INTERNET LIGHTSPEED

SR808ac Cable Modem 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 SR808ac is targeted towards DOCSIS/EuroDOCSIS3.0 cable modem, eMTA and gateway with 24 downstream channels and 8 upstream channels. The SR808ac incorporates a variety of industry standard peripheral interfaces including dual IEEE802.3 10/100/1000Mbps interface, one with integrated GPHY, and dual USB2.0 interfaces (Host and Host/Device) with integrated PHYs. The SR808ac integrates a complete 2-channel voice system.

The SR808ac supports WLAN access. It complies with IEEE 802.11,802.11b/g, 802.11n, 802.11a and 802.11ac specifications, WEP, WPA, and WPA2 security specifications. The WLAN of the SR808ac 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 300 Mbps, compatible with IEEE 802.11a/b/g/n/ac, dual mode WLAN 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

- Print server
- Web filtering
- Remote update
- System statistics and monitoring

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- DOCSIS/EuroDOCSIS3.0
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11a
- IEEE 802.11ac
- 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 frenquency
		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.
Ethernet 1/2/3/4	Green	On	The Ethernet interface is connected.
		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.
USB	Green	On	The connection of USB flash disk has established.
		Off	No signal is detected.

Indicator	Color	Status	Description
FXS1/2	Green	On	EMTA has registered with CMTS
		Blink	EMTA send register request to CMTS
		Off	EMTA is no detected

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 1 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.
USB 0~1	USB port, for connecting other USB storage devices.
Power	Power interface, for connecting the power adapter.
TEL1~2	RJ-11 port, for connecting the router to Phones.

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 1 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 CMRG with HFC cable.

Step2 Connect the **Eth** port of the CMRG 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 CMRG.

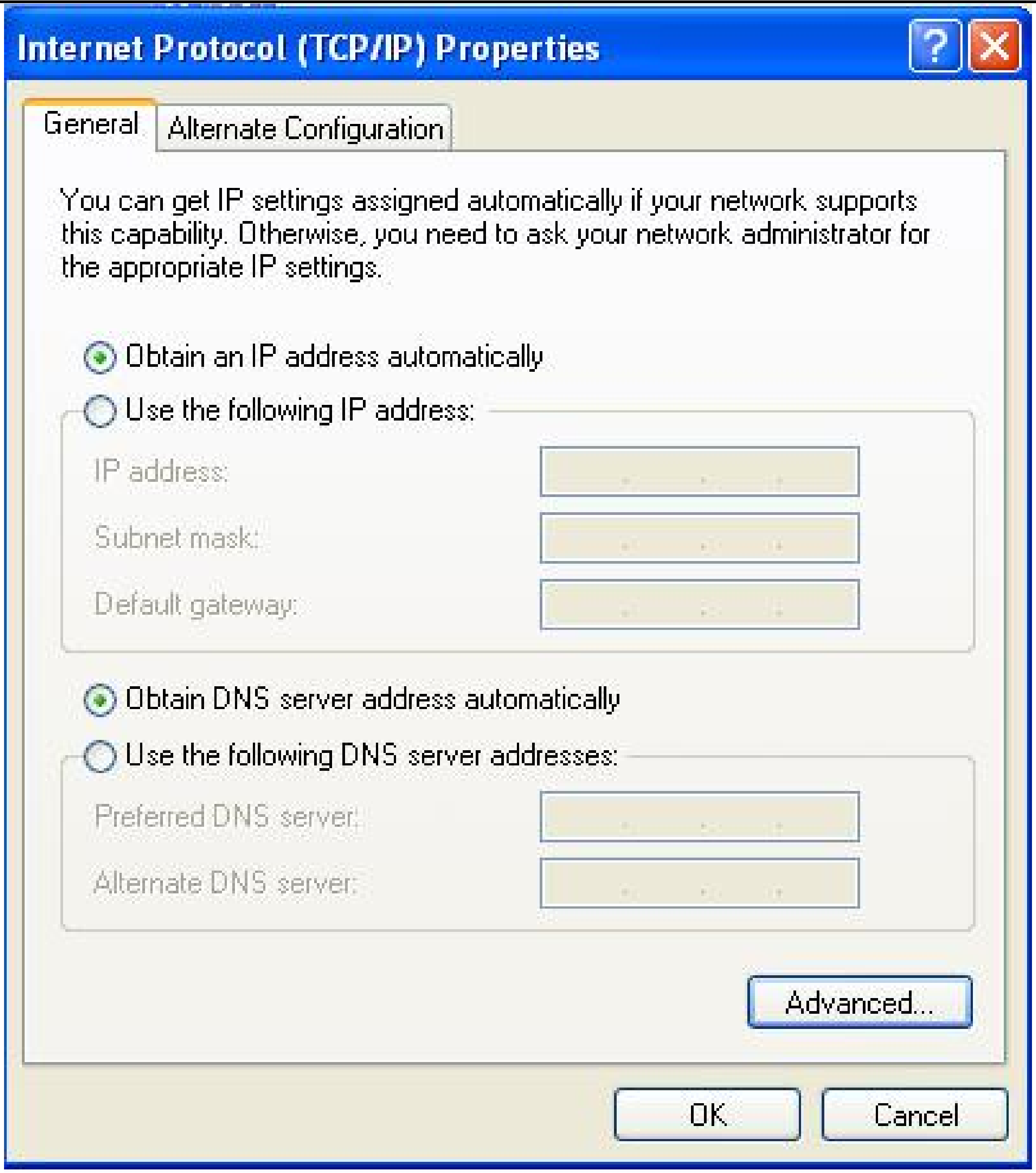
4 PC Network Configuration and Login

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. BCM3384 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 XP.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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 BCM3384 Cable Modem

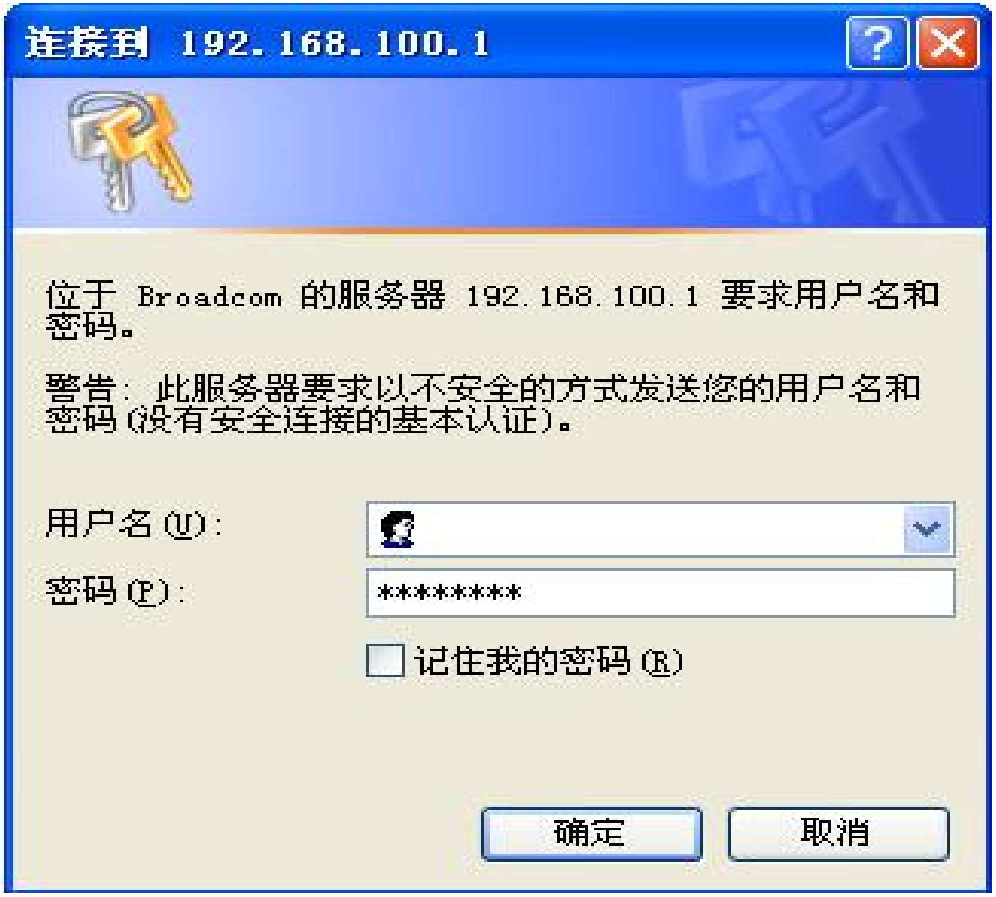
To log in to the BCM3384 cable modem, do as follows:

Step1 Open a Web browser on your computer.

Step2 Enter ***http://192.168.100.1*** (the default IP address of the BCM3384 cable modem) in the address bar. The login page appears.

Step3 Enter the user name and the password. The default username is blank and enter “**Broadcom**” in the Password field.

Step4 Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.



连接到 192.168.100.1

位于 Broadcom 的服务器 192.168.100.1 要求用户名和密码。

警告：此服务器要求以不安全的方式发送您的用户名和密码(没有安全连接的基本认证)。

用户名(U):

密码(P): ********

□ 记住我的密码(R)

Figure 2 Login page

After logging in to the BCM3384 cable modem, 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:

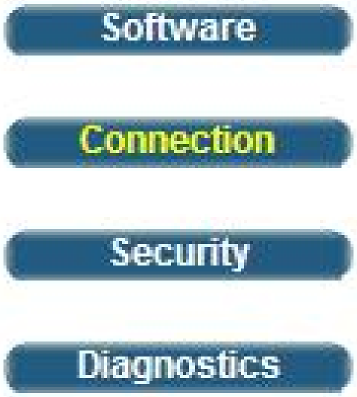
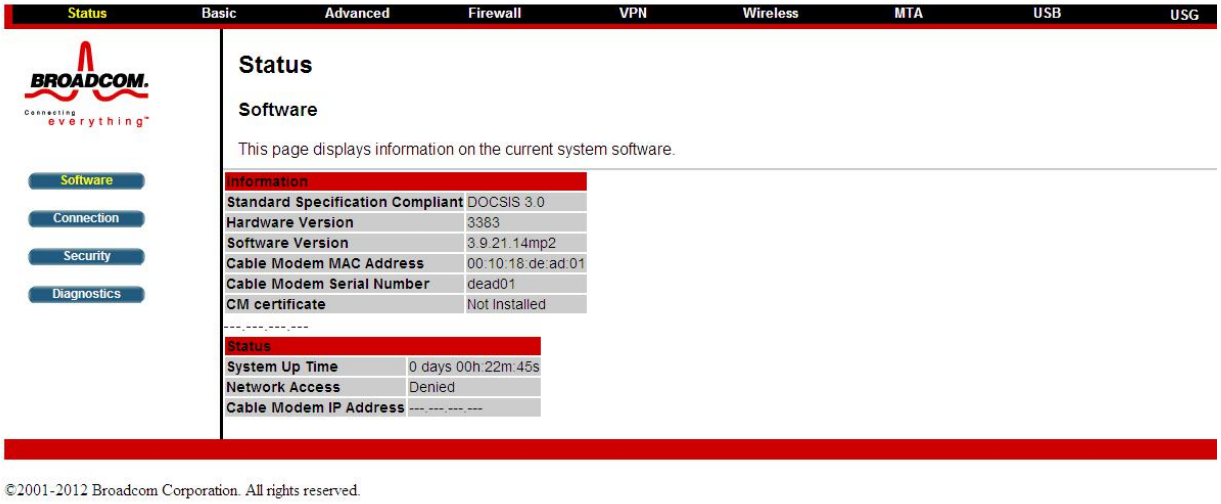


Figure 3 Submenus of status

5.1.1 Software

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



Status

Software

This page displays information on the current system software.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	3383
Software Version	3.9.21.14mp2
Cable Modem MAC Address	00:10:18:de:ad:01
Cable Modem Serial Number	dead01
CM certificate	Not Installed

---.---.---.---

Status	
System Up Time	0 days 00h:22m:45s
Network Access	Denied
Cable Modem IP Address	---.---.---.---

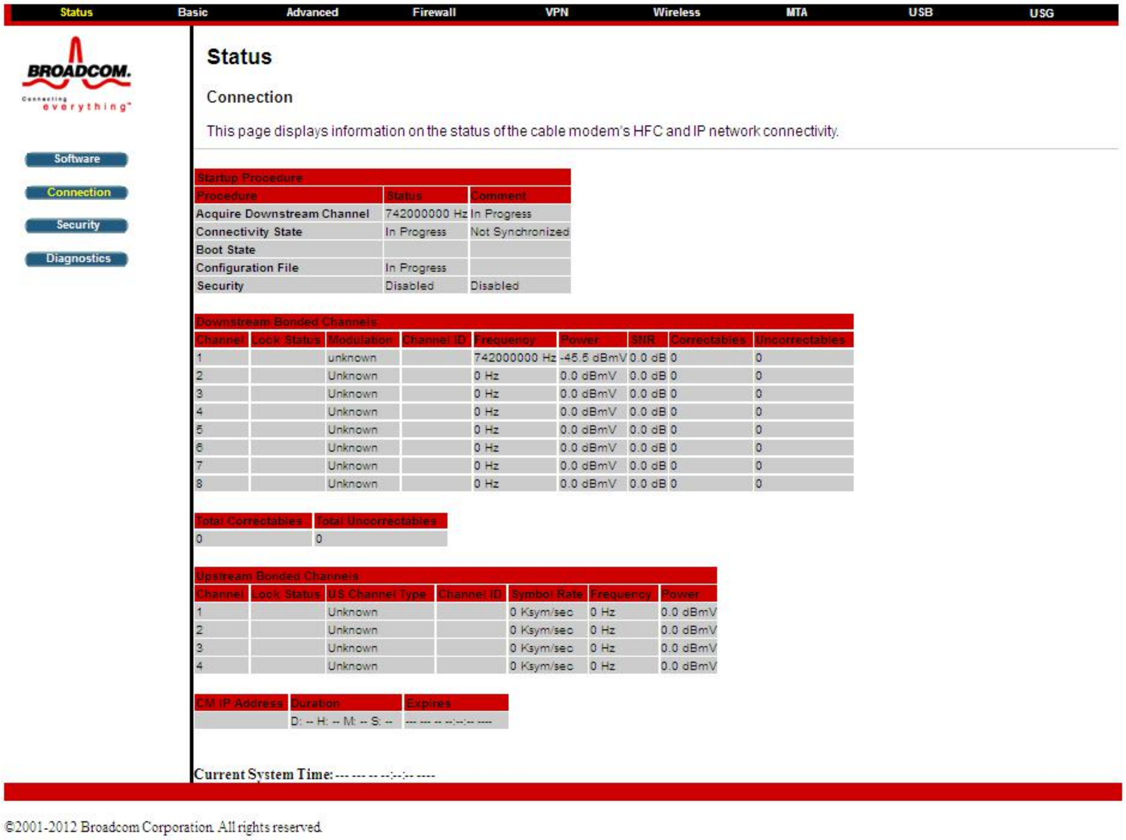
©2001-2012 Broadcom Corporation. All rights reserved.

Figure 4 Software page

This page displays information about the hardware version, software version, MAC address, cable modem IP address, serial number, system "up" time, and network registration status.

5.1.2 Connection

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



Status

Connection

This page displays information on the status of the cable modem's HFC and IP network connectivity.

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	742000000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State		
Configuration File	In Progress	
Security	Disabled	Disabled

Downstream Bonded Channels								
Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1		unknown		742000000 Hz	-45.5 dBmV	0.0 dB	0	0
2		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
3		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
4		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
5		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
6		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
7		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0
8		Unknown		0 Hz	0.0 dBmV	0.0 dB	0	0

Total Correctables	Total Uncorrectables
0	0

Upstream Bonded Channels						
Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV
2		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV
3		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV
4		Unknown		0 Ksym/sec	0 Hz	0.0 dBmV

CM IP Address	Duration	Expires
	D: -- H: -- M: -- S: --	--- --- -- --:--:-- ----

Current System Time: --- --- -- --:--:-- ----

©2001-2012 Broadcom Corporation. All rights reserved.

