Step1 Choose **Start** > **Control Panel** > **Network Connections**.

Step2 Right-click the Ethernet connection icon and choose **Properties**.

Step3 On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.

Step4 The **Internet Protocol (TCP/IP) Properties** window appears.

Step5 Select the **Obtain an IP address automatically** radio button.

Step6 Select the **Obtain DNS server address automatically** radio button.

Step7 Click **OK** to save the settings.

4.2 Logging In to the MG7315 Cable Modem

To log in to the MG7315 cable modem, do as follows:

Step1 Open a Web browser on your computer.

Step2 Enter ***http://192.168.100.1*** (the default IP address of the MG7315cable modem) in the address bar. The login page appears.

Step3 Enter the user name and the password. The default Username is **admin** and the Password is **motorola**.

Step4 Click **Login** to log in to the MG7315 cable Modem.

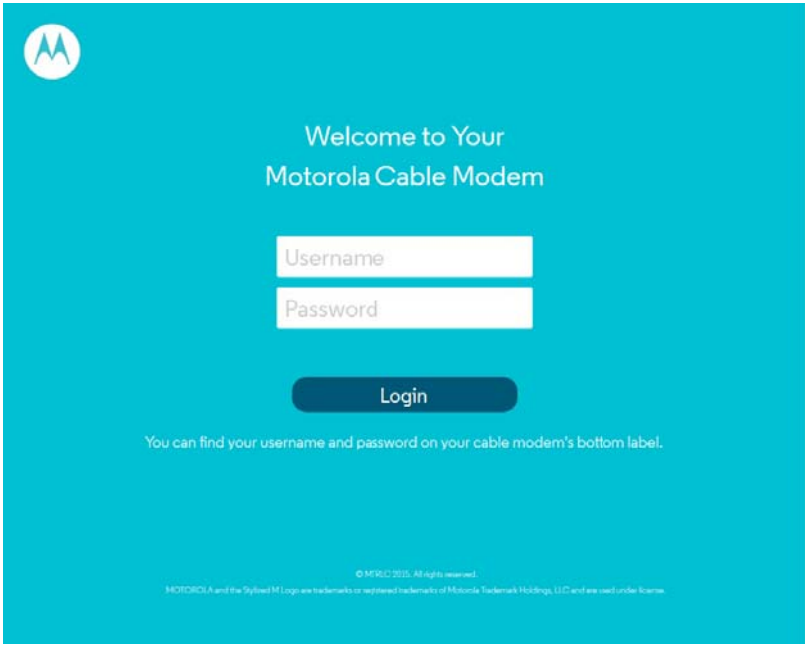

Figure 2 Login page

After logging in to the MG7315 cable modem, click on the Advanced options you can query, configure, and modify all the settings, and diagnose the system.

5 Web-Based Management

This chapter describes how to use Web-based management of the Cable Modem, which allows you to configure and control all of cable modem residential gateway features and system parameters in a user-friendly GUI.

5.1 Status

Choose **Status**, and the submenus of **Status** are shown as below.

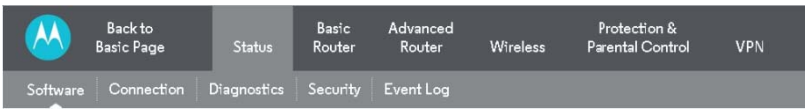

Figure 3 Submenus of status

5.1.1 Software

Choose **Status > Software** and the following page appears.

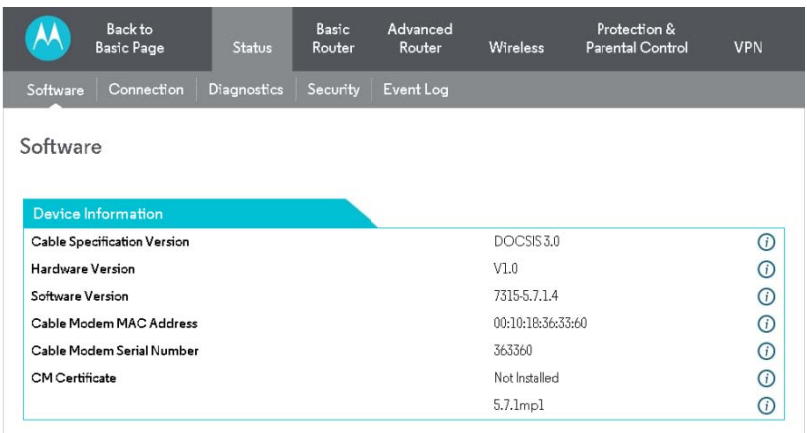

Figure 4 Software page

This page displays information about the hardware version, software version, MAC

address, cable modem IP address,serial number and CM Certificate status.

5.1.2 Connection

Choose **Status > Connection** and the following page appears.

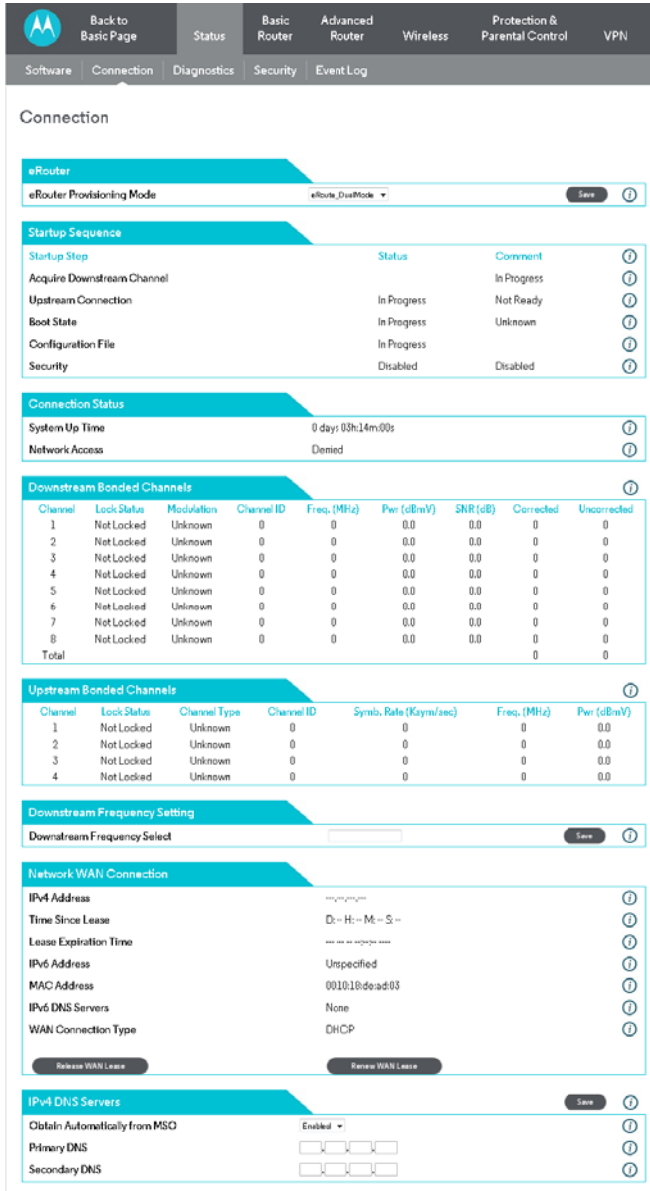
Back to Basic Page
Status
Basic Router
Advanced Router
Wireless
Protection & Parental Control
VPN
Software
Connection
Diagnostics
Security
Event Log
Connection
eRouter
eRouter Provisioning Mode
eRouter_DualMode
Save
Startup Sequence
Startup Step
Status
Comment
Acquire Downstream Channel
In Progress
Upstream Connection
In Progress
Not Ready
Boot State
In Progress
Unknown
Configuration File
In Progress
Security
Disabled
Disabled
Connection Status
System Up Time
0 days 03h:14m:00s
Network Access
Denied
Downstream Bonded Channels
Channel
Lock Status
Modulation
Channel ID
Freq. (MHz)
Pwr (dBmV)
SNR (dB)
Corrected
Uncorrected
1 Not Locked Unknown 0 0 0.0 0.0 0 0
2 Not Locked Unknown 0 0 0.0 0.0 0 0
3 Not Locked Unknown 0 0 0.0 0.0 0 0
4 Not Locked Unknown 0 0 0.0 0.0 0 0
5 Not Locked Unknown 0 0 0.0 0.0 0 0
6 Not Locked Unknown 0 0 0.0 0.0 0 0
7 Not Locked Unknown 0 0 0.0 0.0 0 0
8 Not Locked Unknown 0 0 0.0 0.0 0 0
Total 0 0
Upstream Bonded Channels
Channel
Lock Status
Channel Type
Channel ID
Symb. Rate (Ksym/sec)
Freq. (MHz)
Pwr (dBmV)
1 Not Locked Unknown 0 0 0 0.0
2 Not Locked Unknown 0 0 0 0.0
3 Not Locked Unknown 0 0 0 0.0
4 Not Locked Unknown 0 0 0 0.0
Downstream Frequency Setting
Downstream Frequency Select
Save
Network WAN Connection
IPv4 Address
Time Since Lease
D: -- H: -- M: -- S: --
Lease Expiration Time
IPv6 Address
Unspecified
MAC Address
0010:18:de:ad:03
IPv6 DNS Servers
None
WAN Connection Type
DHCP
Release WAN Lease
Renew WAN Lease
IPv4 DNS Servers
Save
Obtain Automatically from MSO
Enabled
Primary DNS
Secondary DNS

Figure 5 Connection information

This page displays information about the RF upstream and downstream channels, including downstream channel frequencies, upstream channel IDs, and upstream and downstream signal power and modulation.

This page also displays IP lease information, including the current IP address of the cable modem, the duration of both leases, the expiration time of both leases, and the current system time from the DOCSIS timeserver.

The information on this page can be refreshed at any time by clicking your web browser's Refresh button.

5.1.3 Diagnostics

Choose **Status > Diagnostics** and the following page appears.