Figure 5 Connection information

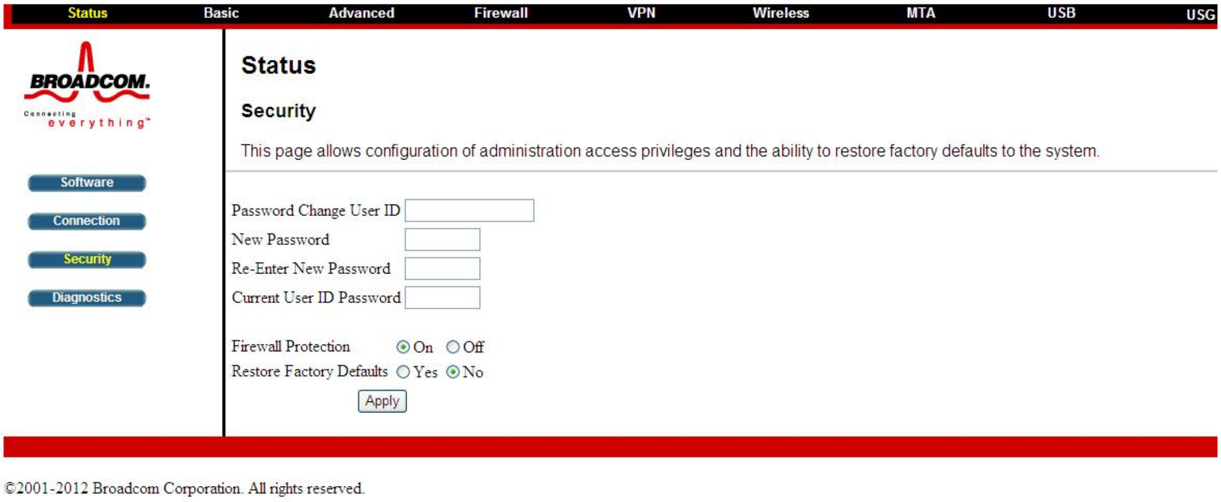
This page displays information about the RF upstream and downstream channels, including downstream channel frequencies, upstream channel IDs, and upstream and downstream signal power and modulation.

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 Security

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



Status

Security

This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

Password Change User ID
New Password
Re-Enter New Password
Current User ID Password

Firewall Protection ● On ○ Off
Restore Factory Defaults ○ Yes ● No

Apply

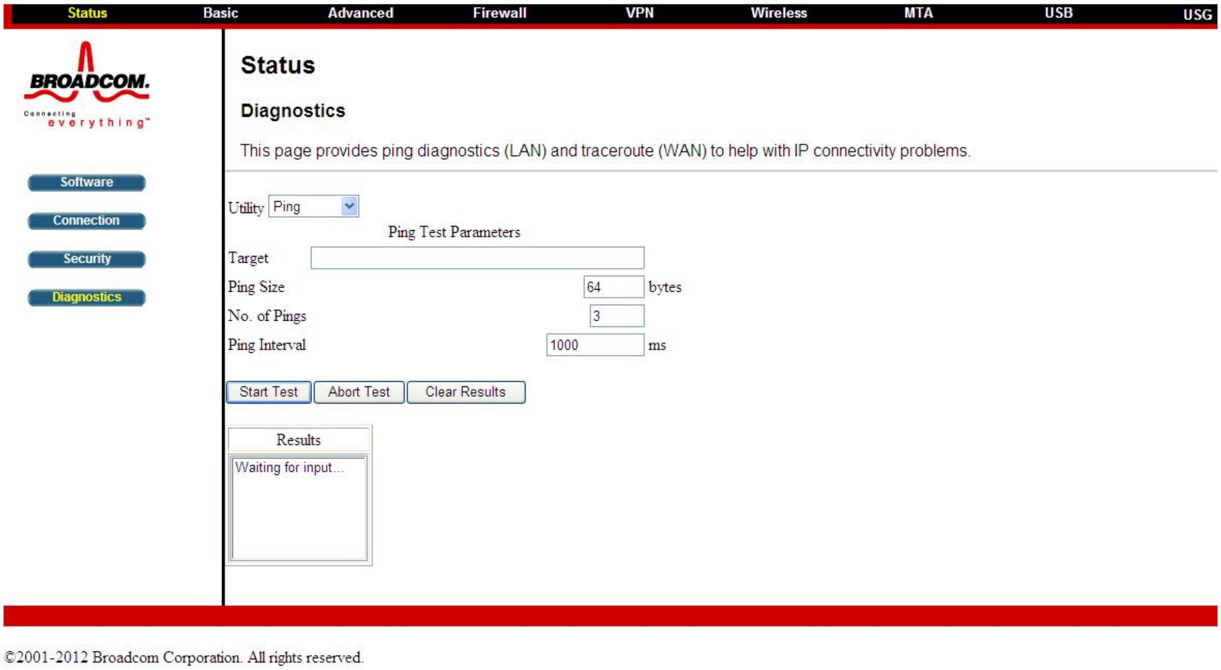
©2001-2012 Broadcom Corporation. All rights reserved.

To restore factory defaults, select the Yes radio button and click Apply. This will cause the device to reset. The factory default password is “Broadcom” and is case sensitive.

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 Apply will change the password. You do NOT have to restore factory defaults to change the password.

5.1.4 Diagnostics

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



Status

Diagnostics

This page provides ping diagnostics (LAN) and traceroute (WAN) to help with IP connectivity problems.

Utility: Ping

Ping Test Parameters

Target		
Ping Size	64	bytes
No. of Pings	3	
Ping Interval	1000	ms

Results

Waiting for input...

©2001-2012 Broadcom Corporation. All rights reserved.

Figure 6 Diagnostic information

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

Ping allows you to check connectivity between the CMRG and devices on the LAN.

Traceroute allows you to map the network path from the CMRG 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.

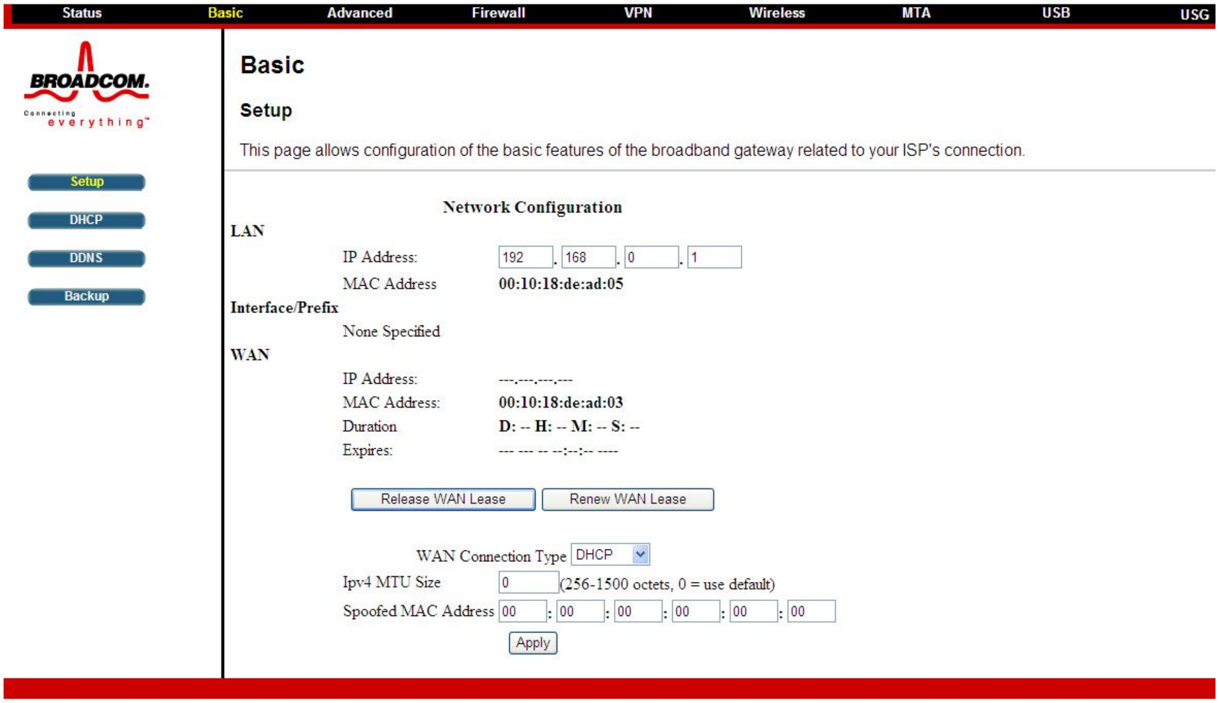
5.2 Basic

Choose **Basic** and the submenus of **Basic** are shown as below:

Figure 7 Submenus of basic

5.2.1 Setup

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



Basic

Setup

This page allows configuration of the basic features of the broadband gateway related to your ISP's connection.

Network Configuration

LAN

IP Address: 192 . 168 . 0 . 1

MAC Address 00:10:18:de:ad:05

Interface/Prefix

None Specified

WAN

IP Address: ---.---.---.---

MAC Address: 00:10:18:de:ad:03

Duration D: -- H: -- M: -- S: --

Expires: --- --- -- --:--:-- ----

WAN Connection Type DHCP

Ipv4 MTU Size 0 (256-1500 octets, 0 = use default)

Spoofed MAC Address 00 : 00 : 00 : 00 : 00 : 00

Figure 8 Setup configuration

Enter the information from the Required Information section as indicated:

1.If your ISP uses DHCP, select “DHCP” for the WAN Connection Type, and enter Host Name and Domain name if required. OR

If your ISP uses static IP addressing, select “Static IP” for the WAN Connection Type, and enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.

2.Enter a unicast MAC address in the Spoofed MAC Address field. Your ISP may require this to be your PC’s MAC address. If not, you can simply supply the WAN side MAC address of the router as your CPE and leave the spoofed MAC address entry set to all 0’s, since there will be no spoofing required.

3.Select the Apply button. This will reset the CMRG.

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

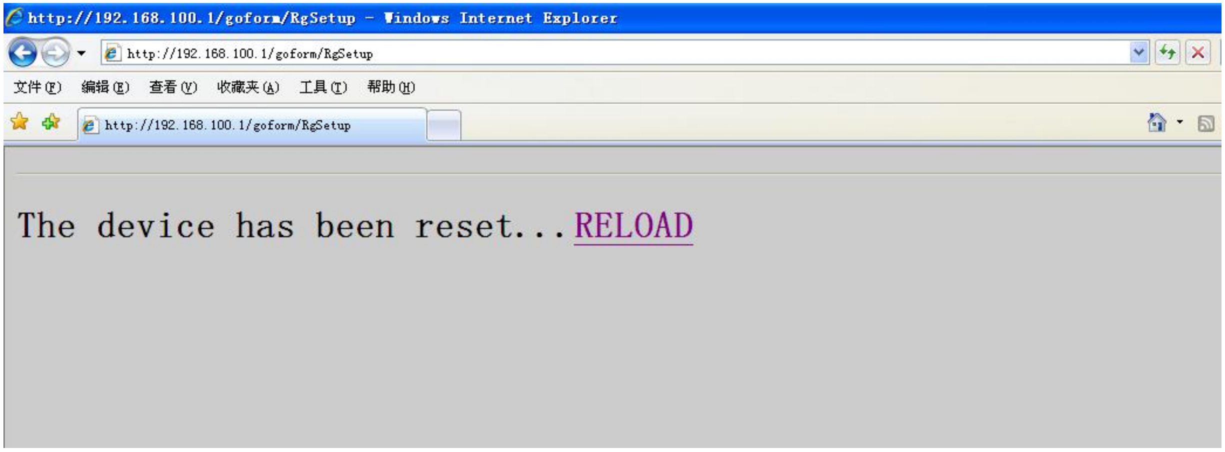
1.Power up the CMRG and wait for it to register with the CMTS and obtain an Internet-routable IP address

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

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 CMRG first powers up. One such setting is changing the Static WAN IP address parameters. Any changes to these settings will force the CMRG 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:


http://192.168.100.1/goform/RgSetup - Windows Internet Explorer
http://192.168.100.1/goform/RgSetup
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)
http://192.168.100.1/goform/RgSetup

The device has been reset...RELOAD

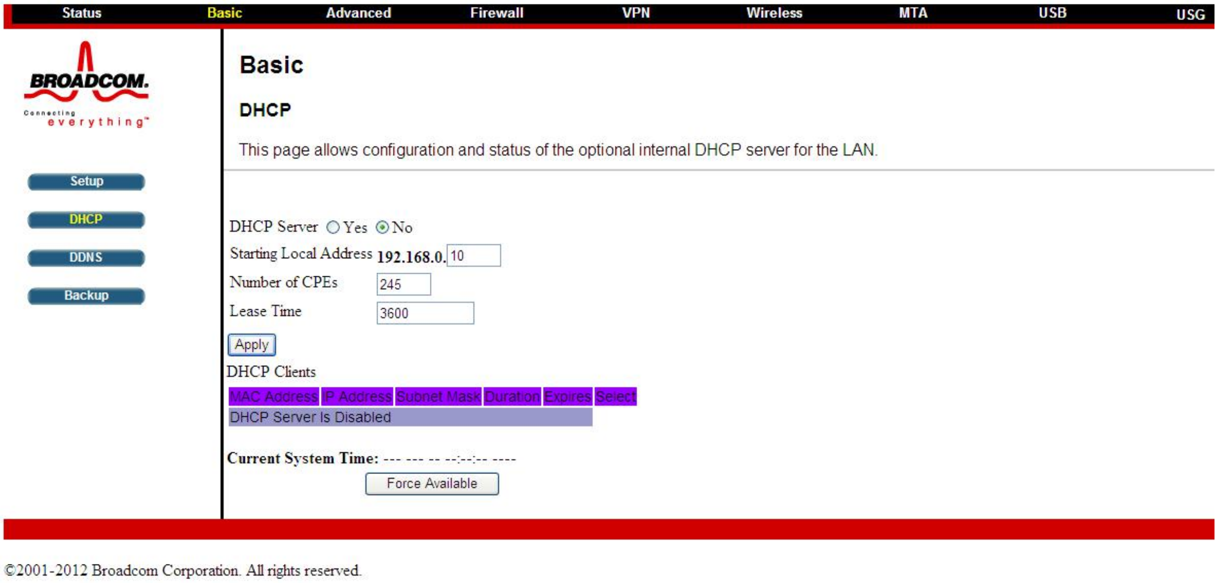
Figure 9 Reload page

Simply wait for the modem to reboot and click on the “Reload” 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 > DHCP,** and the following page appears.



Basic

DHCP

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

DHCP Server ○ Yes ● No

Starting Local Address 192.168.0. 10

Number of CPEs 245

Lease Time 3600

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
DHCP Server Is Disabled					

Current System Time: --- --- -- --:--:-- ----

©2001-2012 Broadcom Corporation. All rights reserved.

Figure 10 DHCP configuration

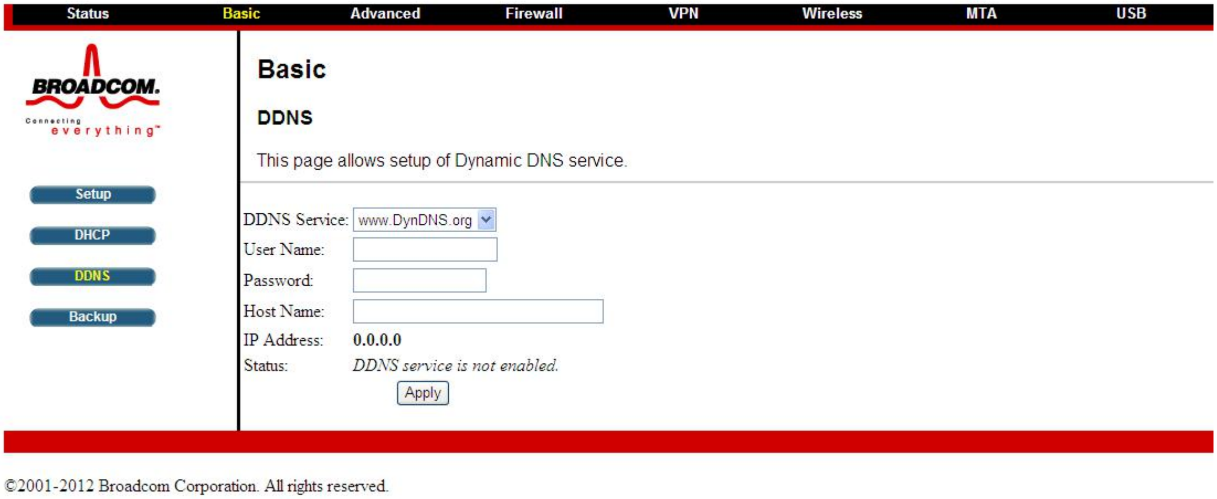
This page allows configuration and status of the optional internal DHCP server for the LAN.

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 selecting the No radio button. If you do this, make sure the IP address assigned to the CMRG 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 CMRG from the LAN. The IP address of the CMRG can be set from the Basic 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 CMRG via DHCP.

5.2.3 DDNS

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



Basic

DDNS

This page allows setup of Dynamic DNS service.

DDNS Service: www.DynDNS.org
User Name:
Password:
Host Name:
IP Address: 0.0.0.0
Status: *DDNS service is not enabled.*

©2001-2012 Broadcom Corporation. All rights reserved.

Figure 11 DDNS setup

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

To activate the DDNS client:

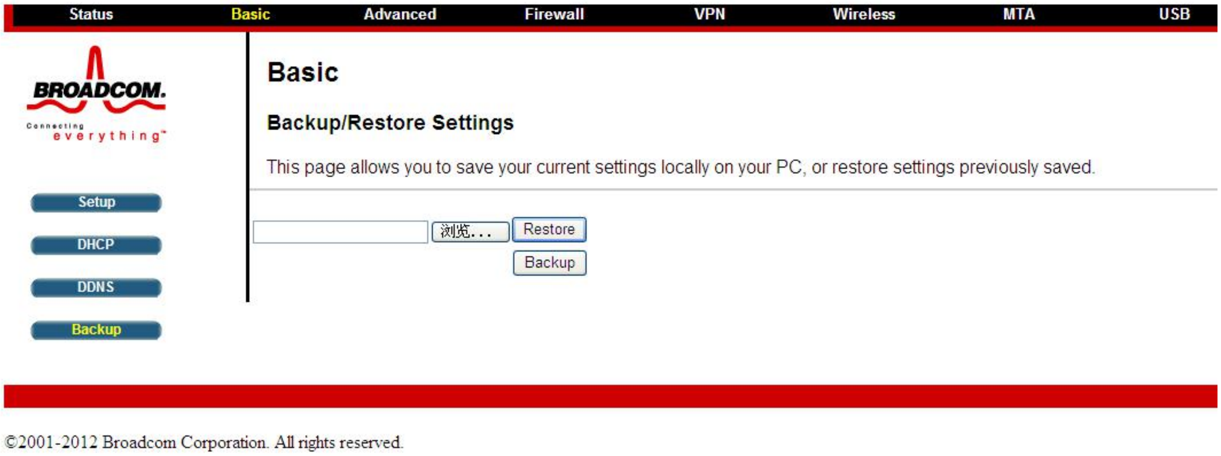
1. Go to the DynDNS website and create an account for the Dynamic DNS service. You will create a username and password, and be asked to choose a host name for your server, and the dynamic DNS domain to which your host will be assigned. You will also be asked for your host’s current IP address. This is the WAN IP address that has been assigned to your CMRG during provisioning. (See WAN IP Address on the Basic / Setup web page.)

2. Enter your account information on the Basic / DDNS web page, enable the service by selecting www.DynDNS.org from the DDNS Service drop-down list, and click Apply.

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.

5.2.4 Backup

Choose **Basic > Backup**, and the following page appears.



Basic

Backup/Restore Settings

This page allows you to save your current settings locally on your PC, or restore settings previously saved.

©2001-2012 Broadcom Corporation. All rights reserved.

Figure 12 Backup setup

In this page, you can save the current CMRG 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 backup 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

Choose **Advanced** and the submenus of **Advanced** are shown as below:

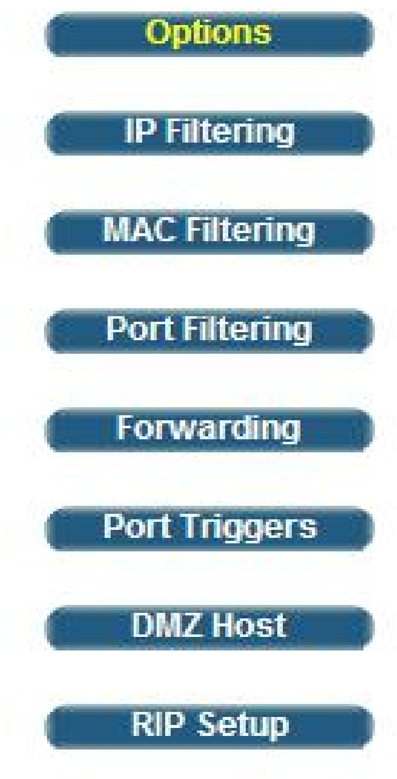
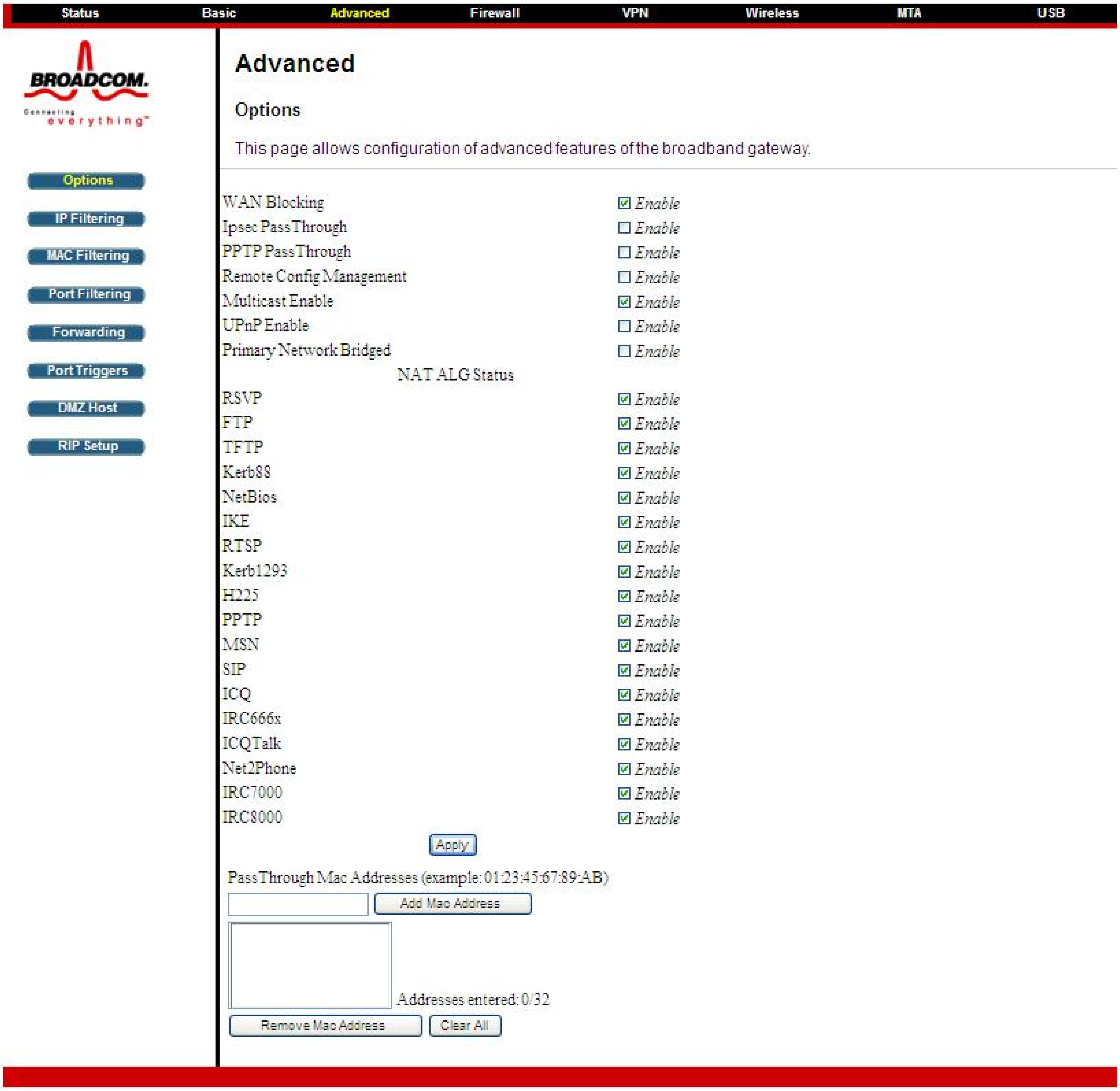


Figure 13 Submenus of advanced

5.3.1 Options

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



Advanced

Options

This page allows configuration of advanced features of the broadband gateway.

WAN Blocking	☑ Enable
Ipsec PassThrough	☐ Enable
PPTP PassThrough	☐ Enable
Remote Config Management	☐ Enable
Multicast Enable	☑ Enable
UPnP Enable	☐ Enable
Primary Network Bridged	☐ Enable
NAT ALG Status	
RSVP	☑ Enable
FTP	☑ Enable
TFTP	☑ Enable
Kerb88	☑ Enable
NetBios	☑ Enable
IKE	☑ Enable
RTSP	☑ Enable
Kerb1293	☑ Enable
H225	☑ Enable
PPTP	☑ Enable
MSN	☑ Enable
SIP	☑ Enable
ICQ	☑ Enable
IRC666x	☑ Enable
ICQTalk	☑ Enable
Net2Phone	☑ Enable
IRC7000	☑ Enable
IRC8000	☑ Enable

Apply

PassThrough Mac Addresses (example: 01:23:45:67:89:AB)

Add Mac Address

Addresses entered: 0/32

Remove Mac Address   Clear All

Figure 14 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 Apply button. These features can be modified on the fly without a system reset.

" WAN Blocking" prevents the CMRG or the PCs behind it from being visible to the WAN. For instance, pings to the CMRG's WAN IP address or the PCs behind it are not returned. Therefore, it will be more difficult for hacker to discover your WAN IP address to begin an attack on your private LAN.

" IpSec" and "PPTP" (Point-to-Point Tunneling Protocol) pass-through modes enable these protocols to be used through the CMRG such that a VPN device (or software) may communicate properly with the WAN.

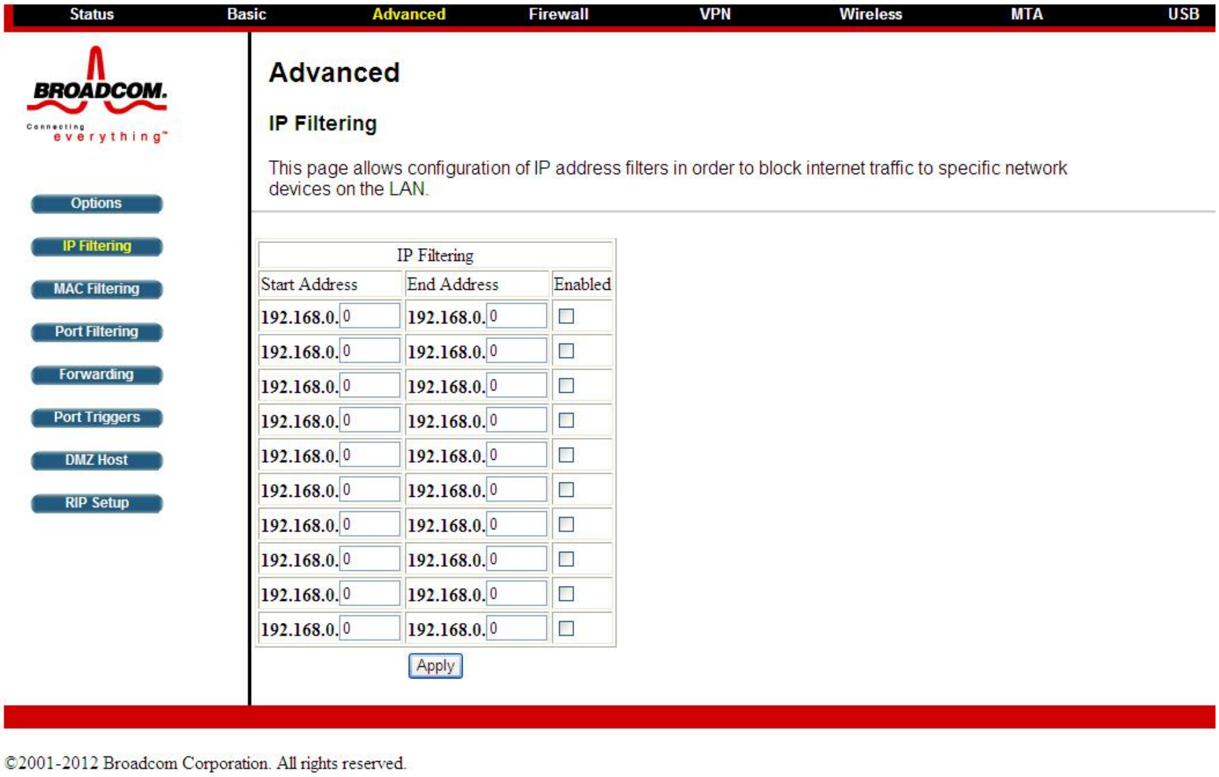
“ Remote Configuration Management” allows the CMRG to be administered (configured) from the WAN via surfing to the WAN IP address on port 8080 of the CMRG from anywhere on the Internet (e.g. at the browser URL window enter http://WanIPAddress:8080/ to access the CMRG remotely).

“ Multicast Enable” allows multicast specific traffic (denoted by a multicast specific address) to be passed to and from the PC’s on the private network behind the CMRG.

“ UPnP Enable” enables the UPnP agent in the CMRG. If you are running a CPE application that requires UPnP, check this box.

5.3.2 IP Filtering

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



Advanced

IP Filtering

This page allows configuration of IP address filters in order to block internet traffic to specific network devices on the LAN.

IP Filtering		
Start Address	End Address	Enabled
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□
192.168.0. 0	192.168.0. 0	□

©2001-2012 Broadcom Corporation. All rights reserved.

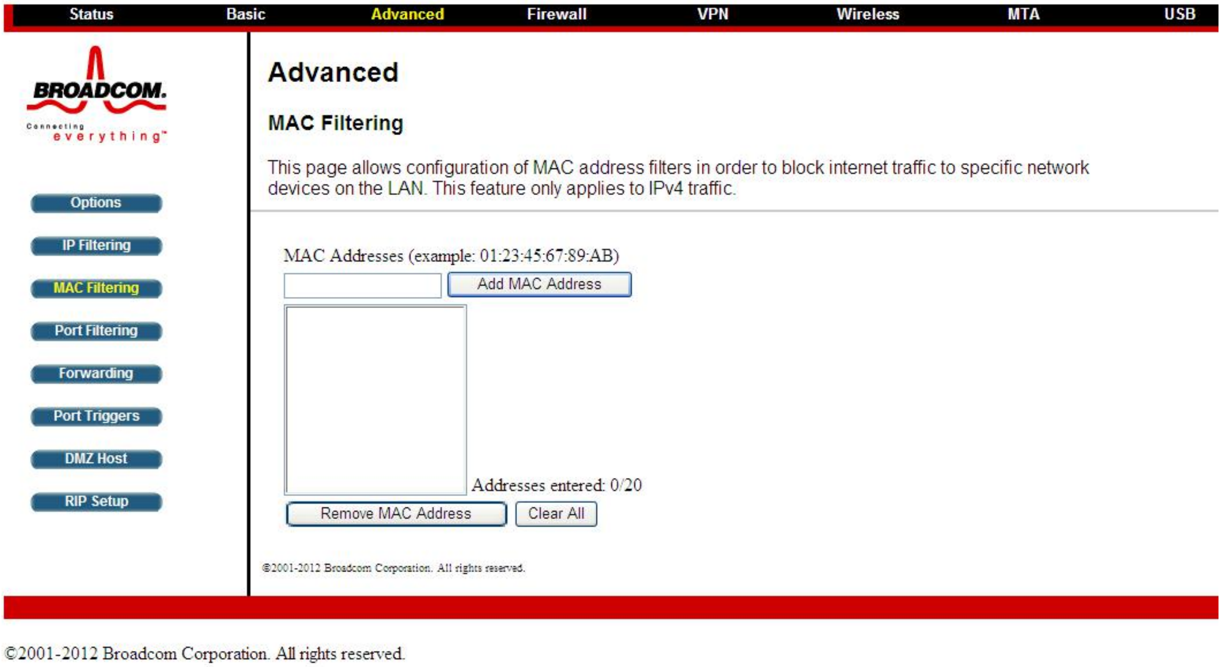
Figure 15 IP Filtering configuration

This page allows you to configure the CMRG 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 CMRG IP address. To activate the IP address filter, you must also check the “enable” box and click apply. The enable box allows you to store filter settings commonly used but not have them active.