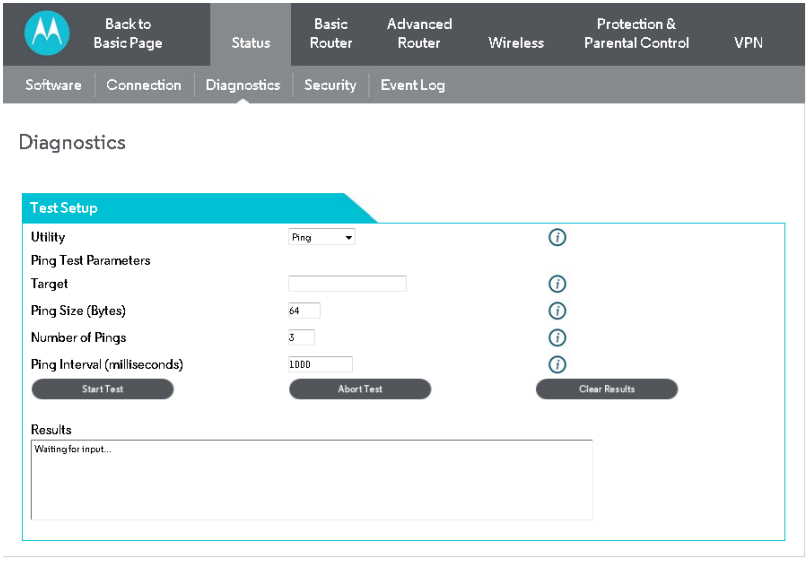

Figure 6 Diagnostic information

Two utilities are provided for troubleshooting network connectivity: Ping and Traceroute.

Ping allows you to check connectivity between the CM/RG and devices on the LAN.

Traceroute allows you to map the network path from the CM/RG to a public host. Selecting Traceroute from the drop-down Utility list will present alternate controls for the traceroute utility: To run either utility, make any changes to the default parameters and select Start Test to begin. The window will automatically be refreshed as the results are displayed in the Results table.

5.1.4 Security

Choose **Status > Security** and the following page appears.

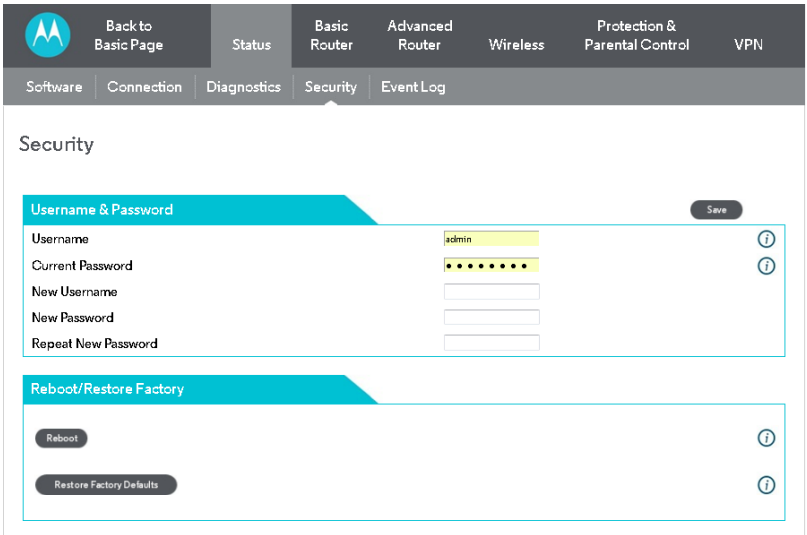

Figure 7 Security configuration

Restore Factory Defaults:

Click this button to restore factory defaults. Note that you will lose any settings you may have changed.

Note that you can also change the security password from this page by entering a new password in both the New Password and Re-Enter New Password fields, and the current password in the Current User ID Password field. Clicking Save will change the password. You do NOT have to restore factory defaults to change the password.

5.1.5 Event Log

Choose **Status > Event Log** and the following page appears.

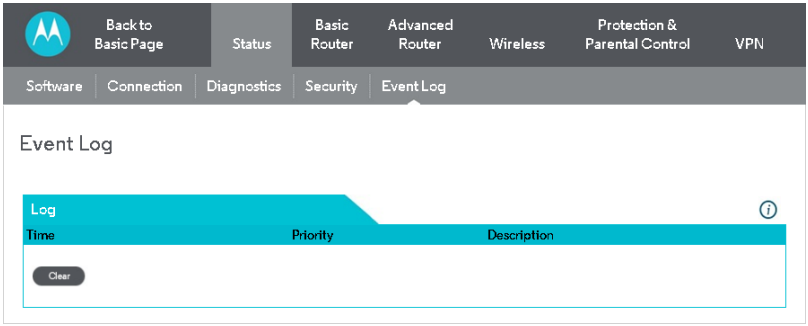

Figure 8 Event Log information

The Event Log displays information about your cable modem's connection to your service provider. This information may be particularly helpful if you experience problems with your connection.

5.2 Basic Router

Choose **Basic Router** and the submenus of **Basic Router** are shown as below.

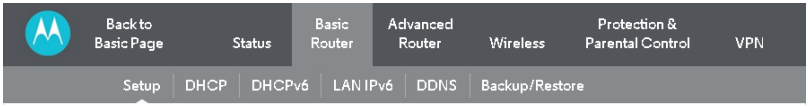

Figure 9 Submenus of Basic Router

5.2.1 Setup

Choose **Basic Router > Setup** , and the following page appears.

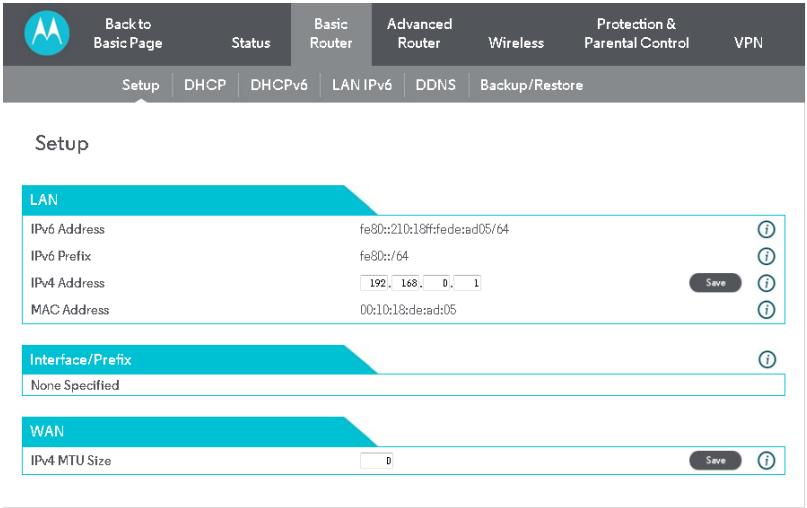

Figure 10 Setup configuration

Enter the information from the Required Information section as indicated:

At this point, the CM/RG is configured for basic use. To connect to the Internet, you must do the following:

1. Power up the CM/RG and wait for it to register with the CMTS and obtain an Internet-routable IP address

2. Get an IP lease from the internal DHCP server for each PC attached to the CM/RG.

Note that communication on the LAN will work regardless of whether the WAN connection provided by the cable modem is up. However, you will not be able to access the Internet until the WAN connection is enabled and has an IP address.

Some configurations settings are retrieved only once from non-volatile storage when the CM/RG first powers up. One such setting is changing the IPv4 Address parameters. Any changes to these settings will force the CM/RG to reset so that the new configuration can be read from non-volatile storage.

When this mandatory reset is required, the web interface will notify as follows:

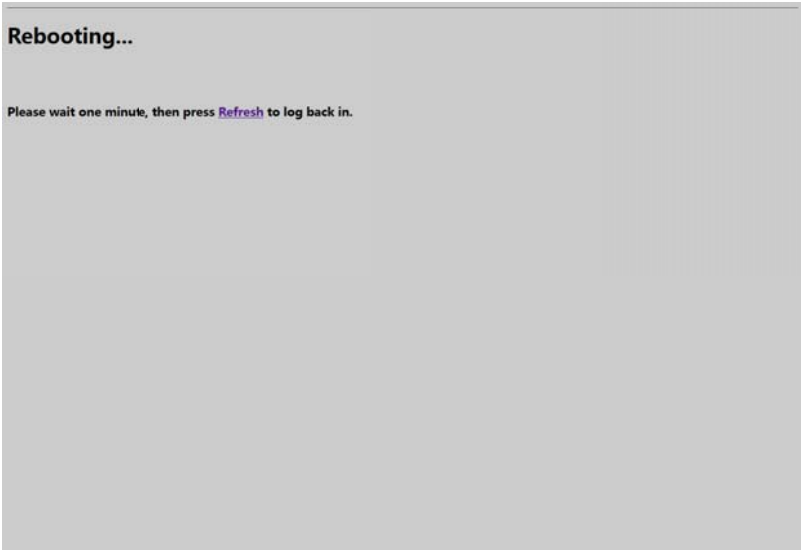

Figure 11 Reload page

Simply wait for the modem to reboot and click on the “Refresh” link to re-enter the web interface where you made your last change.

Most configuration items may be changed on the fly without a reboot.

5.2.2 DHCP

Choose **Basic Router > DHCP,** and the following page appears.

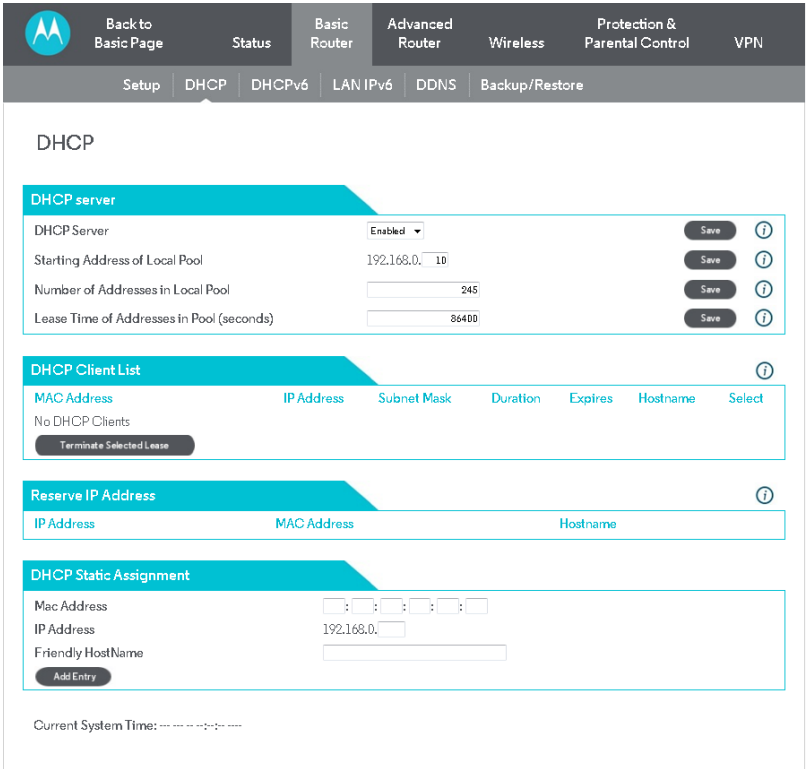

Figure 12 DHCP configuration

This page allows configuration and status of the optional internal DHCP server for the LAN.