5.3.3 MAC Filtering

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



Advanced

MAC Filtering

This page allows configuration of MAC address filters in order to block internet traffic to specific network devices on the LAN. This feature only applies to IPv4 traffic.

MAC Addresses (example: 01:23:45:67:89:AB)

Addresses entered: 0/20

©2001-2012 Broadcom Corporation. All rights reserved.

©2001-2012 Broadcom Corporation. All rights reserved.

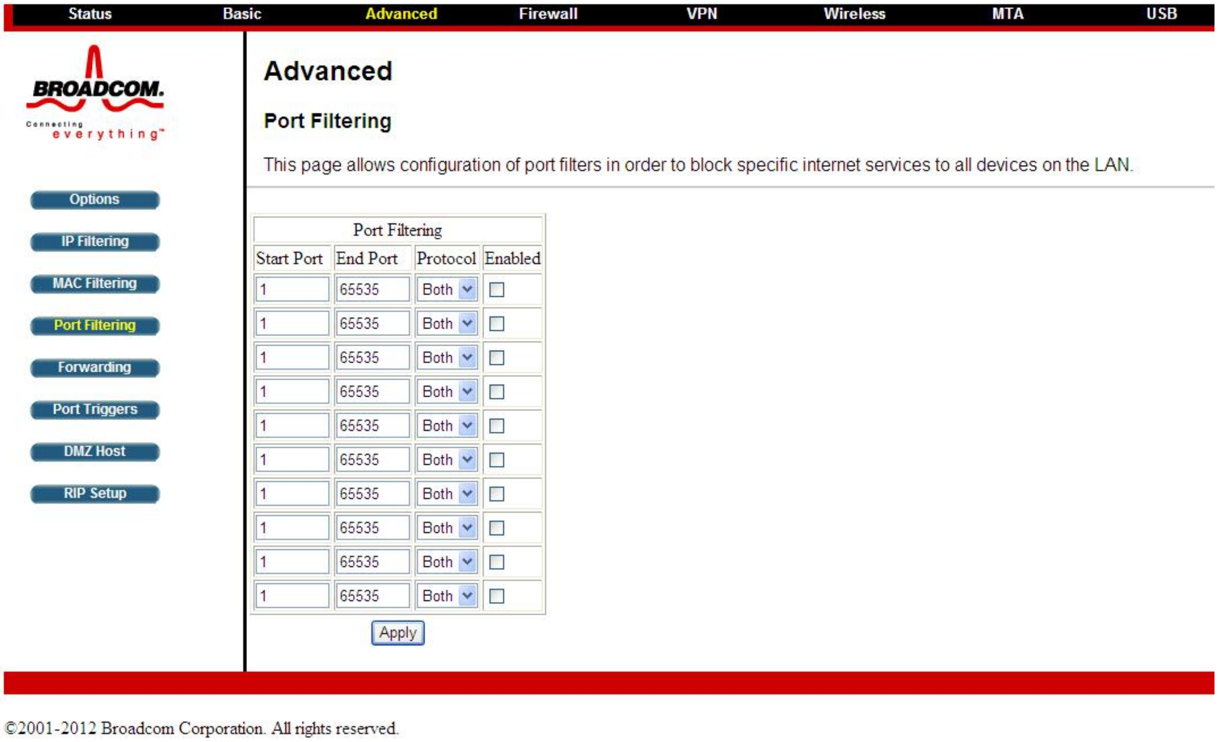
Figure 16 MAC filtering configuration

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 > Port Filtering** to display the following page.



Advanced

Port Filtering

This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.

Port Filtering

Start Port	End Port	Protocol	Enabled
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□

©2001-2012 Broadcom Corporation. All rights reserved.

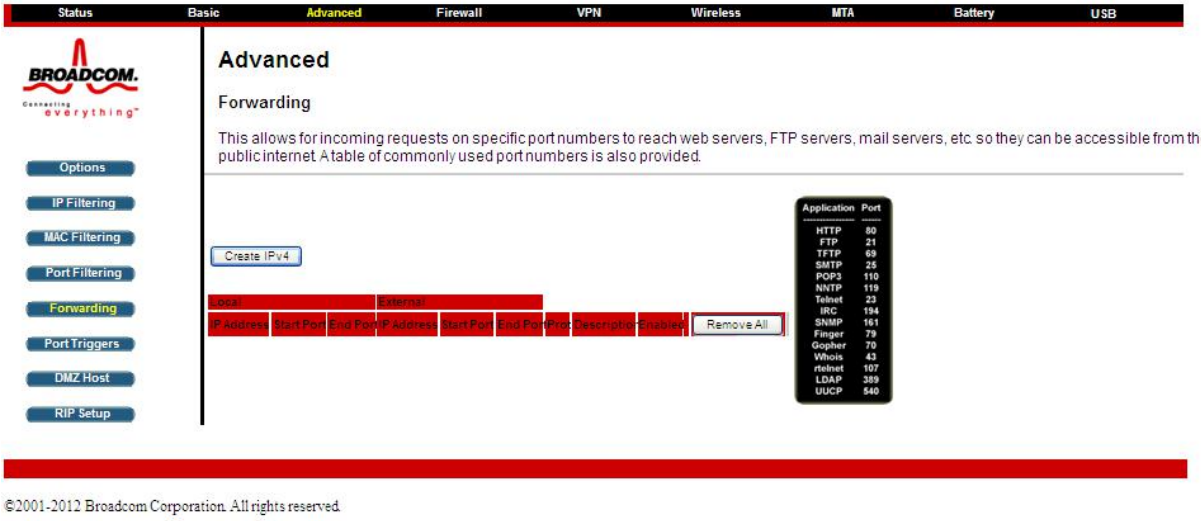
Figure 17 Port Filtering configuration

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 Apply.

5.3.5 Forwarding

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



Advanced

Forwarding

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.

Local			External					
IP Address	Start Port	End Port	IP Address	Start Port	End Port	Prot	Description	Enabled

Application	Port
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP3	110
NNTP	119
Telnet	23
IRC	194
SNMP	161
Finger	79
Gopher	70
Whois	43
rtelnet	107
LDAP	389
UUCP	540

©2001-2012 Broadcom Corporation. All rights reserved.

Figure 18 Forwarding

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.

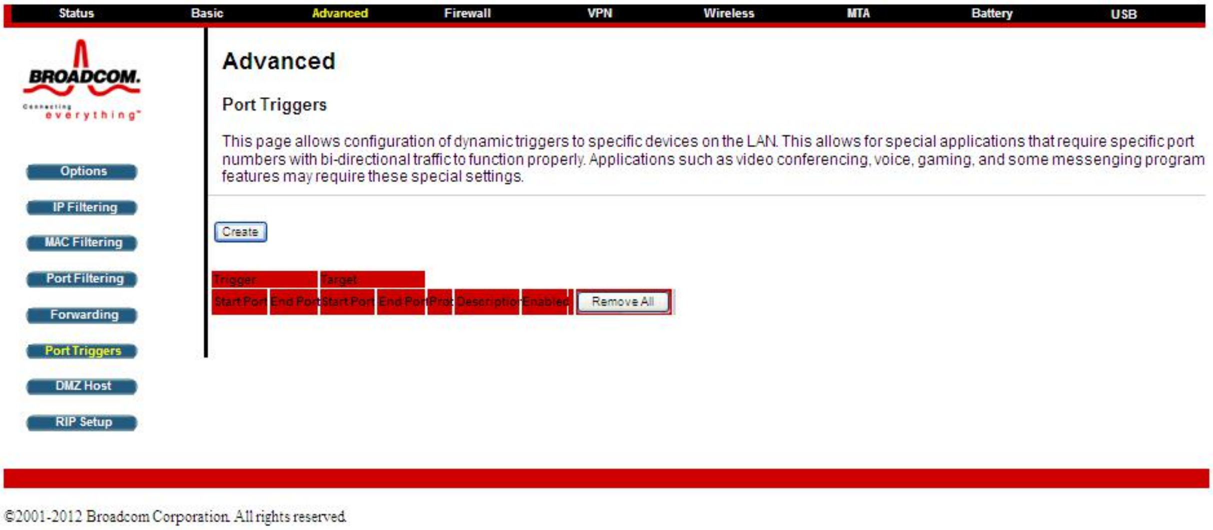
Forwarding allows you to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC

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** > **Port Triggers** to display the following page.



Advanced

Port Triggers

This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messenging program features may require these special settings.

Trigger		Target				
Start Port	End Port	Start Port	End Port	Prot	Description	Enabled

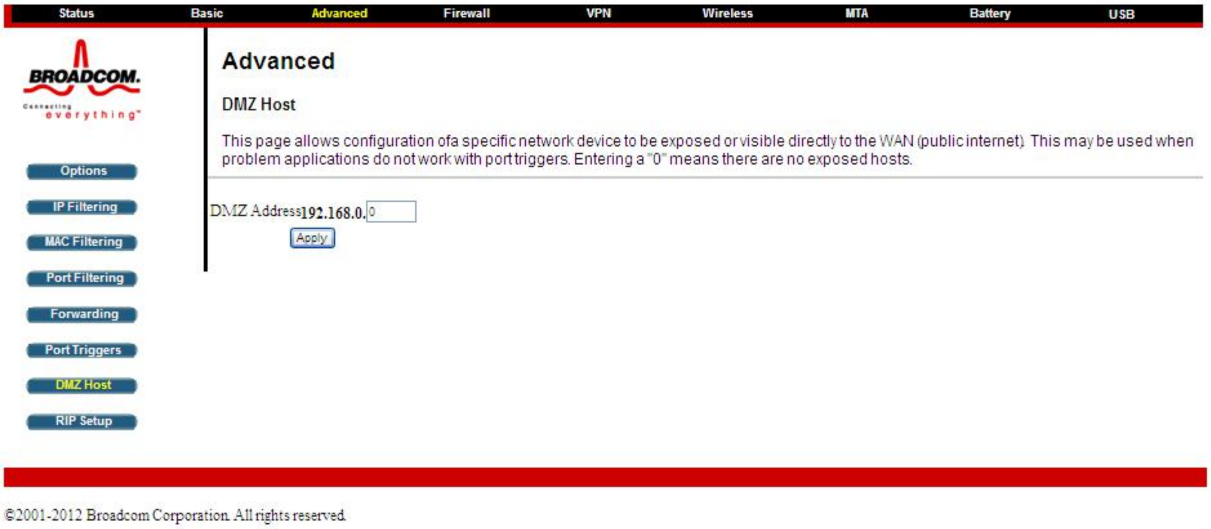
©2001-2012 Broadcom Corporation. All rights reserved.

Figure 19 Port Triggers

Port Triggers are similar to Port Forwarding except that they are not static ports held open all the time. When the CMRG 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 DMZ Host

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



Advanced

DMZ Host

This page allows configuration of a specific network device to be exposed or visible directly to the WAN (public internet). This may be used when problem applications do not work with port triggers. Entering a "0" means there are no exposed hosts.

DMZ Address 192.168.0. 0

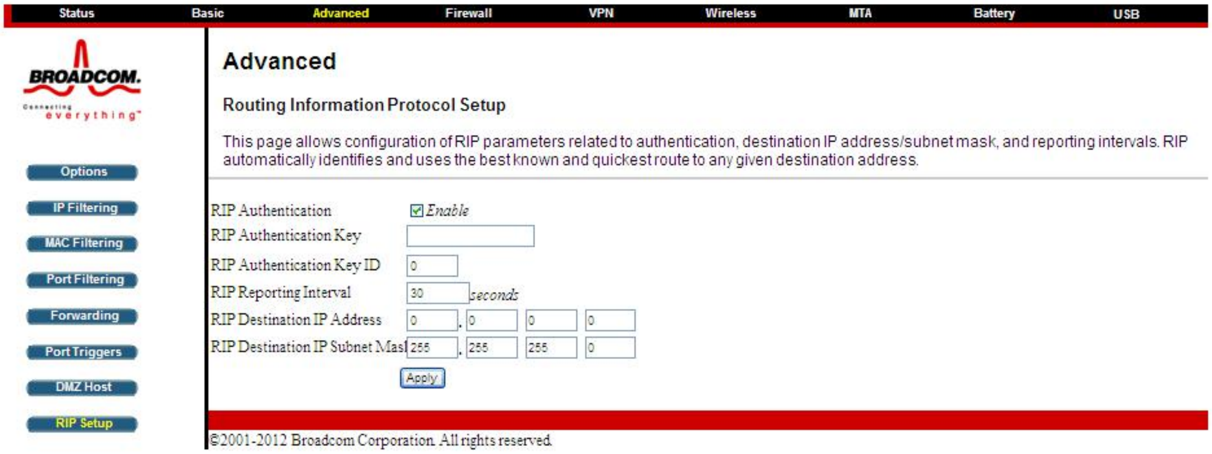
©2001-2012 Broadcom Corporation. All rights reserved.

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.

5.3.8 RIP Setup

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



Advanced

Routing Information Protocol Setup

This page allows configuration of RIP parameters related to authentication, destination IP address/subnet mask, and reporting intervals. RIP automatically identifies and uses the best known and quickest route to any given destination address.

RIP Authentication	☑ *Enable*			
RIP Authentication Key				
RIP Authentication Key ID	0			
RIP Reporting Interval	30 *seconds*			
RIP Destination IP Address	0	. 0	0	0
RIP Destination IP Subnet Masl	255	. 255	255	0

Apply

©2001-2012 Broadcom Corporation. All rights reserved.

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. CMRG and CMTS). The ISP would normally set this up because of their knowledge of their CMTS settings to match the configuration in the CMRG.

To enable the CMRG 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 CMRG 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 CMRG 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 CMRG was set up to send RIPv2 messages to the CMTS. The CMTS was also set up to receive these messages.

5.4 Firewall

Choose **Firewall** and the submenus of **Firewall** are shown as below:

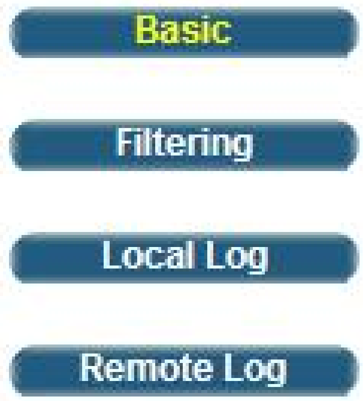
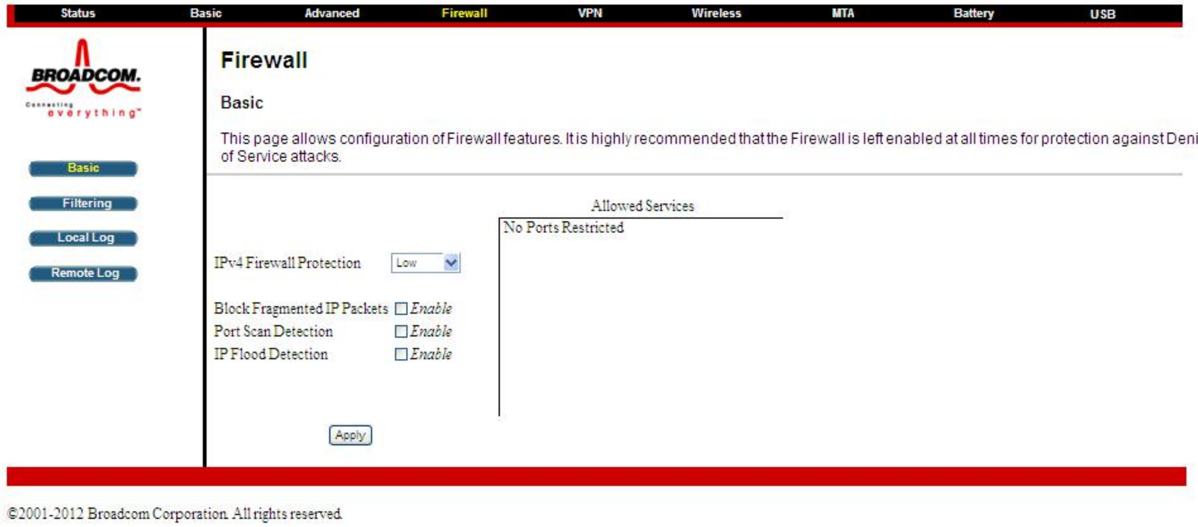


Figure 20 submenus of **Firewall**

5.4.1 Basic

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

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



Firewall

Basic

This page allows configuration of Firewall features. It is highly recommended that the Firewall is left enabled at all times for protection against Denial of Service attacks.