If you have your own DHCP server servicing the LAN side (or choose to “hardcode” all of your PC’s IP addresses), you can disable the internal DHCP server by chose the Disabled. If you do this, make sure the IP address assigned to the CM/RG is on the same subnet as the external DHCP server (the subnet mask is always 255.255.255.0), or you won’t be able to access the CM/RG from the LAN. The IP address of the CM/RG can be set from the Basic Router Setup page.

You can also set the starting IP address for IP leases available to the LAN, and change the number of PCs supported on the LAN. In the case above, addresses

192.168.0.2 through 192.168.0.9 can be used as hard-coded IP addresses with no fear of IP address conflict with the DHCP pool. Configured WINS server addresses can also be passed to CPEs behind the CM/RG via DHCP.

5.2.3 DHCPv6

Choose **Basic Router > DHCPv6** , and the following page appears.

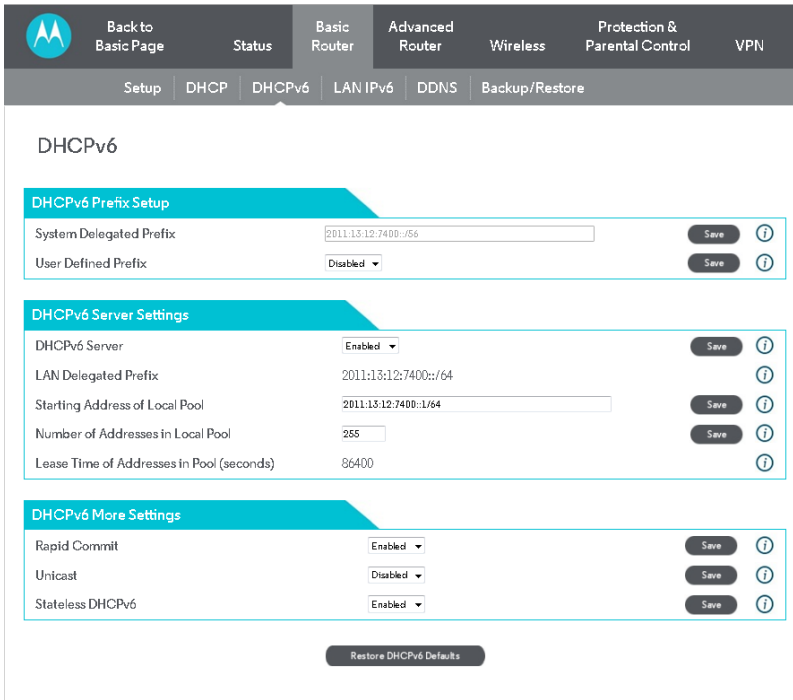

Figure 13 DHCPv6 configuration

This page allows configuration of the internal DhcpV6 server for the LAN. When modifying the System Delegated Prefix, set the System Delegated Prefix first, and press Save so that the system can calculate its LAN Delegated Prefix.

5.2.4 LAN IPv6

Choose **Basic Router> LAN IPv6** and the following page appears.

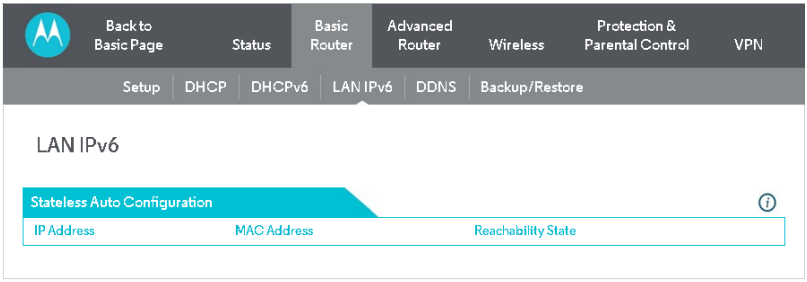

Figure 14 LAN IPv6 information

This page displays information related to IPv6 on the LAN.

5.2.5 DDNS

Choose **Basic Router > DDNS** , and the following page appears.

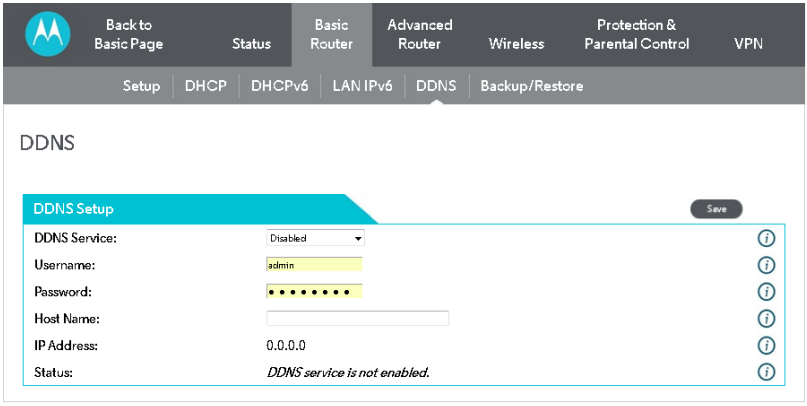

Figure 15 DDNS configuration

This page is used to configure DDNS. Dynamic DNS (DDNS) allows a dynamic IP address to be aliased to a static, pre-defined host name so that the host can be easily contacted by other hosts on the internet even if its IP address changes.

The CM/RG supports a dynamic DNS client compatible with the Dynamic DNS service (http://www.dyndns.com/).

To activate the DDNS client:

1. Go to the Dynamic DNS website and create an account for the Dynamic DNS service. You will create a username and password, and be asked to choose a host name for your server, and the dynamic DNS domain to which your host will be assigned. You will also be asked for your host's current IP address. This is the WAN IP address that has been assigned to your CM/RG during provisioning. (See WAN IP Address on the Basic Router/ Setup web page.)
2. Enter your account information on the Basic Router/ DDNS web page, enable the service by selecting www.DynDNS.org from the DDNS Service drop-down list, and click Save.
3. The DDNS client will notify the DDNS service whenever the WAN IP address changes so that your chosen host name will be resolved properly by inquiring hosts. The current status of the service is shown at the bottom of the DDNS web page.

5.2.6 Backup/Restore

Choose **Basic Router > Backup/Restore** and the following page appears.

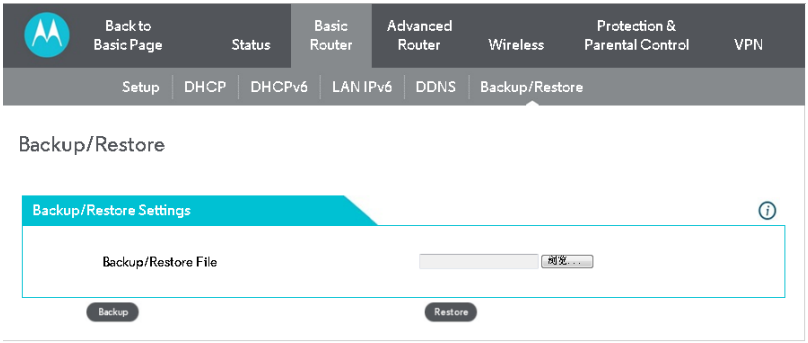

Figure 16 Backup/Restore setup

In this page, you can save the current CM/RG configuration settings to a local PC. You can then later restore these settings if you need restore a particular

configuration, or to recover from changes you may have made that have had an undesirable effect.

To back up the current configuration, click Backup and follow the prompts.

To restore a previous configuration, click Browse and use the navigation window to locate the file. (Usually GatewaySettings.bin, unless you rename it before saving.) Once the file has been located, click Restore to restore the settings. Note that once the settings are restored, the device will reboot.

5.3 Advanced Router

Choose **Advanced Router** and the submenus of **Advanced Router** are shown as below.

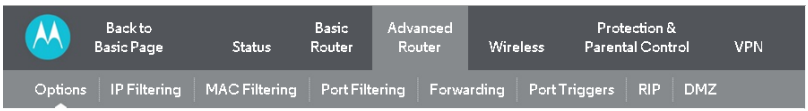

Figure 17 Submenus of Advanced Router

5.3.1 Options

Choose **Advanced Router > Options** to display the following page.

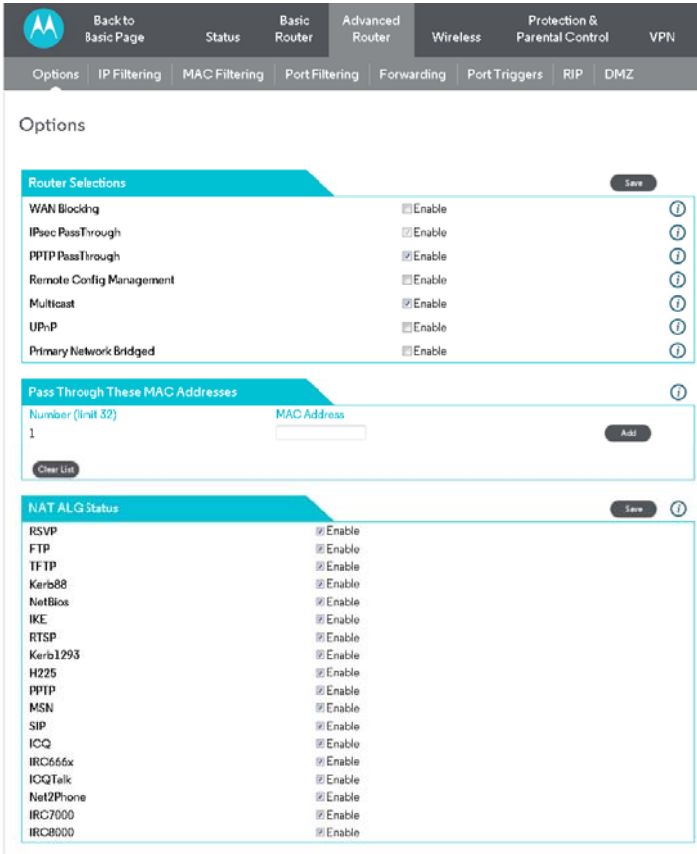

Figure 18 Options configuration

This page allows you to configure the accessible features.To enable a feature, click the appropriate check box until it is “checked”. When you are satisfied with your selections, click on the Save button. These features can be modified on the fly without a system reset.

WAN Blocking prevents your cable modem/router or the devices behind it from being visible from the Internet. This makes it difficult for hackers to discover your WAN IP address and launch an attack on your private LAN.

IpSec PassThrough enables a VPN device or VPN software located behind your cable modem/router and running IpSec to communicate successfully with endpoints on the Internet.

PPTP (Point-to-Point Tunneling Protocol) PassThrough enables a VPN device or VPN software located behind your cable modem/router and running PPTP to communicate successfully with endpoints on the Internet.

Remote Config Management: When enabled, navigate to http://‹CM WAN IPAddress›:8080/ to administer your Cable Modem/Router remotely. You can find your Cable Modem/Router's WAN IP address on the Basic Setup page. Multicast :Allows multicast specific traffic to be passed to and from the PCs on your LAN behind your Cable Modem/Router

UPnP: If you are running an application that requires UPnP, Enable UPnP.

Primary Network Bridged: Enable or Disable the feature Pass Through These MAC Addresses.

5.3.2 IP Filtering

Choose **Advanced Router> IP Filtering** to display the following page.

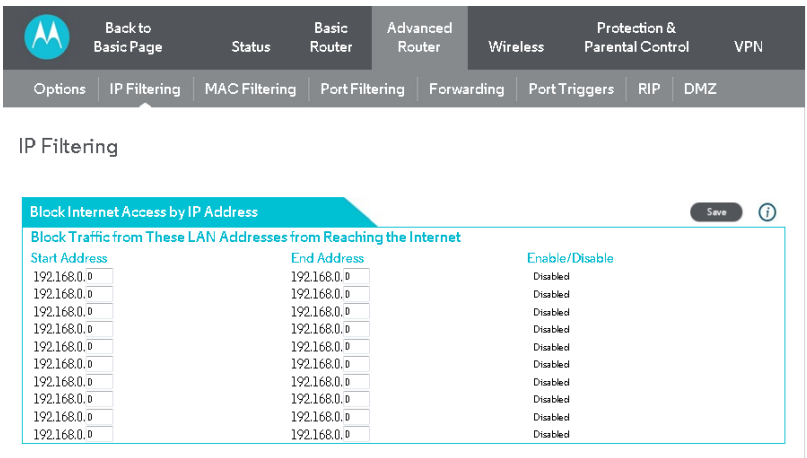

Figure 19 IP Filtering configuration

This page allows you to configure the CM/RG to prevent local PCs from getting access to the WAN by specifying those IP addresses that should be filtered.

By entering starting and ending IP address ranges, you can configure which local PCs are denied access to the WAN. Note that you only need to enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the CM/RG IP address. To activate the IP address filter, you must also check the “enable” box and click Save. The enable box allows you to store filter settings commonly used but not have them active.

5.3.3 MAC Filtering

Choose **Advanced Router > MAC Filtering** to display the following page.

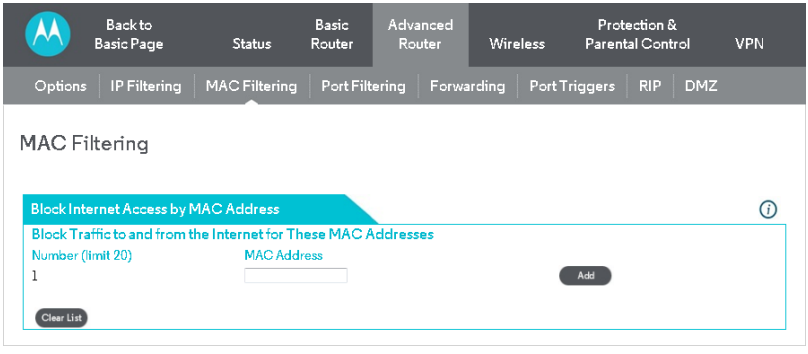

Figure 20 MAC Filtering configuration

This page is used to prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC address

This is useful for the fact that the MAC address of a specific NIC card never changes, unlike its IP address which can be assigned via DHCP server or hard-coded to various addresses over time.

5.3.4 Port Filtering

Choose **Advanced Router> Port Filtering** to display the following page.

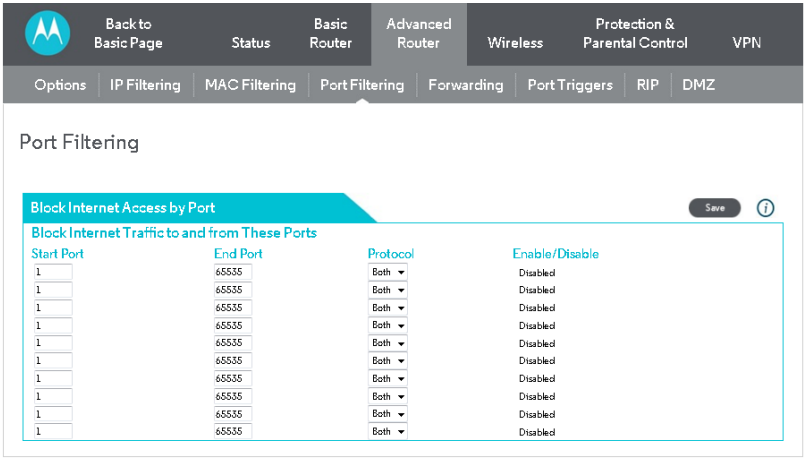

Figure 21 Port Filtering configuration

This page is used to prevent PCs from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers.

By specifying a starting and ending port range, you may determine what TCP/UDP traffic is allowed out to the WAN on a per-port basis. Note the specified port ranges are blocked for ALL PCs and this setting is not IP address or MAC address specific. For instance, if you would like to block all PCs on the private LAN from accessing HTTP sites (or “web surfing”), you would set the “Start Port” to 80, the “End Port” to 80, the “Protocol” to TCP, check the “Enabled” box, and click Save.

5.3.5 Forwarding

Choose **Advanced Router > Forwarding** to display the following page.

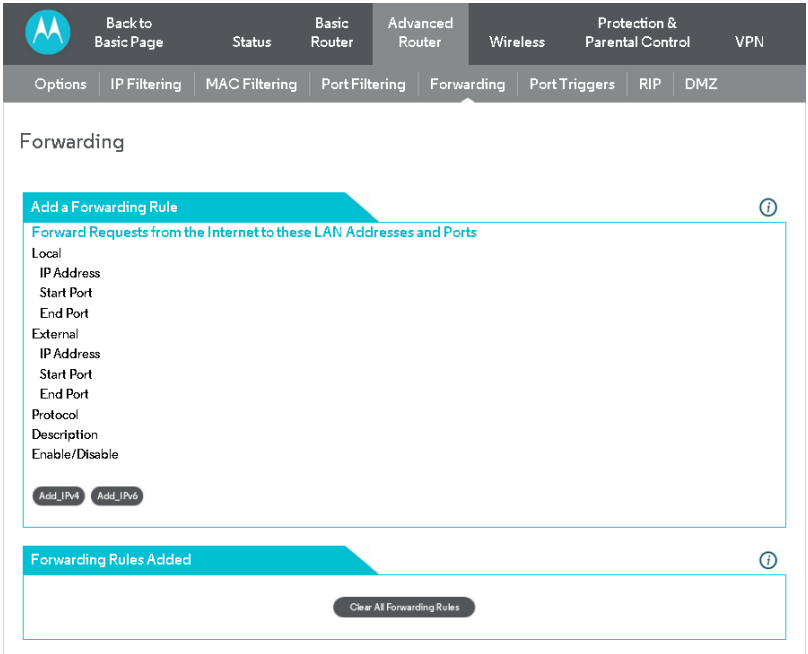

Figure 22 Forwarding configuration

This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Forwarding allows you to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC

To specify a mapping, you must enter the range of port numbers that should be forwarded locally, and the IP address to which traffic to those ports should be sent. If only a single port specification is desired, enter the same port number in the “start” and “end” locations for that IP address. A table of commonly used Port numbers is supplied on the page for convenience.

If both external and Local/internal port numbers are present, the Local port number is a mandatory field and the external port number is optional. If the external port number is used, the RG will perform a translation from external port number to internal port number.

5.3.6 Port Triggers

Choose **Advanced Router > Port Triggers** to display the following page.

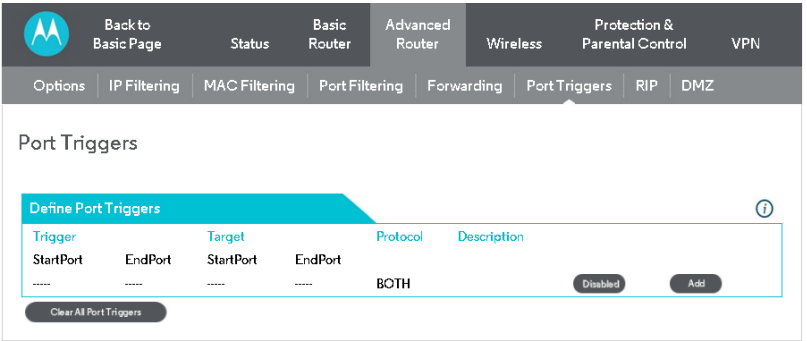

Figure 23 Port Triggers configuration

Port Triggers are similar to Port Forwarding except that they are not static ports held open all the time. When the CM/RG detects outgoing data on a specific IP port number set in the “Trigger Range”, the resulting ports set in the “Target Range” are opened for incoming (or sometimes referred to as bi-directional ports) data. If no outgoing traffic is detected on the “Trigger Range” ports for 10 minutes, the “Target Range” ports will close. This is a safer method for opening specific ports for special applications (e.g. video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.