Allowed Services

No Ports Restricted

IPv4 Firewall Protection: Low

Block Fragmented IP Packets □ *Enable*
Port Scan Detection □ *Enable*
IP Flood Detection □ *Enable*

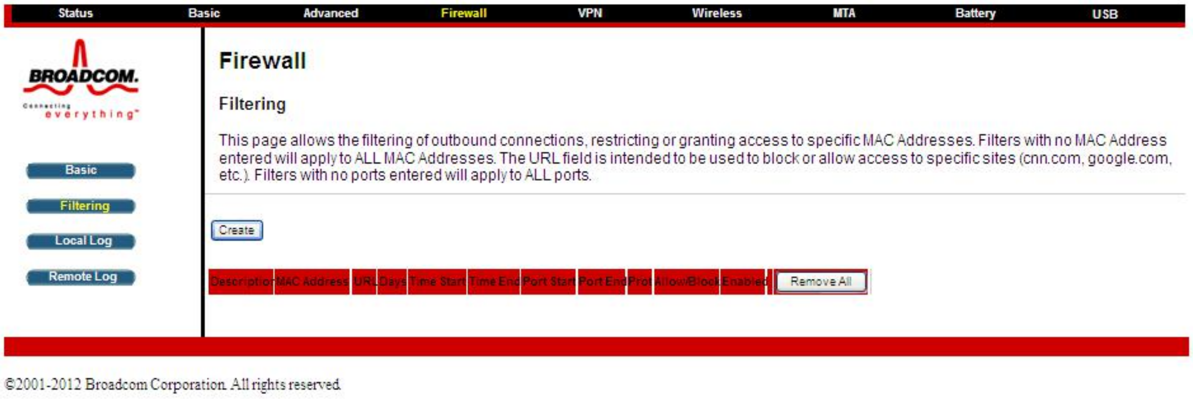
©2001-2012 Broadcom Corporation. All rights reserved.

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 prevents 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 Apply 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 CMRG reboot.

5.4.2 Filtering

Choose **Firewall** > **Filtering** to display the following page.



Firewall

Filtering

This page allows the filtering of outbound connections, restricting or granting access to specific MAC Addresses. Filters with no MAC Address entered will apply to ALL MAC Addresses. The URL field is intended to be used to block or allow access to specific sites (cnn.com, google.com, etc.). Filters with no ports entered will apply to ALL ports.

Description	MAC Address	URL	Days	Time Start	Time End	Port Start	Port End	Prot	Allow/Block	Enabled

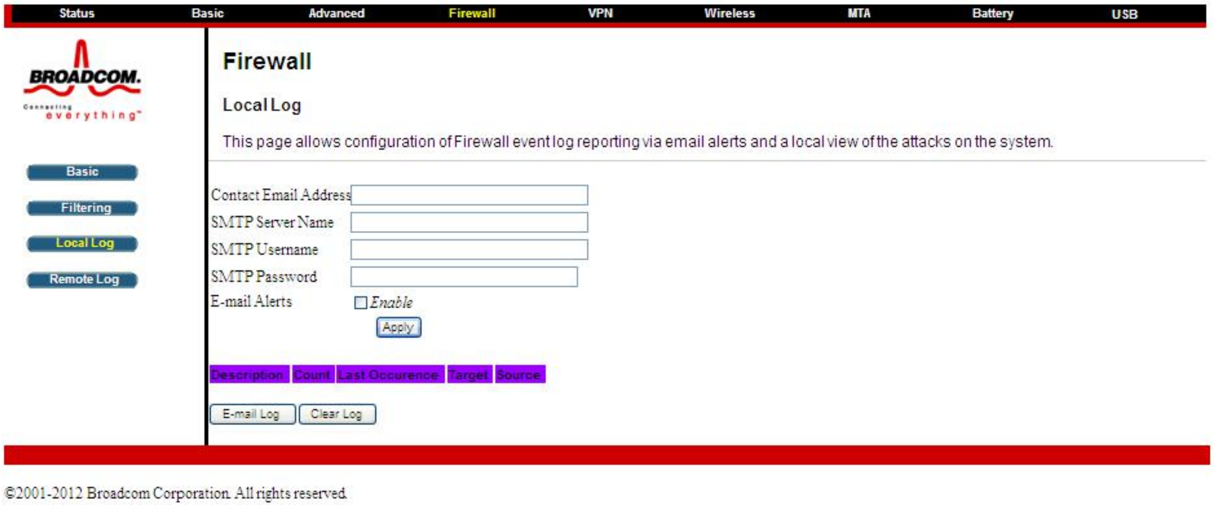
©2001-2012 Broadcom Corporation. All rights reserved.

CPE's can be prevented or permitted to access the Internet with entries in this webpage. Filter criteria is the mac address of the CPE and what types of packets that will be dropped. ToD filtering is accomplished on this page also.

An Ethernet mac address of all 0's will apply to all CPE's. A start and end port of 0 will apply to all ports.

5.4.3 Local Log

Choose **Firewall** > **Local Log** to display the following page.



Firewall

Local Log

This page allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system.

Contact Email Address
SMTP Server Name
SMTP Username
SMTP Password
E-mail Alerts □ *Enable*

Description	Count	Last Occurence	Target	Source

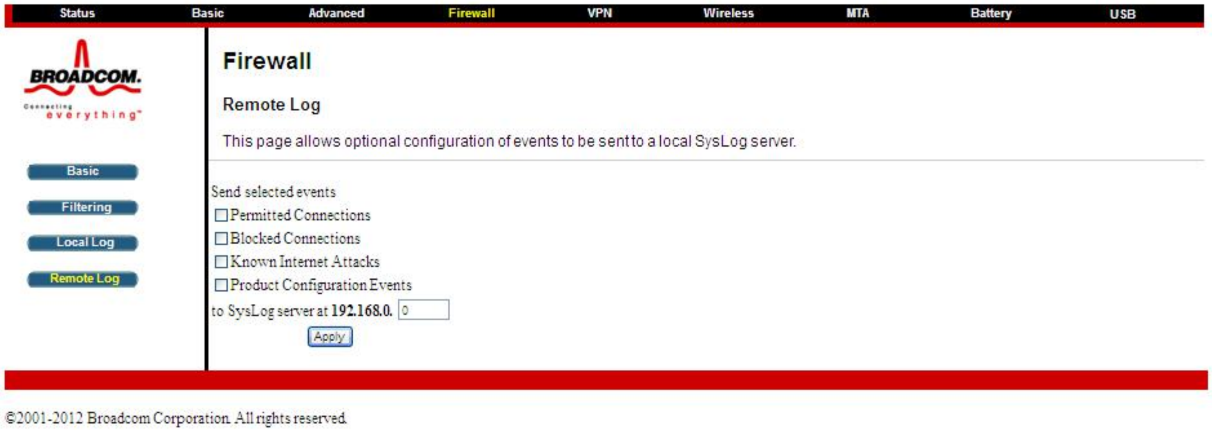
©2001-2012 Broadcom Corporation. All rights reserved.

The Local Log can send firewall attack reports out in two different ways. Individual emails can be sent out automatically, each time the firewall is under attack, and also a local log is stored within the modem and displayed in table form on the Local Log page.

To enable the automatic email alerts, enter your email address in the space provided, enter that email account's associated SMTP (Outgoing) mail server address and authentication credentials if required (provided by your ISP), check the "enable" box and click the Apply button. Individual emails will now be sent to the specified address each time an attack is detected. Each attack is also logged in the table on the Event Log page. If desired, a summary of the Event Log Table can be sent to the specified contact email address by clicking on the Email Log button. Clicking on the Clear Log button can also clear the table.

5.4.4 Remote Log

Choose **Firewall** > **Remote Log** to display the following page.



Firewall

Remote Log

This page allows optional configuration of events to be sent to a local SysLog server.

Send selected events

☐ Permitted Connections

☐ Blocked Connections

☐ Known Internet Attacks

☐ Product Configuration Events

to SysLog server at 192.168.0. 0

©2001-2012 Broadcom Corporation. All rights reserved.

The Remote Log can send firewall attack reports out to a standard SysLog server so many instances can be logged over a long period of time. Individual attack or configuration items can be selected that will be sent to the SysLog server such that only the items of interest can be monitored. Permitted connections, blocked connections, known Internet attack types, and CMRG configuration events can be logged. The SysLog server must be on the same network as the Private LAN behind the CMRG (typically 192.168.0.x). To activate the SysLog monitoring feature, check all desired event types to monitor and enter the last byte of the IP address of the SysLog server. Normally, the IP address of this SysLog server would be hard-coded so that the address will not change and always agrees with the entry on this page.

5.5 VPN

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

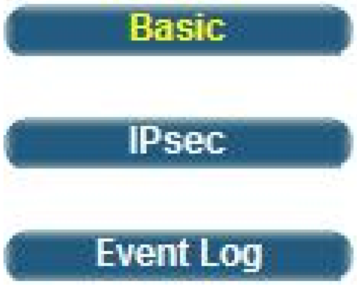
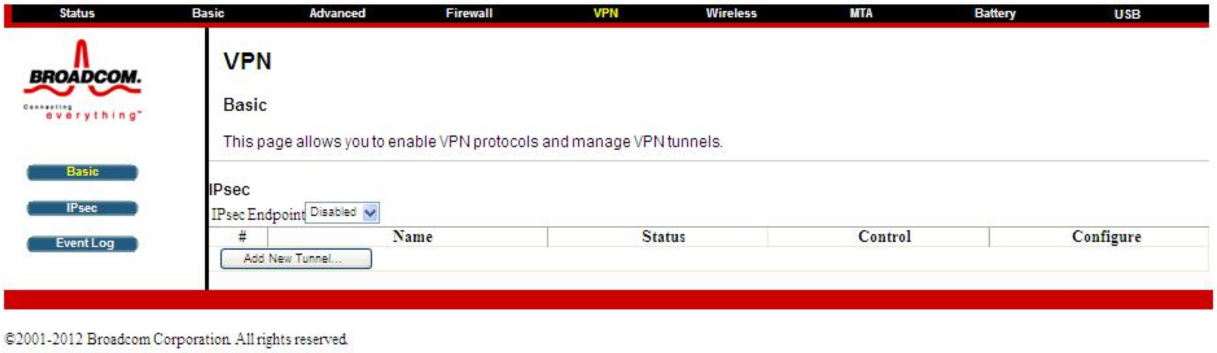


Figure 21 Submenus of VPN

5.5.1 Basic

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



VPN

Basic

This page allows you to enable VPN protocols and manage VPN tunnels.

IPsec

IPsec Endpoint Disabled

#	Name	Status	Control	Configure
Add New Tunnel...				

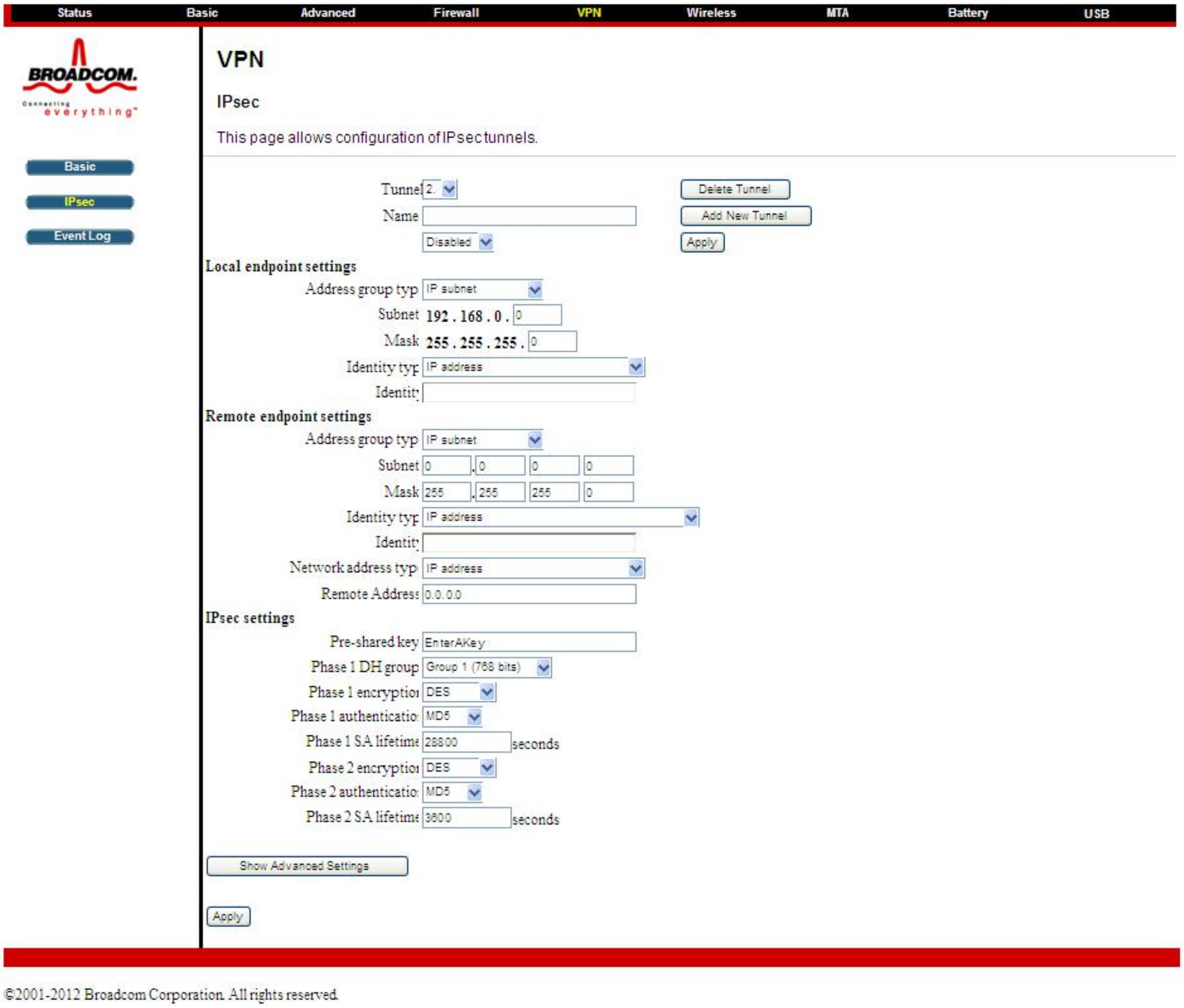
©2001-2012 Broadcom Corporation. All rights reserved.

Figure 22 Basic settings

This page will the status of configured tunnels.To start the process of manually adding a new tunnel select the “Add New Tunnel” button.

5.5.2 IPsec

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



VPN

IPsec

This page allows configuration of IPsec tunnels.

Tunnel 2.