5.3.7 RIP Setup

Choose **Advanced Router> RIP Setup** to display the following page.

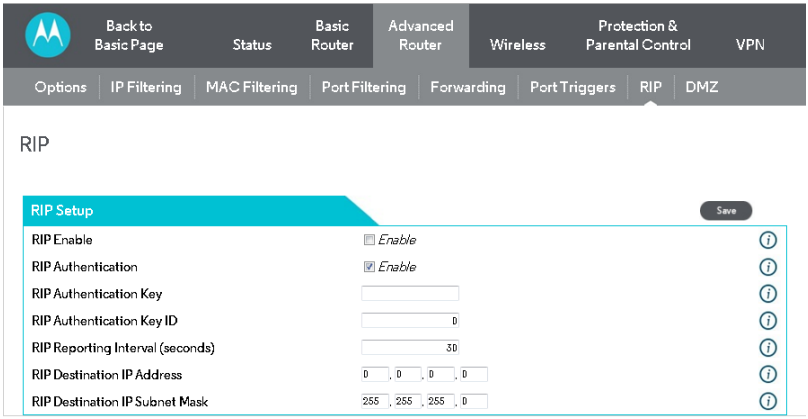

Figure 24 RIP configuration

RIP (Router Information Protocol) is used in WAN networks to identify and use the best known and quickest route to given destination addresses to help reduce network congestion and delays.

NOTE: RIP messaging will only be sent upstream when running in Static IP Addressing mode on the Basic – Setup page. You must enable Static IP Addressing and the set the Wan IP network information! RIP is normally a function that is tightly controlled via the ISP. RIP Authentication Keys and IDs are normally held as secret information from the end user to prevent unauthorized RIP settings.

RIP is a protocol that requires negotiation from both sides of the network (i.e. CM/RG and CMTS). The ISP would normally set this up because of their knowledge of their CMTS settings to match the configuration in the CM/RG.

To enable the CM/RG to perform RIP, do the following (this example uses BRCMV2 as the RIP Authentication Key and 1 as the Key ID):

1.) To turn on RIP MD5 Authentication, check the “Enable” box.

2.) To specify a RIP MD5 Authentication Key String, type “BRCMV2” for this example.

key name = a string value to match CMTS key name value

3.) To specify a RIP MD5 Auth Key ID, type “1”

key number = a number to match the CMTS key number value

4.) To change the RIP annoucement interval, type in a number in seconds.reporting interval by default = 30 seconds

5.) To specify a RIP unicast destination IP address, enter the IP address and subnet mask.

To enable the CMTS for RIPv2 with MD-5 authentication (Cisco uBR example shown below):

1.) The following steps go through configuring RIPv2 for a Cisco CMTS. The network number used in this configuration will vary from network to network so use the network number that matches your set-up.

```
7223#configure terminal
7223(config)#key chain ubr
7223(config-keychain)#key 1
7223(config-keychain-key)#key-str BRCMV2
7223(config-keychain-key)#exit
7223(config-keychain)#exit
7223(config)#router rip
7223(config-router)#ver 2
7223(config-router)#no validate-update
7223(config-router)#passive-interface cable 2/0
7223(config-router)#network 10.0.0.0
7223(config-router)#exit
7223(config)#inter cable 2/0
7223(config-if)#ip rip receive ver 2
7223(config-if)#ip rip authentication mode md5
7223(config-if)#ip rip authentication key-chain ubr
7223(config-if)#exit
7223(config)#exit
```

In this example, we have named the key chain ‘ubr’. This was chosen arbitrarily. You can use any name you like as long as you specify the correct name when specifying which key chain to use for RIPv2 authentication.

2.) The next step is enable RIP debugging to ensure that the CMTS is receiving and authenticating messages from the residential gateway.

```
7223#debug ip rip
RIP protocol debugging is on
```

7223#term mon

The CMTS is now configured to accept RIPv2 messages. If the CM/RG is registered on the CMTS, you should see messages that are similar to the message below:

00:28:41: RIP: received packet with MD5 authentication

00:28:41: RIP: received v2 update from 10.24.81.148 on Cable2/0

00:28:41: 10.24.81.0/24 via 10.24.81.148 in 1 hops

The CM/RG has broadcast that is connected to the network 10.24.81.0/24 through the interface 10.24.81.148. This information is not very useful to the CMTS because it already knows that the network 10.24.81.0/24 is connected directly to one of its interfaces (Cable2/0). It ignores this message and doesn't add any information to the IP routing table. Here is the IP routing table after the CMTS has received RIPv2 messages:

7223#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 10.24.95.17 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.24.80.0/24 is directly connected, Cable2/0

C 10.24.81.0/24 is directly connected, Cable2/0

C 10.24.95.16/28 is directly connected, FastEthernet0/0

S* 0.0.0.0/0 [1/0] via 10.24.95.17

In the example above, the CM/RG was set up to send RIPv2 messages to the CMTS. The CMTS was also set up to receive these messages.

5.3.8 DMZ Host

Choose **Advanced Router > DMZ Host** to display the following page.

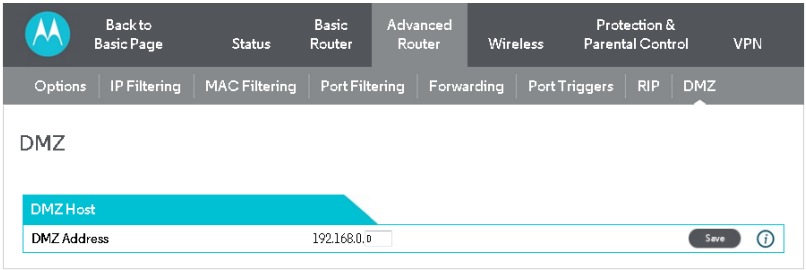

Figure 25 DMZ Host configuration

DMZ (De-militarized Zone) hosting (also commonly referred to as “Exposed Host”) allows you to specify the “default” recipient of WAN traffic that NAT is unable to translate to a known local PC. This can also be described as a computer or small sub-network that sits between the trusted internal private LAN, and the untrusted public Internet.

You may configure one PC to be the DMZ host. This setting is generally used for PC’s using “problem” applications that use random port numbers and do not function correctly with specific port triggers or port forwarding setups mentioned earlier. If a specific PC is set as a DMZ Host, remember to set this back to “0” when finished with the needed application, since this PC will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the Firewall.

5.4 Wireless

Choose **Wireless** and the submenus of **Wireless** are shown as below.

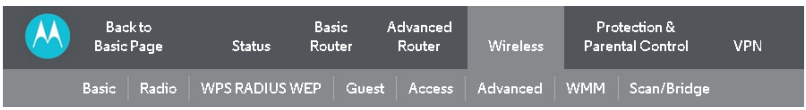

Figure 26 The submenus of Wireless

5.4.1 Basic

Choose **Wireless > Basic** to display the following page.

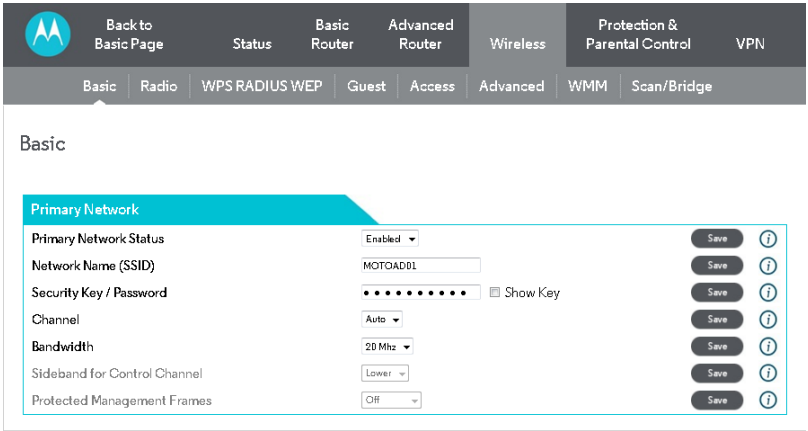

Figure 27 Basic configuration

This page allows you to configure the Primary Wireless Network.

Primary Network:

Enable or Disable the primary network. Guest networks may still be operational when the primary network is disabled.

Network Name (SSID):

Sets the Network Name (also known as SSID) of the primary network.This is a 1-32 ASCII character string.

WPA-PSK / WPA2-PSK Security Key / Password:

Motorola assigned your device a unique Security Key (or Password) at the factory. This security key is displayed here.

If you want, you can change the security key by entering the new key here and then clicking the Save button. **Channel:**

Selects the control channel for AP operation.The list of available channels depends on the selected country as presented in.

Bandwidth:

802.11b/g channels are only 20 MHz wide, but 802.11n channels may be 40 MHz wide. There are some backward compatibility issues with 40 MHz channels though. These issues are more likely to be encountered in the 2.4 GHz band where legacy (802.11b/g) devices may be operating using 20 MHz channels.

Sideband for Control Channel (40 MHz only):

Whether the 20 MHz control channel uses the upper or lower half of the 40 MHz channel. Changes to this setting may change the control channel setting. For example (in the 2.4 GHz band), if the upper 20 MHz is selected as the sideband for the control channel, then the lowest control channel available would be channel 5 to allow the lower 20 MHz for data.

5.4.2 Radio

Choose **Wireless > Radio** to display the following page.

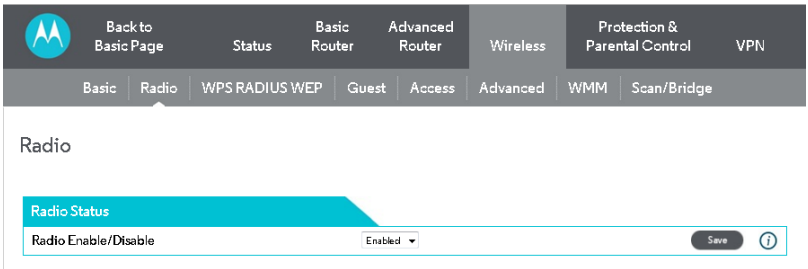

Figure 28 Radio configuration

Radio Enable/Disable:

Allows the wireless interface to be enabled and disabled.

5.4.3 WPS_RADIUS_WEP

Choose **Wireless > WPS_RADIUS_WEP** to display the following page.

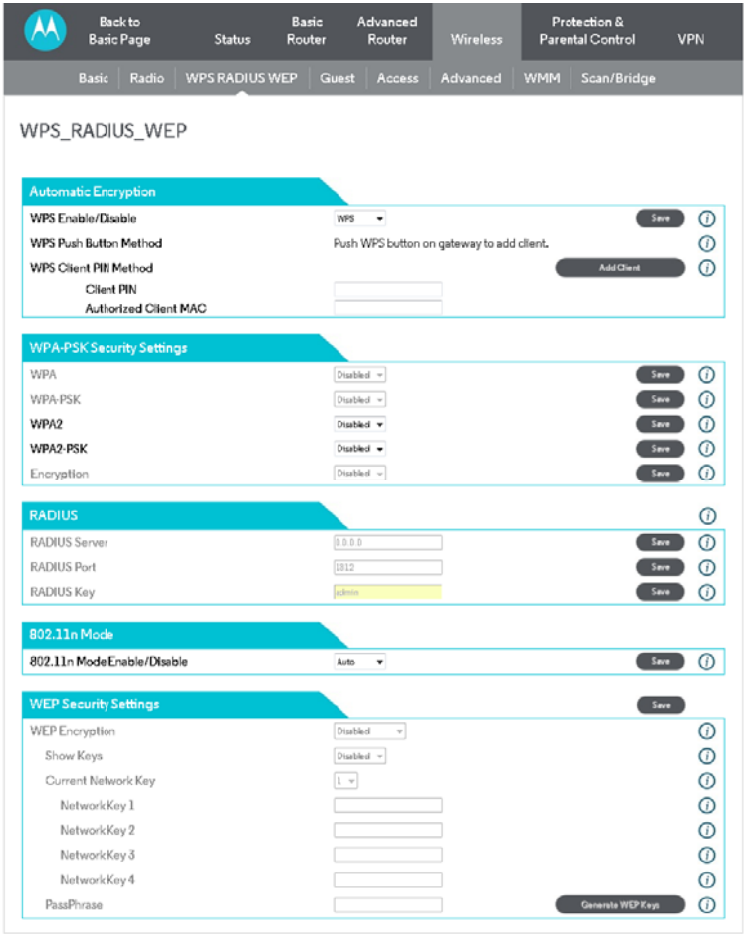

Figure 29 WPS_RADIUS_WEP configuration

This page allows you to configure the WPS_RADIUS_WEP

WPS Enable/Disable:

WPS stands for Wi-Fi Protected Setup. WPS provides two methods to automatically distribute wireless keys to clients that support this feature, described below. For the record, as of July, 2015, Apple devices did not support WPS.

WPS Client PIN Method:

On your client device, run a utility to generate a WPS PIN.

Copy the PIN that the client generates and enter it here, then press the Save button. Once this process is complete, your cable modem/router will display the results, or it will time out after about two minutes.

Note that this method will change the default SSID and key for your network.

WPA:

Wi-Fi Protected Access is a slightly older and less secure algorithm for securing a wireless network. This is the Enterprise variant that requires configuration of a RADIUS server.

WPA-PSK:

The Pre-Shared Key mode of the WPA algorithm which does not require use of a RADIUS server. This is also known as WPA Personal. WPA and WPA-PSK cannot be used at the same time.

WPA2:

An advanced form of WPA that is more secure. This is the Enterprise mode of WPA2 which requires the use of a RADIUS server. WPA2 and WPA may be used at the same time to provide backward compatibility with devices that do not support WPA2.

WPA2-PSK:

The Pre-Shared Key mode of WPA2, also known as WPA2 Personal.WPA2 and WPA2-PSK cannot be used at the same time. WPA2-PSK and WPA-PSK may be used at the same time to provide backward compatibility with devices that do not support WPA2.

Encryption:

Select the desired encryption protocol for your network. The default is TKIP+AES**.**

RADIUS:

Disable WPA-PSK / WPA2-PSK and Enable WPA / WPA2 to un-gray out RADIUS settings.

802.11n Mode:

Set this parameter to OFF to force 802.11g mode (required to enable WEP). The default value is Auto.

WEP Encryption:

Disabled and grayed out by default. If you need WEP Encryption, set 802.11n Mode to OFF to un-gray out, and then Enable this parameter.

Network Key 1 thru Network Key 4:

When WEP encryption is enabled, sets the static WEP keys. Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key. Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

Current Network Key:

This selects the Network Key used for transmissions. Select 1 - 4 (default 1).

PassPhrase:

Enter a 10 or 26 character string, then press Generate WEP Keys to generate Network Keys 1 - 4.

5.4.4 Guest

Choose **Wireless > Guest** to display the following page.

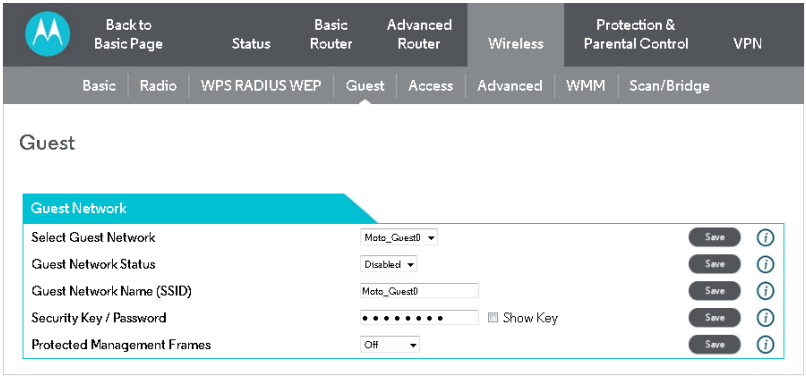

Figure 30 Guest configuration

The page allows you to configure a secondary guest network on the wireless interface.

Select Guest Network:

This is a pulldown of Moto_Guest0 to Moto_Guest7.

Guest Network Status:

Enable or Disable the Guest Network selected above.

Guest Network Name (SSID):

Either accept the default Network Name, or change the name by entering the new name here, and clicking the Save button.

WPA-PSK / WPA2-PSK Security Key / Password:

Enter a key here, and click the Save button to save it.

5.4.5 Access

Choose **Wireless > Access** to display the following page.

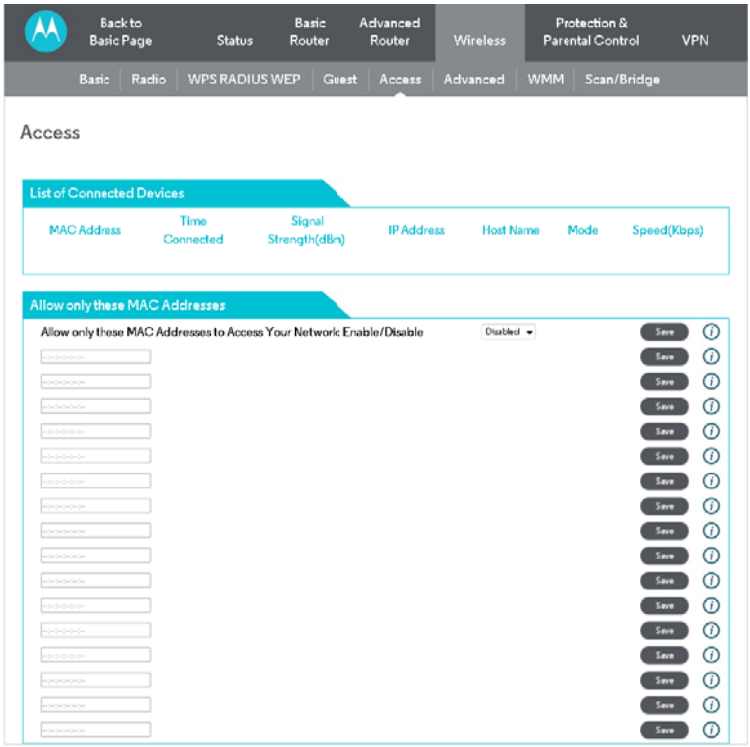

Figure 31 Access configuration

This page allows you to control which wireless clients can access your wireless network. It also provides information about wireless clients connected to your access point.

Connected Clients:

A list of connected wireless clients. When a client connects (associates) to the network, it is added to the list; when a client leaves (disassociates) from the network, it is removed from the list. For each client, the age (in seconds), estimated average receive signal strength (in dBm), IP address, and host name are presented. The age is the amount of time elapsed since data was transmitted to or received from the client.

5.4.6 Advanced

Choose **Wireless > Advanced** to display the following page.

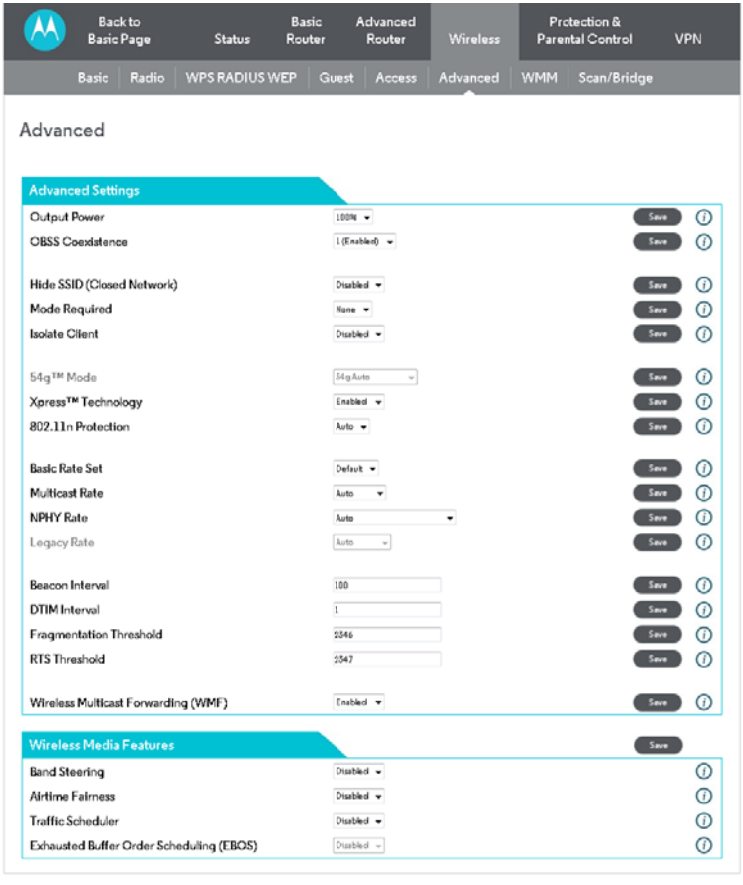

Figure 32 Advanced configuration

This page allows you to configure advanced wireless settings.