Name

Disabled

Local endpoint settings

Address group typ IP subnet

Subnet 192 . 168 . 0 . 0

Mask 255 . 255 . 255 . 0

Identity typ IP address

Identity

Remote endpoint settings

Address group typ IP subnet

Subnet 0 . 0 0 0

Mask 255 . 255 255 0

Identity typ IP address

Identity

Network address typ IP address

Remote Address 0.0.0.0

IPsec settings

Pre-shared key EnterAKey

Phase 1 DH group Group 1 (768 bits)

Phase 1 encryption DES

Phase 1 authentication MD5

Phase 1 SA lifetime 28800 seconds

Phase 2 encryption DES

Phase 2 authentication MD5

Phase 2 SA lifetime 3600 seconds

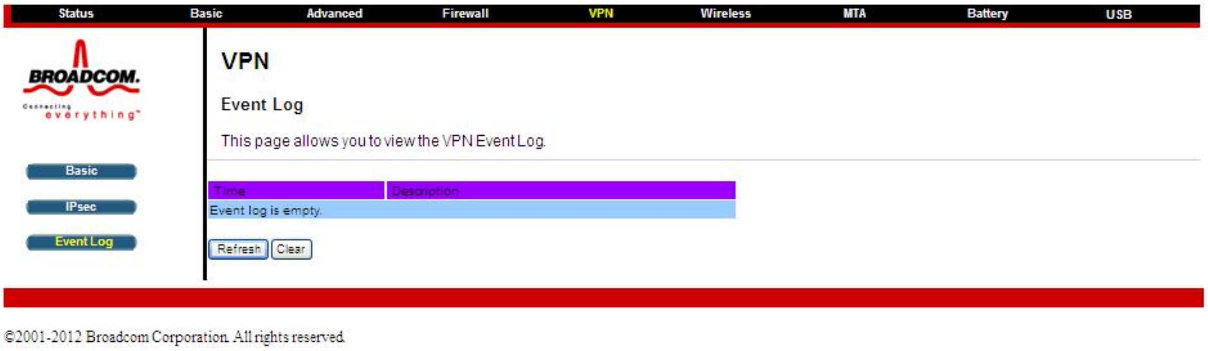
©2001-2012 Broadcom Corporation. All rights reserved.

Figure 23 IPsec

In this page, you are allowed to configure all aspects of the IPSec tunnel.

5.5.3 Event Log

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



VPN

Event Log

This page allows you to view the VPN Event Log.

Time	Description
Event log is empty.	

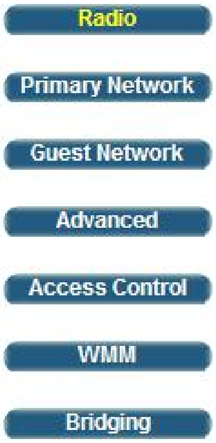
©2001-2012 Broadcom Corporation. All rights reserved.

Figure 24 Event Log configuration

This page will events related to VPN.

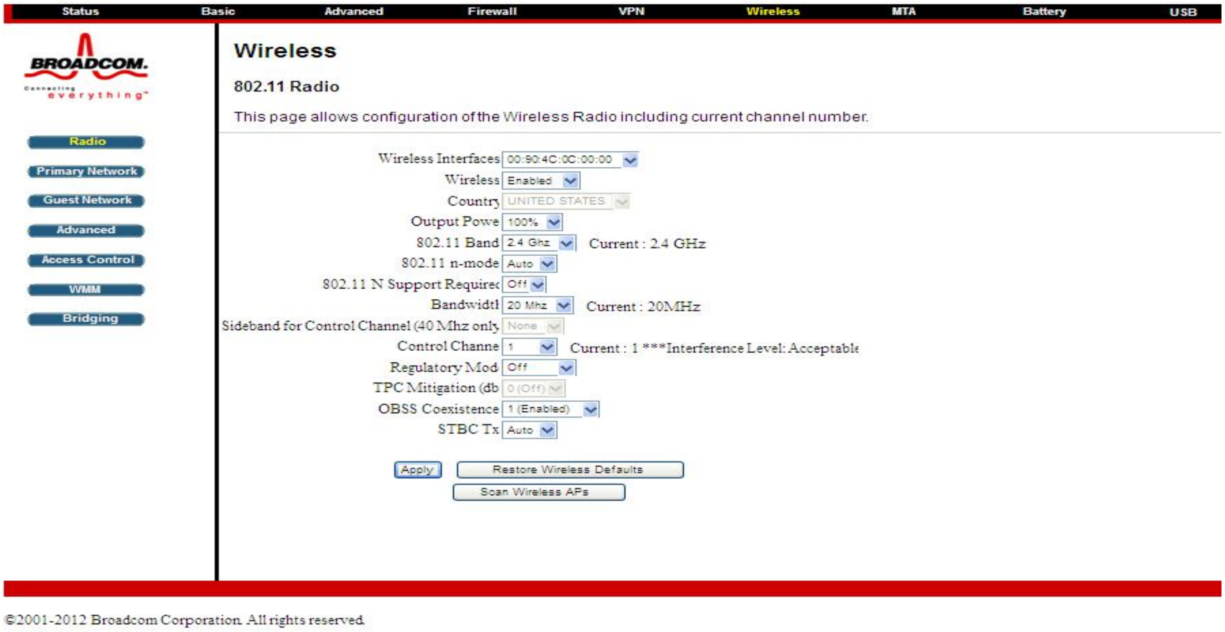
5.6 Wireless

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



5.6.1 Radio

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



Wireless

802.11 Radio

This page allows configuration of the Wireless Radio including current channel number.

Wireless Interfaces	00:90:4C:0C:00:00	
Wireless	Enabled	
Country	UNITED STATES	
Output Powe	100%	
802.11 Band	2.4 Ghz	Current : 2.4 GHz
802.11 n-mode	Auto	
802.11 N Support Requirec	Off	
Bandwidtl	20 Mhz	Current : 20MHz
Sideband for Control Channel (40 Mhz only	None	
Control Channe	1	Current : 1 ***Interference Level: Acceptable
Regulatory Mod	Off	
TPC Mitigation (db	0 (Off)	
OBSS Coexistence	1 (Enabled)	
STBC Tx	Auto	

©2001-2012 Broadcom Corporation. All rights reserved.

This page allows configuration of the physical parameters of your wireless network.The MAC address of the wireless interface is displayed at the top of the page.

Wireless:

Allows the wireless interface to be enabled and disabled.

Country:

Restricts the channel set based on the selected country's regulatory requirements.

Output Power:

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

802.11 Band:

Select whether the radio operates in the 2.4 GHz or 5 GHz band. There may be less interference from other wireless networks and household devices in the 5 GHz band, but 802.11b/g devices will not be able to connect.

802.11 n-mode:

Switch this to Off to force the AP to operate in 802.11g mode.

802.11 N Support Required:

If the 802.11 N support required field is set to "on", then only .n capable stations are allowed to associate with the CM. If it's set to "off" then b/g/n are all allowed.

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.

Control Channel:

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

Table 1. Next to the drop-down list box, the current channel number is displayed.

Table 1. Allowed Channels by Country:

Country	First Channel	Last Channel
USA	1	11
Worldwide, China, Europe	1	13
Japan, Thailand, All Channels	1	14
Israel	5	7
Jordan	10	13

Regulatory Mode:

Selects either 802.11d or 802.11h modes of operation. These are amendments to the 802.11 specifications for solving interference issues with other transmission systems such as satellite or radar, and also transmission requirements in different parts of the world.

TPC Mitigation (dB):

Transmit Power Control mitigation factor in dB. Transmit Power Control is used to automatically reduce the transmission power when other networks are within range. This setting is only used when the Regulatory Mode is set to 802.11h.

OBSS Coexistence:

Enable/Disable Overlapping BSS Coexisistence. OBSS coexistence refers to the ability of the AP to support 20 MHz devices within 40 MHz channels. It also allows the AP to better deal with nearby 20 MHz devices that are interfering with part of its 40 MHz channel.

STBC Tx:

STBC :Space Time Block Code. Switch to on will obtain the full antenna gain.

Scan Wireless AP’s:

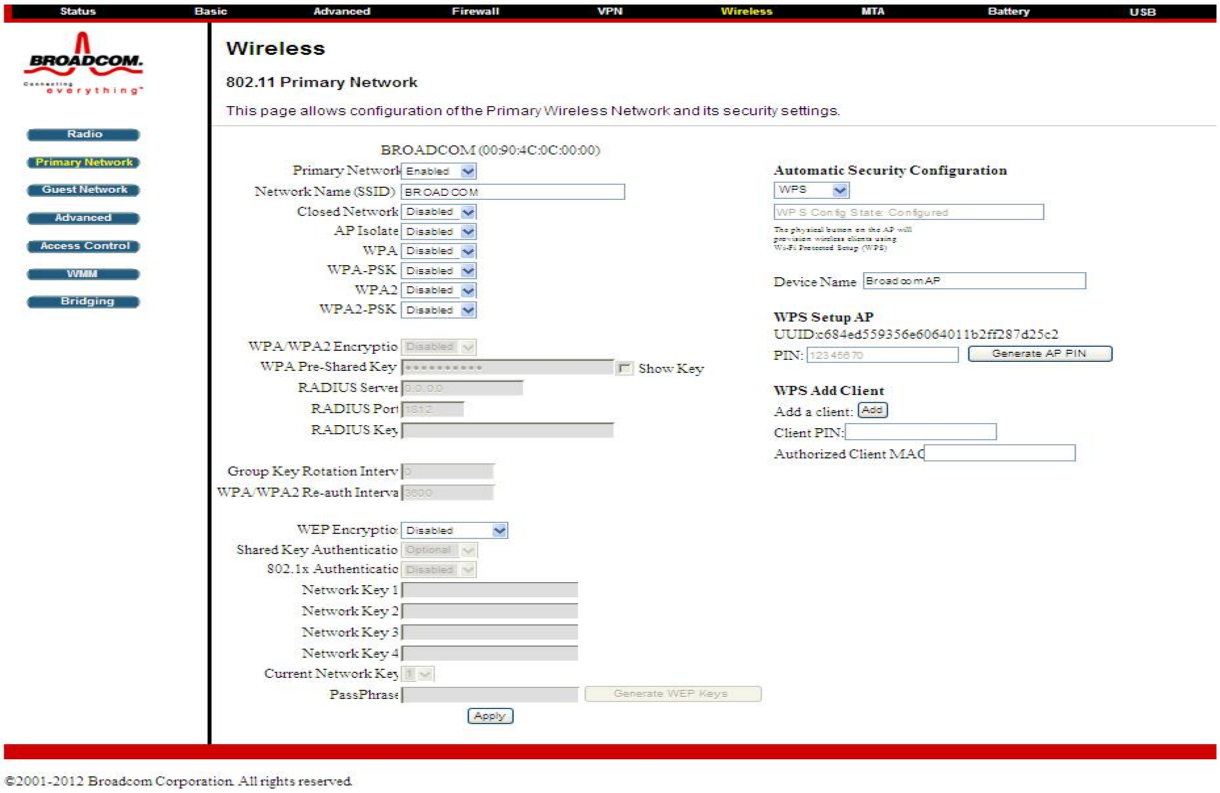
Force the Modems Access Point to scan for other AP’s within receive range.

Apply:

When any of the above settings are changed, the Apply button must be clicked in order to activate them.

5.6.2 Radio

Choose **Wireless > Primary Network** to display the following page.



Wireless

802.11 Primary Network

This page allows configuration of the Primary Wireless Network and its security settings.

BROADCOM (00:90:4C:0C:00:00)

Primary Network: Enabled
Network Name (SSID): BROADCOM
Closed Network: Disabled
AP Isolate: Disabled
WPA: Disabled
WPA-PSK: Disabled
WPA2: Disabled
WPA2-PSK: Disabled

WPA/WPA2 Encryption: Disabled
WPA Pre-Shared Key: ••••••••••• □ Show Key
RADIUS Server: 0.0.0.0
RADIUS Port: 1812
RADIUS Key:

Group Key Rotation Interval: 0
WPA/WPA2 Re-auth Interval: 3600

WEP Encryption: Disabled
Shared Key Authentication: Optional
802.1x Authentication: Disabled
Network Key 1:
Network Key 2:
Network Key 3:
Network Key 4:
Current Network Key: 1
PassPhrase:

Automatic Security Configuration
WPS
WPS Config State: Configured
The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS)

Device Name: BroadcomAP

WPS Setup AP
UUID:c684ed559356e6064011b2ff287d25c2
PIN: 12345670

WPS Add Client
Add a client:
Client PIN:
Authorized Client MAC:

©2001-2012 Broadcom Corporation. All rights reserved.

This page allow 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.

Closed Network:

The Network Name is not broadcast by the AP in a Closed Network. Therefore, only clients who already know the network name will be able to connect.

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.

WPA/WPA2 Encryption:

When using any of the WPA authentication schemes, AES, or TKIP + AES encryption modes can be set. AES provides the strongest encryption, while TKIP provides strong encryption with improved backward compatibility. The TKIP + AES mode allows both TKIP and AES-capable clients to connect.

WPA Pre-Shared Key:

Sets the WPA Pre-Shared Key (PSK). This is an 8-63 ASCII character string, or a 64-digit hex number. Enabled when the Network Authentication method is WPA-PSK or WPA2-PSK.

RADIUS Server:

Sets the IP address of the RADIUS server to use for client authentication. The RADIUS server may be on either the public network (WAN) or private network (LAN). This is only for WPA or WPA2 (Enterprise) modes.

RADIUS Port:

Sets the UDP port number of the RADIUS server. The default is 1812.

RADIUS Key:

Sets the shared secret for the RADIUS connection. The key is a 0 to 255 character ASCII string.

Group Key Rotation Interval:

The rotation interval in seconds indicating how often transmission keys should be rotated. Set to zero to disable periodic rekeying.

WPA/WPA2 Re-auth Interval:

This value indicates how often a station using Enterprise security needs to contact the RADIUS server.

WEP Encryption:

Sets the WEP encryption mode. Both 64-bit and 128-bit WEP encryption modes are supported. When running Shared Key or 802.1x authentication, WEP encryption must be enabled. WEP encryption cannot be used at the same time as WPA or WPA2.

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:

When WEP encryption is enabled, selects the encryption (transmit) key.

PassPhrase:

Sets the text to use for WEP key generation.

Generate WEP Keys:

When WEP encryption is enabled, this action button converts the passphrase entered to a set of WEP keys. Remember to click the Apply button to save the keys.

Automatic Security Configuration

Wi-Fi Protected Setup (WPS);

WPS is the standard method to achieve the same goal as Broadcom’s SES. The protocol is described in a specification issued by the Wi-Fi Alliance.

Device Name:

The name of the device that will advertised to wireless stations.

WPS Setup AP:

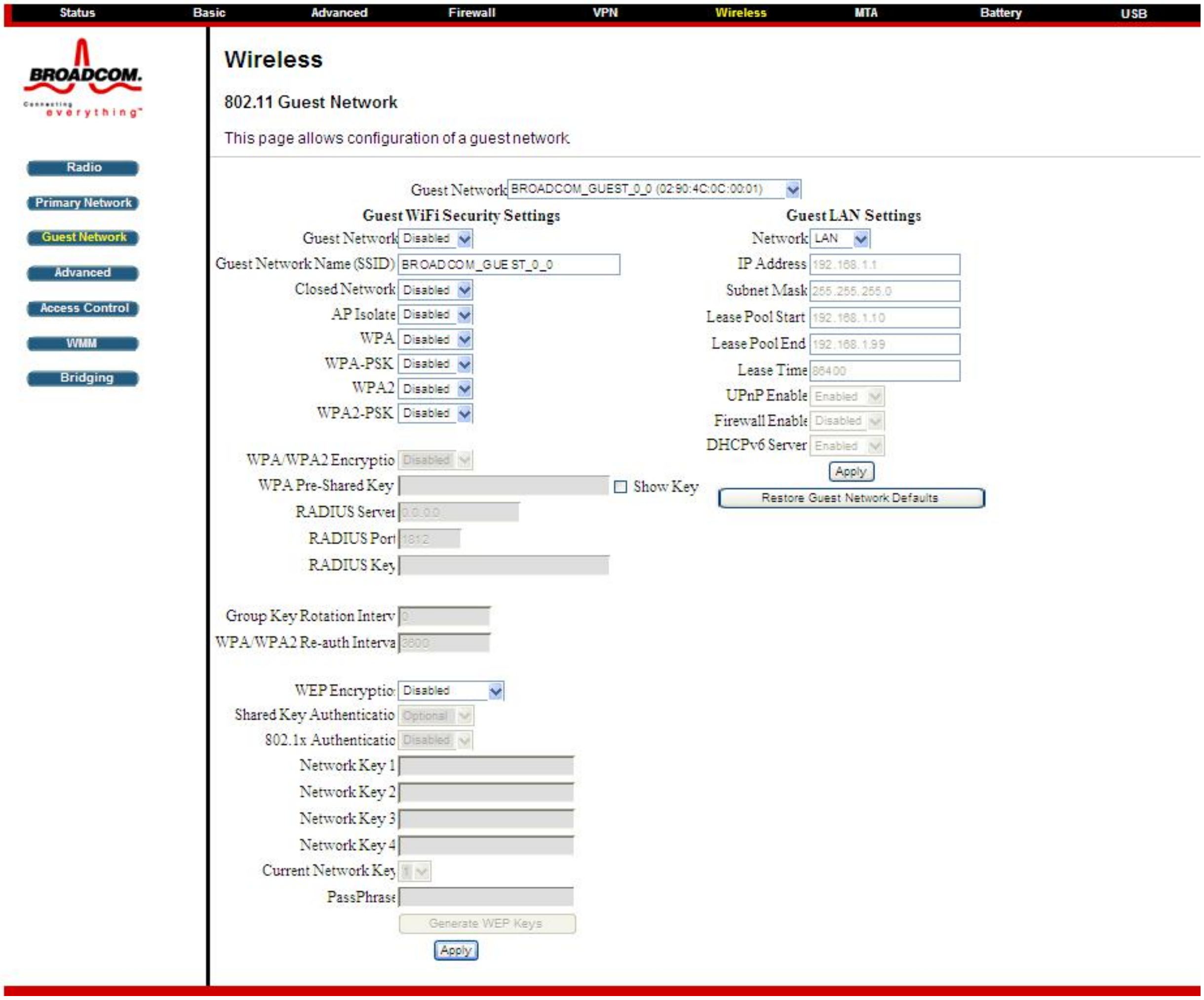
Set the PIN and click the ‘Configure’ button in this section when using an External Registrar.