Output Power:

Control the range of the AP by adjusting the radio output power.

OBSS Coexistence:

OBSS coexistence refers to the ability of your device to support 20 MHz clients within 40 MHz channels. It also allows your device to reduce interference from nearby 20 MHz devices that are interfering with part of your device's 40 MHz channel.

Hide SSID (Closed Network):

When this feature is enabled, the SSID is not broadcast. Therefore, only devices that already know the SSID will be able to connect.

Mode Required:

Select None, HT or ERP, where HT and ERP refer to High Throughput and Extended Rate PHY, respectively. These settings determine how your network interacts with older (802.11b/g) and newer (802.11n) wireless clients. Most users will leave this at the default setting of None.

Isolate Client:

When this feature is enabled, wireless clients are isolated from your wired network and from each other. They can only access the Internet, but not any servers or other devices on your network.

54g™ Mode:

Sets the network mode for legacy 802.11g & 802.11b networks. To un-gray out this selection, under the 2.4GHz tab in WPS_RADIUS_WEP, Disable 802.11n Mode.

Choices are 54g Auto, 54g only, 54g Performance, 54g LRS, and 802.11b Only. 54g Auto accepts 54g, 802.11g, and 802.11b clients, but optimizes performance based on the type of clients connected. 54g Performance accepts only 54g™ clients and provides the highest throughout; nearby 802.11b networks may have degraded performance. 54g LRS interoperates with the widest variety of 54g™, 802.11g, and 802.11b clients. 80211b accepts only 802.11b clients.

Xpress Technology:

Enable Broadcom proprietary method of block frame acknowledgement for 802.11g frames. This feature may improve throughput, but may cause problems.

Afterburner Technology

This feature removes the need for the acknowledgement of data frames. It may improve throughput, but may cause problems.

802.11n Protection:

802.11n Protection protects legacy 802.11b&g devices that are within range of your cable modem/router. This feature is enabled (**Auto**) by default.

In some environments with no legacy devices, you may improve performance by disabling this feature.

Basic Rate Set:

Determines which rates are advertised as “basic” rates. Default uses the driver defaults. Sets all available rates as basic rates.

Multicast Rate:

This is the rate at which you send out multicast packets to stations. Multicast packets are not acknowledged.

NPHY Rate:

Choose 802.11n rate to be applied to all unicast packets.

Legacy Rate:

“N” mode must be off on the “radio” webpage for this control to be active. When active the user can force the rate in which the AP will operate.

Beacon Interval:

Sets the beacon interval in milliseconds for the AP. The default is 100, which is fine for nearly all applications.

DTIM Interval:

Sets the wakeup interval for clients in power-save mode. When a client is running in power save mode, lower values provide higher performance but result in decreased client battery life, while higher values provide lower performance but result in increased client battery life.

Fragmentation Threshold:

Sets the fragmentation threshold. Packets exceeding this threshold will be fragmented into packets no larger than the threshold before packet transmission.

RTS Threshold:

Sets the RTS threshold. Packets exceeding this threshold will cause the AP to perform an RTS/CTS exchange to reserve the wireless medium before packet transmission.

Wireless Multicast Forwarding (WMF):

Multicast involves sending the same packets to two or more endpoints, for example of a video stream.

5.4.7 WMM

Choose **Wireless > WMM** to display the following page.

Figure 33 WMM configuration

This page allows you to configure WiFi Multi-Media (WMM). WMM is an implementation of Quality of Service (Qos) which is defined by the IEEE standard 802.11e.

WMM Support:

Sets WMM support. Choices are Auto, On, or Off. If enabled (Auto or On), the WME Information Element is included in beacon frame.

No-Acknowledgement:

Sets No-Acknowledgement support. Choices are On or Off. When enabled, acknowledgments for data are not transmitted.

Power Save Support:

Sets Power Save support. Choices are On or Off. When Power Save is enabled, the AP queues packets for STAs that are in power-save mode. Queued packets are transmitted when the STA notifies AP that it has left power-save mode.

EDCA AP Parameters:

Specifies the transmit parameters for traffic transmitted from the AP to the STA for the four Access Categories: Best Effort (AC_BE), Background (AC_BK), Video (AC_VI), and Voice (AC_VO). Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).

There are also two AP-specific settings: Admission Control and Discard Oldest First. Admission control specifies if admission control is enforced for the Access Categories. Discard Oldest First specifies the discard policy for the queues. On discards the oldest first; Off discards the newest first.

EDCA STA Parameters:

Specifies the transmit parameters for traffic transmitted from the STA to the AP for the four Access Categories: Best Effort (AC_BE), Background (AC_BK), Video (AC_VI), and Voice (AC_VO). Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).

5.4.8 Scan/Bridging

Choose **Wireless > Scan/Bridging** to display the following page.

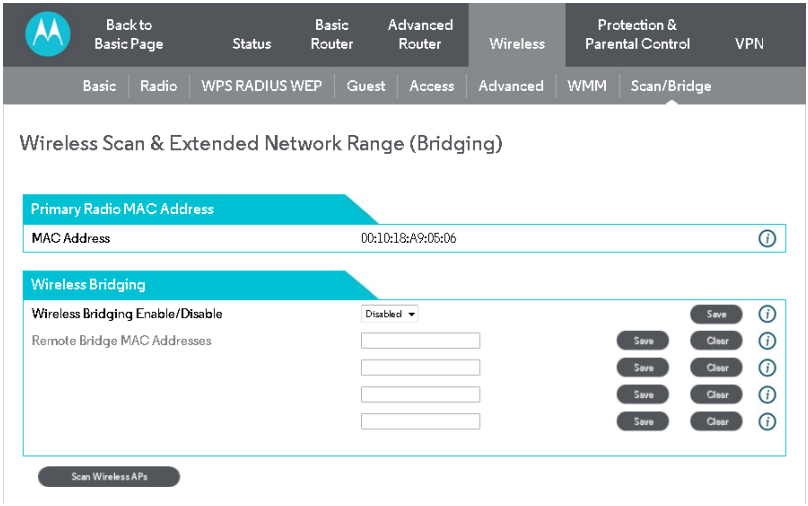

Figure 34 Scan/Bridging configuration

This page allows you to configure wireless bridging, which is also known as Wireless Distribution System (WDS). Bridging allows you connect multiple wireless access points together to form a single network using wireless point-to-point links.

Wireless Bridging:

This setting enables or disables wireless bridging.

Remote Bridges:

Table of remote bridge MAC addresses authorized to establish a wireless bridge. Up to 4 remote bridges may be connected. Typically, you will also have to enter your AP's MAC address (see section 0) on the remote bridge, too.

5.5 Protection & Parental Control

Choose **Protection & Parental Control** and the submenus of **Protection & Parental Control** are shown as below.

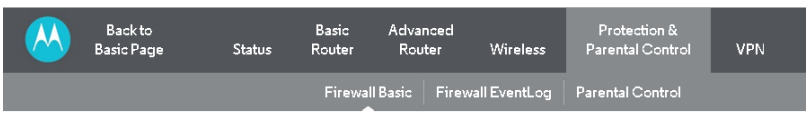

Figure 35 submenus of Protection & Parental Control

5.5.1 Firewall Basic

Choose **Protection & Parental Control> Firewall Basic** to display the following page.

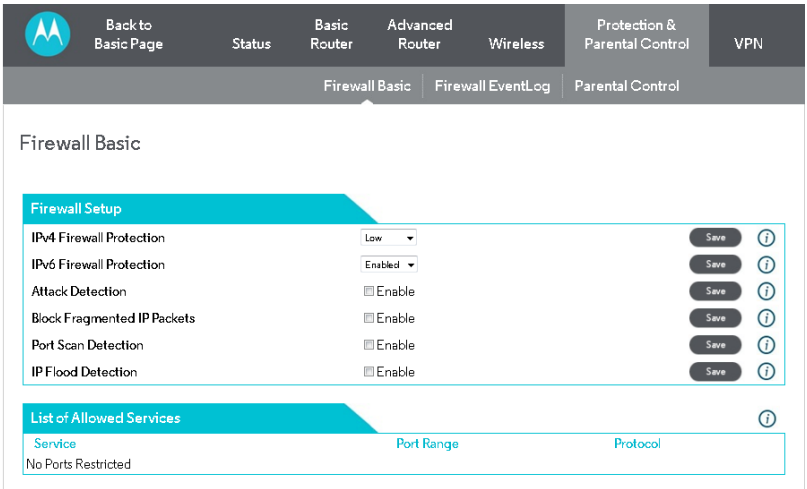

Figure 36 Firewall Basic configuration

This page is used to block or exclusively allow different types of data through the CM/RG from the WAN to the LAN.

The “low” setting does not block any services/ports, however it does protect against invalid packets and well known attacks. The “medium” setting will cause the firewall to drop a packet unless it is on a specific port of allowed services; the allowed services are listed on the same page. The “high” setting is similar to “medium”, but allows access to even fewer services. The “off” setting allows all traffic to pass.

Block Fragmented IP packets prevent all fragmented IP packets from passing through the firewall. Port Scan Detection detects and blocks port scan activity originating on both the LAN and WAN. IP Flood Detection detects and blocks packet floods

originating on both the LAN and WAN. The Save button must be clicked in order to activate any of the checkbox items. All of these settings can be activated on-the-fly without a CM/RG reboot.

5.5.2 Event Log

Choose **Protection & Parental Control >Firewall Event Log** to display the following page.

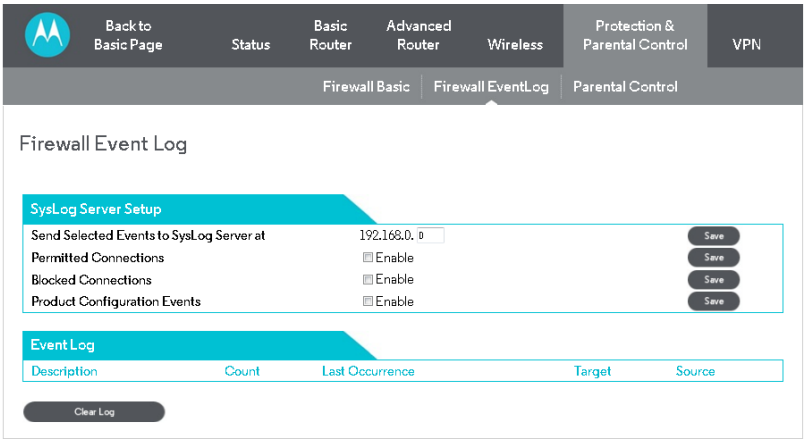

Figure 37 Firewall Event Log configuration

Configure the router to log a record of events to a local Syslog server on your LAN, and/or set up email alerts to warn of the events. First, select the events that you want logged and/or you want to be warned about. Second, enter the address of your local Syslog server, if you have one. Third, enter the email address and SMTP information where you want warnings to be sent, if applicable. Finally, click Save for the settings to take effect. Note that you can view the most recent entries of the log information you have selected at the bottom of the page.

5.5.3 Parental Control

Choose **Protection & Parental Control > Parental Control** to display the following page.

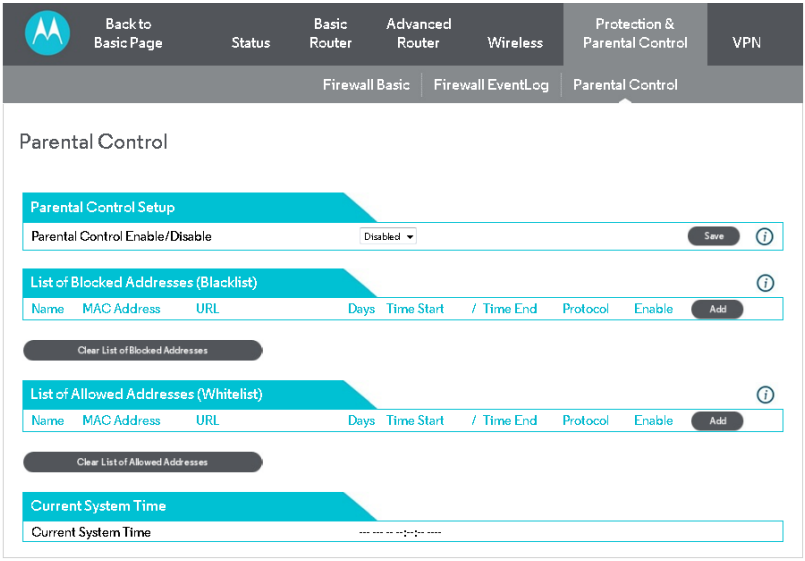

Figure 38 Parental Control configuration

Parental Control: Parental Control lets you define lists of blocked or allowed addresses. If you define Blocked addresses for particular devices on your network, those devices can reach all websites except the Blocked addresses. If you define Allowed Addresses for particular devices on your network, those devices can reach only the Allowed Addresses.

List of Blocked Addresses: Enter the MAC Address of the device whose access you want to block to a particular site. (Check the user documentation for the device if you need help finding its MAC Address). Then enter the URL of the web site whose access you want to block. Next, if you want to block access only during certain times enter the days and start and end times of the blocking. Next, enter the Protocols to block (choose both if you're not sure). Finally, select Enable and click Save to activate

the entry.

Note that you can Disable the entry temporarily if you may want to re-Enable it later.

List of Allowed Addresses: Enter the MAC Address of the device you want to allow access to a particular site. (Check the user documentation for the device if you need help finding its MAC Address). Then enter the URL of the web site whose access you want to allow. Next, if you want to allow access only during certain times enter the days and start and end times of the access. Next, enter the Protocols to allow (choose both if you're not sure). Finally, select Enable and click Save to activate the entry.

Note that you can Disable the entry temporarily if you may want to re-Enable it later.

5.6 VPN

Choose **VPN** and the submenus of **VPN** are shown as below.

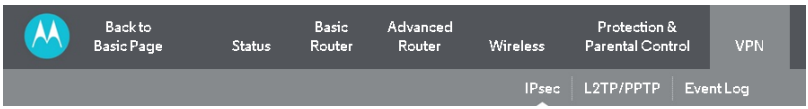

Figure 39 Submenus of VPN

5.6.1 IPSec

Choose **VPN > IPSec** to display the following page.

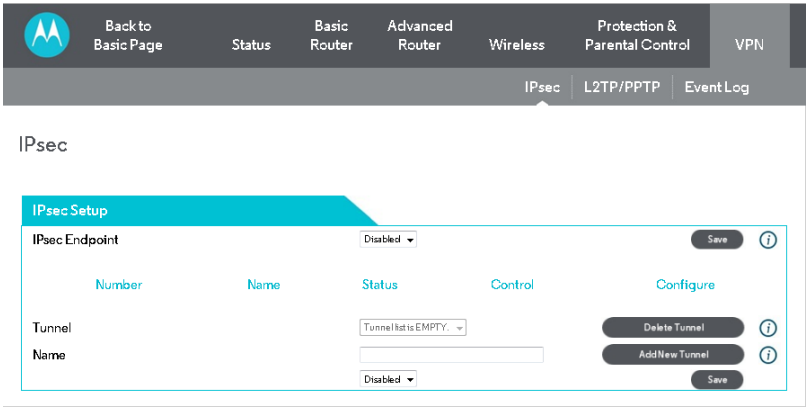

Figure 40 IPSec configuration

This page will show the status of configured tunnels.

Tunnel:

This is a pull-down list of VPN Names defined below. Select the specific VPN tunnel to configure.

Name:

Enter a VPN name and click Add New Tunnel.

5.6.2 L2TP/PPTP

Choose **VPN > L2TP/PPTP** to display the page below.

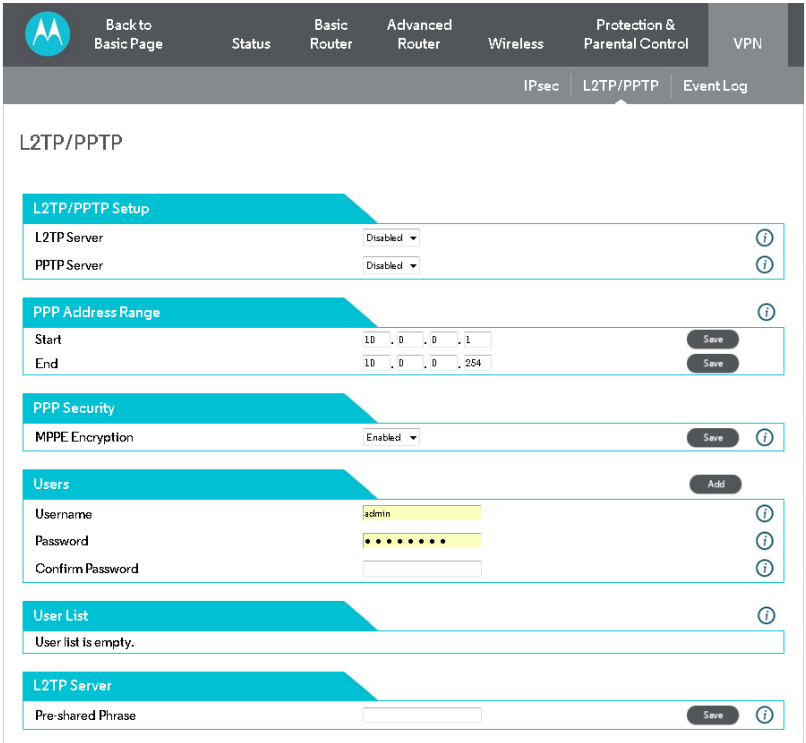

Figure 41 L2TP/PPTP configuration

This page allows configuration of L2TP and PPTP server options.

5.6.3 Event Log

Choose **VPN > Event Log** to display the following page.

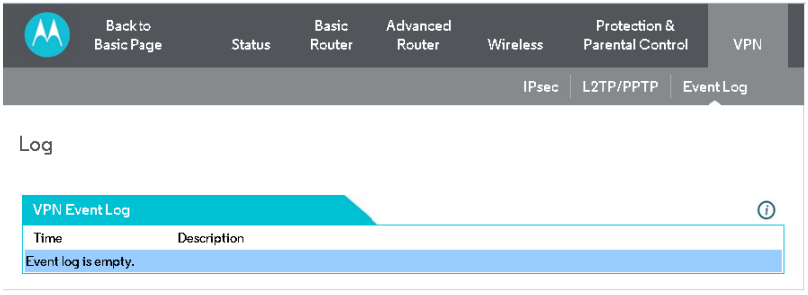

Figure 42 Event Log information

This page allows you to view the VPN Event Log.

5.7 Logout

Choose **Logout** to logout Account and the following page will be shown after logout.

Figure 43 The logout page

6 Q&A

(1) **Q**: Why all the indicators are off?

A: Check the following:

- The connection between the power adaptor and the power socket.
- The status of the power switch.

(2) **Q**: Why the **Ethernet** indicator is off?

A: Check the following:

- The connection between the Cable Modem and your computer, hub, or switch.
- The running status of your PC, hub, or switch.

(3) **Q**: Why the **ONLINE** indicator is off?

A: Check CM DS/US LED is on. Check the connection between the Cable Line and the wall HFC.

Apply customer :

Name: MTRLC LLC

Address: PO Box 121147 Boston, MA 02112-1147

Contact Person: Andy Pollock

Title: Director of Hardware Engineering

Telephone: 6177530663

Fax: 617-423-1075

For applicable power supplies :

1, US: S24B72-120A200-C4

Brand : Shenzhen Gongjin Electronics Co., Ltd

FCC statement

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

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

"FCC RF Radiation Exposure Statement Caution: To maintain compliance with the FCC's RF exposure guidelines, place the product at least 20cm from nearby persons."

keep 20cm away warning :
FCC Radiation Exposure Statement for Mobile Devices
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 7-7/8" (200 mm) between the radiator and your body. The transmitt er must not be collocated or operating in conjunction with any other antenna or transmitter.

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