WPS Add Client:

Add a new wireless client using the Internal Registrar. Choose to add either by push-button or PIN method and then click the ‘Add’ button.

5.6.3 Guest Network

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



Wireless

802.11 Guest Network

This page allows configuration of a guest network.

Guest Network BROADCOM_GUEST_0_0 (02:90:4C:0C:00:01)

Guest WiFi Security Settings

Guest Network Disabled
Guest Network Name (SSID) BROADCOM_GUEST_0_0
Closed Network Disabled
AP Isolate Disabled
WPA Disabled
WPA-PSK Disabled
WPA2 Disabled
WPA2-PSK Disabled

WPA/WPA2 Encryptio Disabled
WPA Pre-Shared Key □ Show Key
RADIUS Server 0.0.0.0
RADIUS Port 1812
RADIUS Key

Group Key Rotation Interv 0
WPA/WPA2 Re-auth Interva 3600

WEP Encryptio Disabled
Shared Key Authenticatio Optional
802.1x Authenticatio Disabled
Network Key 1
Network Key 2
Network Key 3
Network Key 4
Current Network Key 1
PassPhrase
Generate WEP Keys
Apply

Guest LAN Settings

Network LAN
IP Address 192.168.1.1
Subnet Mask 255.255.255.0
Lease Pool Start 192.168.1.10
Lease Pool End 192.168.1.99
Lease Time 86400
UPnP Enable Enabled
Firewall Enable Disabled
DHCPv6 Server Enabled
Apply
Restore Guest Network Defaults

The page allows you to configure a secondary guest network on the wireless interface. This network is isolated from the LAN. Any clients that associate with the guest network SSID will be isolated from the private LAN and can only communicate with WAN hosts. Most of the configuration points on the guest network page are identical to those on the Primary Network page. A few extras are explained below.

DHCP Server:

Enables the DHCP server to gives out leases to guest network clients from the specified lease pool. If the DHCP server is disabled, guest network STAs need to be assigned static IP addresses.

IP Address:

This specifies the gateway IP relayed to guest clients in DHCP lease offers.

Subnet Mask:

This specifies the subnet mask for the guest network.

Lease Pool Start:

This specifies the starting IP address for the guest network lease pool.

Lease Pool End:

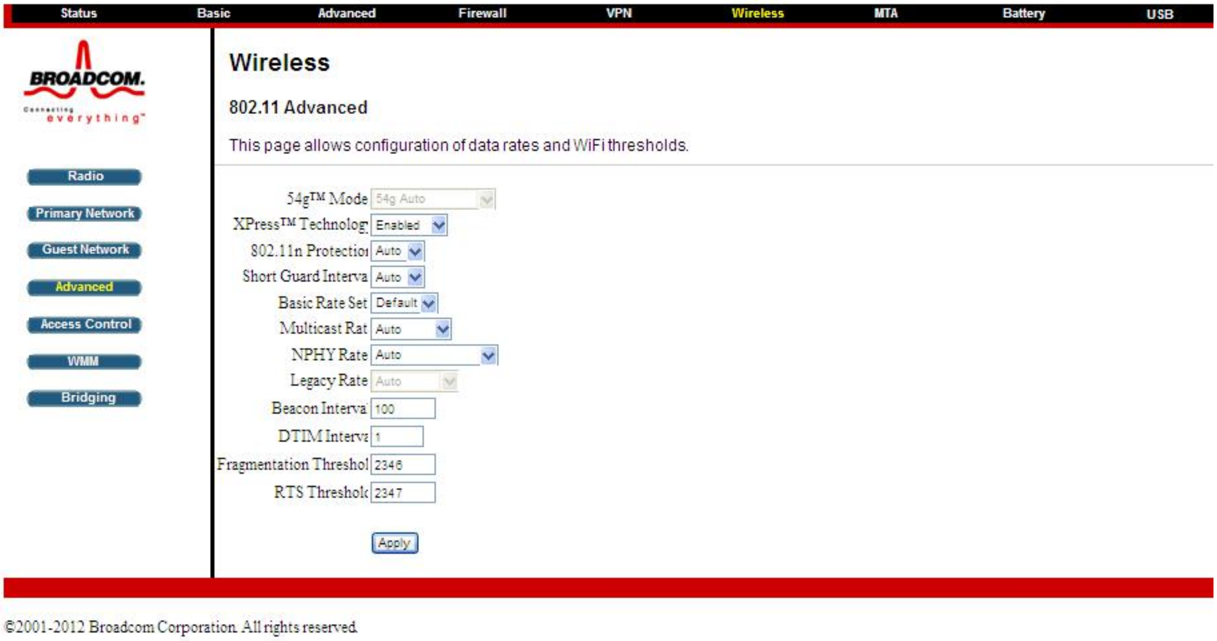
This specifies the ending IP address for the guest network lease pool.

Lease Time:

This specifies the lease time for the guest network lease pool, once the CMRG completes WAN provisioning.

5.6.4 Advanced

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



Wireless

802.11 Advanced

This page allows configuration of data rates and WiFi thresholds.

54g™ Mode: 54g Auto
XPress™ Technolog: Enabled
802.11n Protectio: Auto
Short Guard Interva: Auto
Basic Rate Set: Default
Multicast Rat: Auto
NPHY Rate: Auto
Legacy Rate: Auto
Beacon Interva: 100
DTIM Interva: 1
Fragmentation Threshol: 2346
RTS Threshol: 2347

©2001-2012 Broadcom Corporation. All rights reserved.

This page allows you to configure advanced wireless settings.

54g™ Mode:

Sets the network mode. Choices are 54g Auto, 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.

54g™ Protection:

In Auto mode the AP will use RTS/CTS protection to improve 802.11g performance in mixed 802.11g + 802.11b networks. Turn protection Off to maximize 802.11g throughput under most conditions.

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:

Similar to 54g protection except it applies to 802.11n devices.

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:

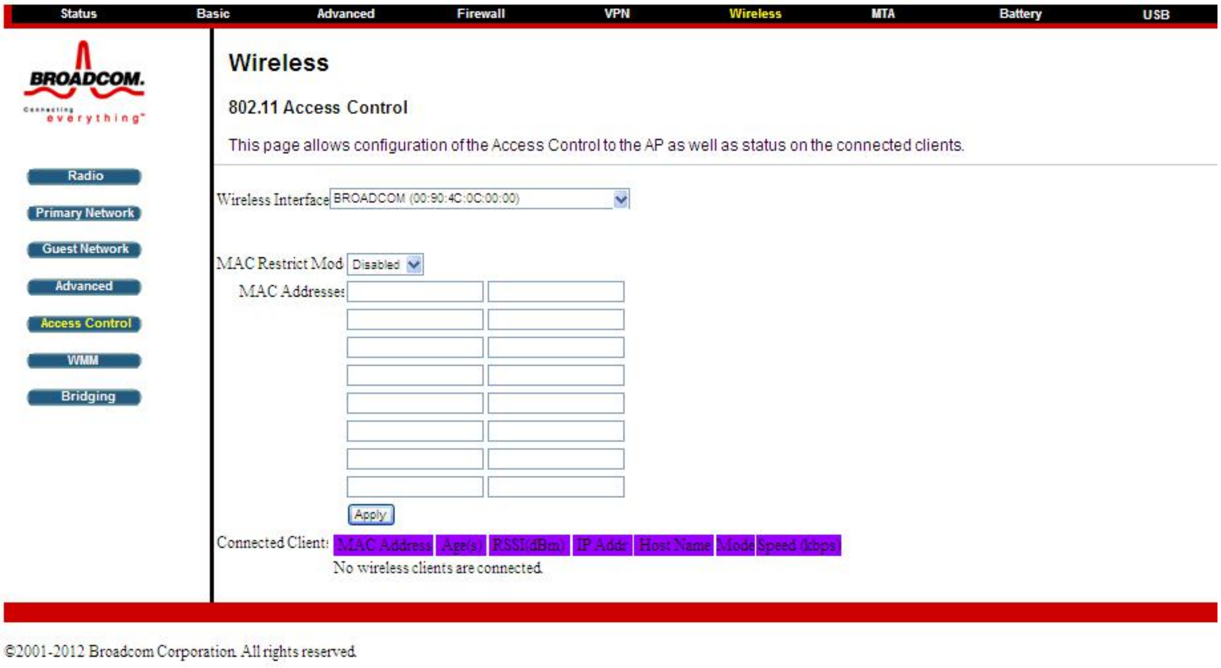
Sets the fragmentation threshold. Packets exceeding this threshold will be fragmented into packets no larger than the threshold before packet transmission.

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.

5.6.5 Access Control

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



Wireless

802.11 Access Control

This page allows configuration of the Access Control to the AP as well as status on the connected clients.

Wireless Interface BROADCOM (00:90:4C:0C:00:00)

MAC Restrict Mod Disabled

MAC Addresses

Connected Client:

MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name	Mode	Speed (kbps)

No wireless clients are connected.

©2001-2012 Broadcom Corporation. All rights reserved.

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.

MAC Restrict Mode:

Selects whether wireless clients with the specified MAC address are allowed or denied wireless access. To allow all clients, select Disabled.

MAC Addresses:

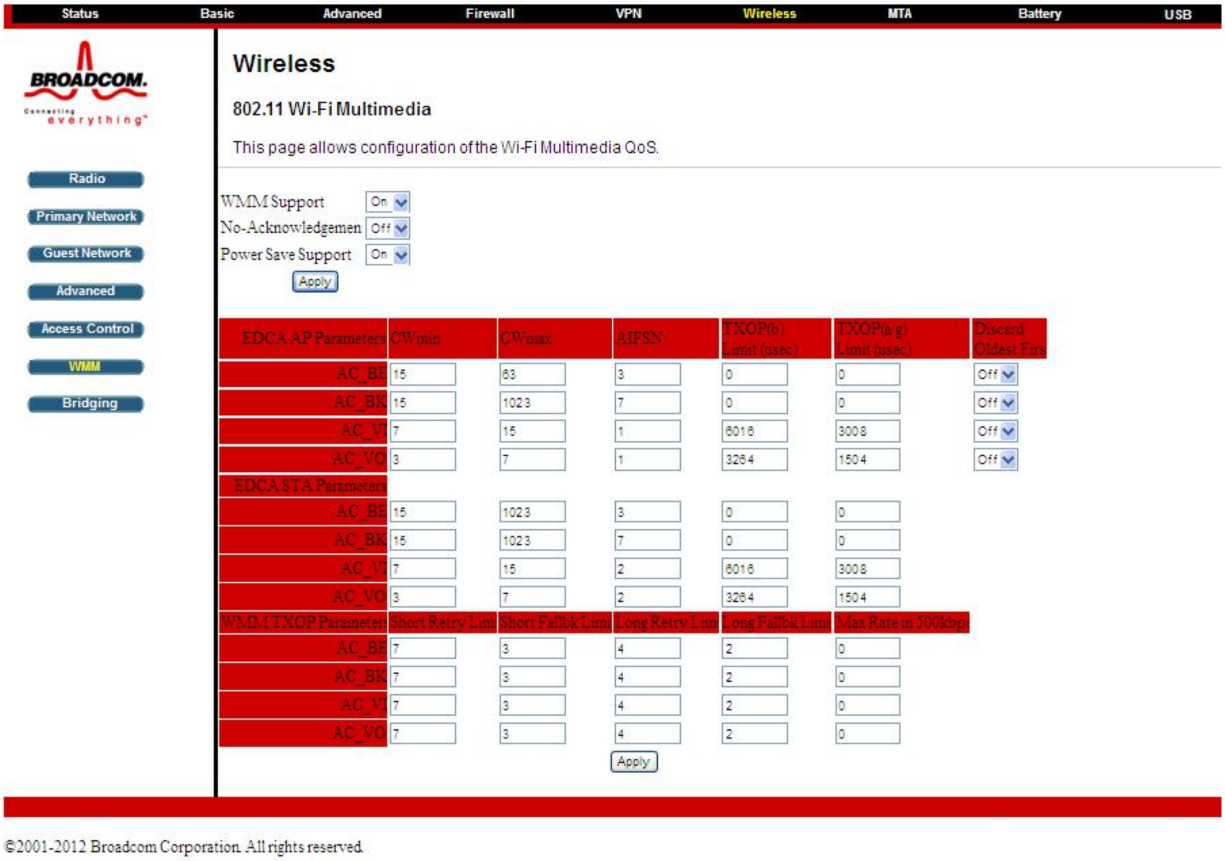
A list of wireless client MAC addresses to allow or deny based on the Restrict Mode setting. Valid input MAC address formats are XX:XX:XX:XX:XX:XX and XX-XX-XX-XX-XX-XX.

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.

5.6.6 WMM

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



Wireless

802.11 Wi-Fi Multimedia

This page allows configuration of the Wi-Fi Multimedia QoS.

WMM Support: On
No-Acknowledgemen: Off
Power Save Support: On
Apply

EDCA AP Parameters	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest Firs
AC_BE	15	63	3	0	0	Off
AC_BK	15	1023	7	0	0	Off
AC_VI	7	15	1	6016	3008	Off
AC_VO	3	7	1	3264	1504	Off
EDCA STA Parameters						
AC_BE	15	1023	3	0	0	
AC_BK	15	1023	7	0	0	
AC_VI	7	15	2	6016	3008	
AC_VO	3	7	2	3264	1504	
WMM TXOP Parameters	Short Retry Limi	Short Fallbk Limi	Long Retry Limi	Long Fallbk Limi	Max Rate in 500kbps	
AC_BE	7	3	4	2	0	
AC_BK	7	3	4	2	0	
AC_VI	7	3	4	2	0	
AC_VO	7	3	4	2	0	

Apply

©2001-2012 Broadcom Corporation. All rights reserved.

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).

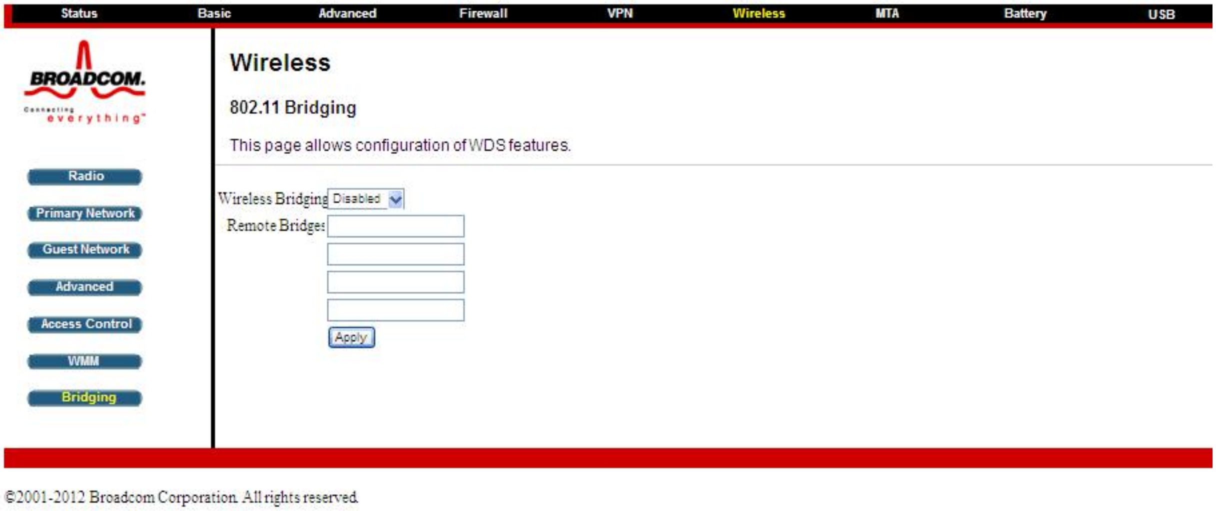
There are also two AP-specific settings: Admission Control and Discard Oldest First. Admission control specifies if admission control is enforced for the Access Categories. Discard Oldest First specifies the discard policy for the queues. On discards the oldest first; Off discards the newest first.

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).

5.6.7 Bridging

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



Wireless

802.11 Bridging

This page allows configuration of WDS features.

Wireless Bridging Disabled

Remote Bridges

©2001-2012 Broadcom Corporation. All rights reserved.

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:

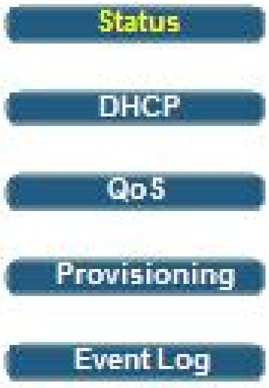
This setting enables or disables wireless bridging.

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.

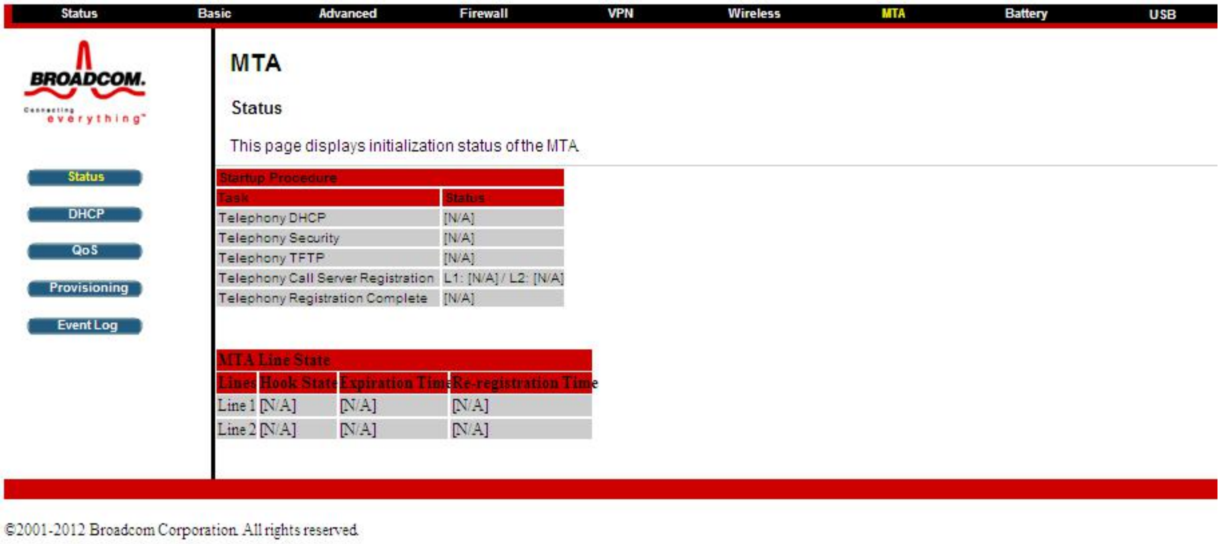
5.7 MTA

Choose **MTA** and the submenus of **MTA** are shown as below:



5.7.1 Status

Choose **MTA > Status** to display the following page.



MTA

Status

This page displays initialization status of the MTA.

Startup Procedure	
Task	Status
Telephony DHCP	[N/A]
Telephony Security	[N/A]
Telephony TFTP	[N/A]
Telephony Call Server Registration	L1: [N/A] / L2: [N/A]
Telephony Registration Complete	[N/A]

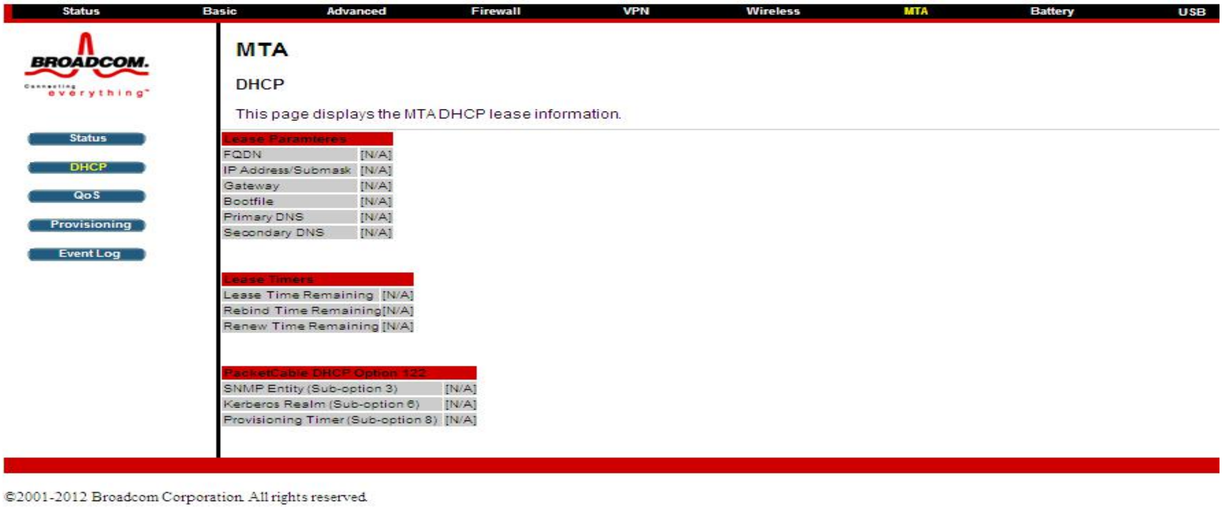
MTA Line State			
Line	Hook State	Expiration Time	Re-registration Time
Line 1	[N/A]	[N/A]	[N/A]
Line 2	[N/A]	[N/A]	[N/A]

©2001-2012 Broadcom Corporation. All rights reserved.

This page displays initialization status of the MTA including Registration/Provisioning and line states.

5.7.2 DHCP

Choose **MTA > DHCP** to display the following page.



MTA

DHCP

This page displays the MTA DHCP lease information.

Lease Paramteres	
FQDN	[N/A]
IP Address/Submask	[N/A]
Gateway	[N/A]
Bootfile	[N/A]
Primary DNS	[N/A]
Secondary DNS	[N/A]

Lease Timers	
Lease Time Remaining	[N/A]
Rebind Time Remaining	[N/A]
Renew Time Remaining	[N/A]

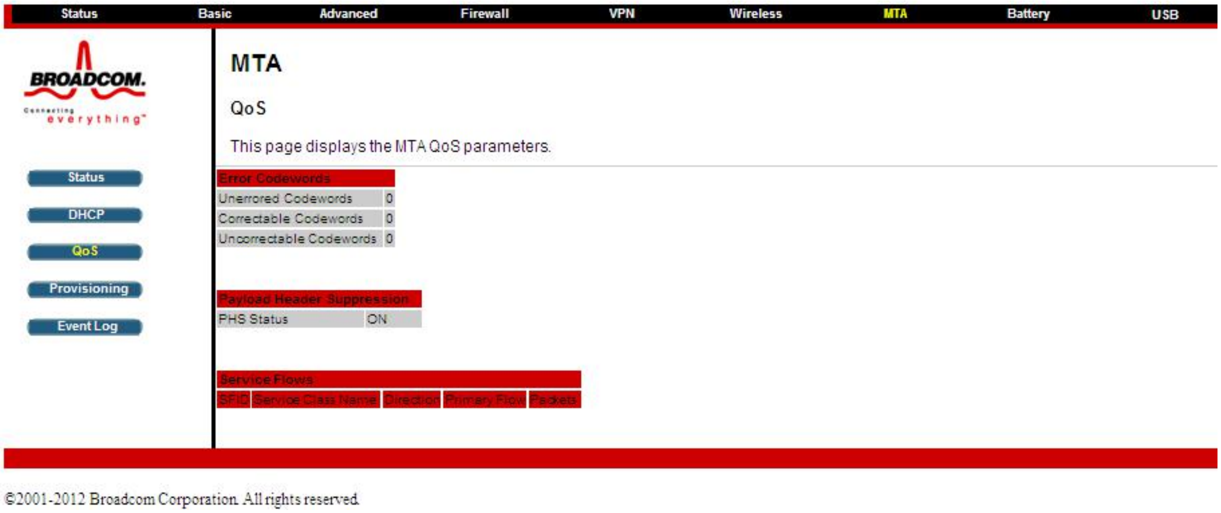
PacketCable DHCP Option 122	
SNMP Entity (Sub-option 3)	[N/A]
Kerberos Realm (Sub-option 6)	[N/A]
Provisioning Timer (Sub-option 8)	[N/A]

©2001-2012 Broadcom Corporation. All rights reserved.

This page display information about the state of the DHCP client, tftp client and IP address of the DNS server, lease timers and DHCP option 122 values.

5.7.3 QoS

Choose **MTA > QoS** to display the following page.



MTA

QoS

This page displays the MTA QoS parameters.

Error Codewords	
Unerrored Codewords	0
Correctable Codewords	0
Uncorrectable Codewords	0

Payload Header Suppression	
PHS Status	ON

Service Flows

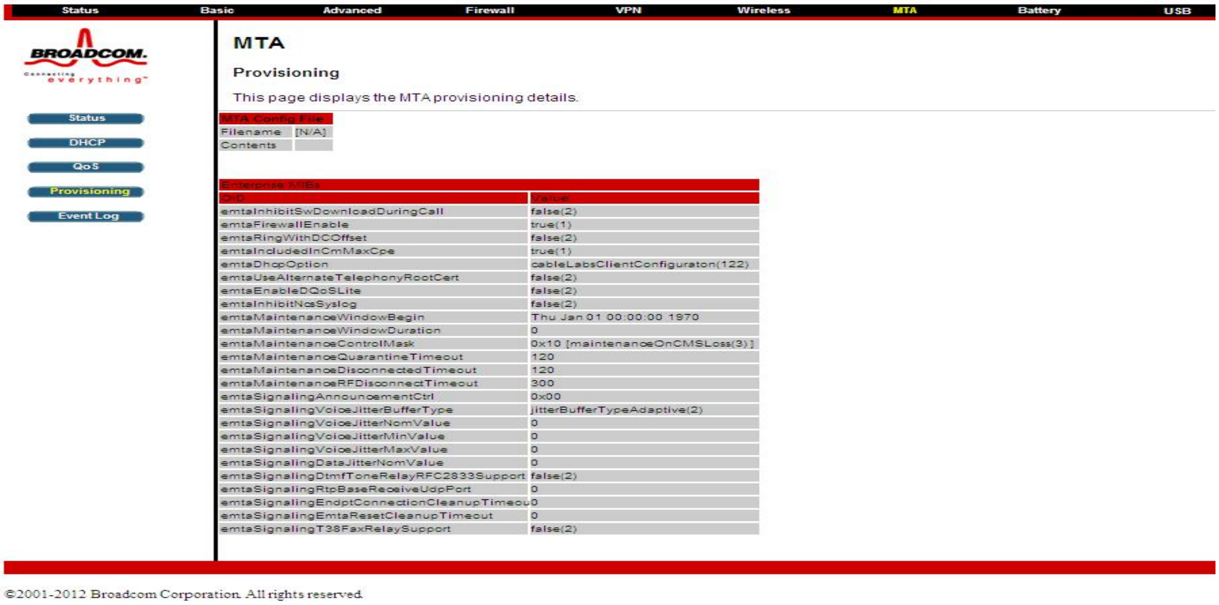
SFID	Service Class Name	Direction	Primary Flow	Packets

©2001-2012 Broadcom Corporation. All rights reserved.

This page displays information about Downstream FEC errors,Service Flow counters and the state of Payload Header Suppression.

5.7.4 Provisioning

Choose **MTA > Provisioning** to display the following page.



MTA

Provisioning

This page displays the MTA provisioning details.

MTA Config File	
Filename	[N/A]
Contents	

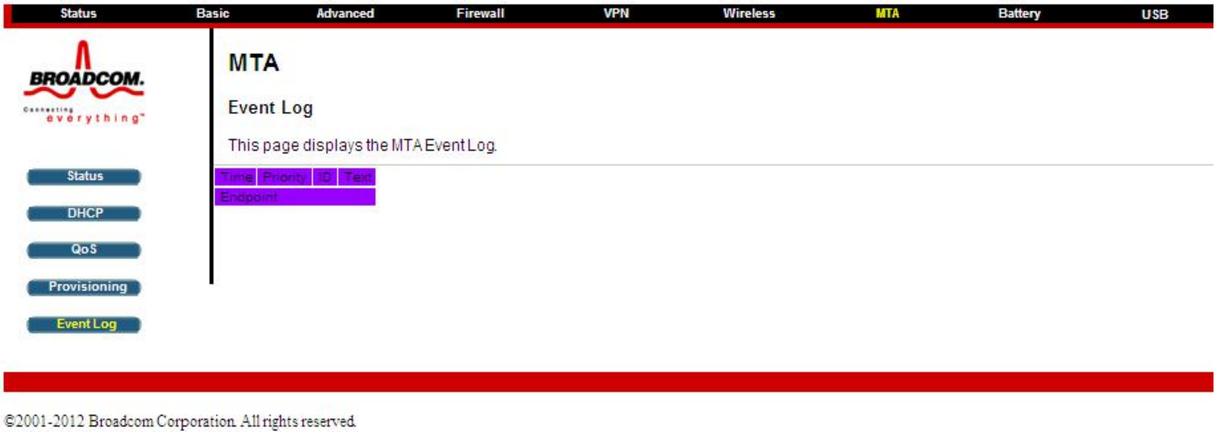
Enterprise MIBs	
OID	Value
emtaInhibitSwDownloadDuringCall	false(2)
emtaFirewallEnable	true(1)
emtaRingWithDCOffset	false(2)
emtaIncludedInCmMaxCpe	true(1)
emtaDhcpOption	cableLabsClientConfiguraton(122)
emtaUseAlternateTelephonyRootCert	false(2)
emtaEnableDQoSLite	false(2)
emtaInhibitNcsSyslog	false(2)
emtaMaintenanceWindowBegin	Thu Jan 01 00:00:00 1970
emtaMaintenanceWindowDuration	0
emtaMaintenanceControlMask	0x10 [maintenanceOnCMSLoss(3)]
emtaMaintenanceQuarantineTimeout	120
emtaMaintenanceDisconnectedTimeout	120
emtaMaintenanceRFDisconnectTimeout	300
emtaSignalingAnnouncementCtrl	0x00
emtaSignalingVoiceJitterBufferType	jitterBufferTypeAdaptive(2)
emtaSignalingVoiceJitterNomValue	0
emtaSignalingVoiceJitterMinValue	0
emtaSignalingVoiceJitterMaxValue	0
emtaSignalingDataJitterNomValue	0
emtaSignalingDtmfToneRelayRFC2833Support	false(2)
emtaSignalingRtpBaseReceiveUdpPort	0
emtaSignalingEndptConnectionCleanupTimeou	0
emtaSignalingEmtaResetCleanupTimeout	0
emtaSignalingT38FaxRelaySupport	false(2)

©2001-2012 Broadcom Corporation. All rights reserved.

This page display the contents of the MTA config file and the value of assorted MTA mib's.

5.7.5 Event Log

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



MTA

Event Log

This page displays the MTA Event Log.

Time	Priority	ID	Text
Endpoint			

©2001-2012 Broadcom Corporation. All rights reserved.

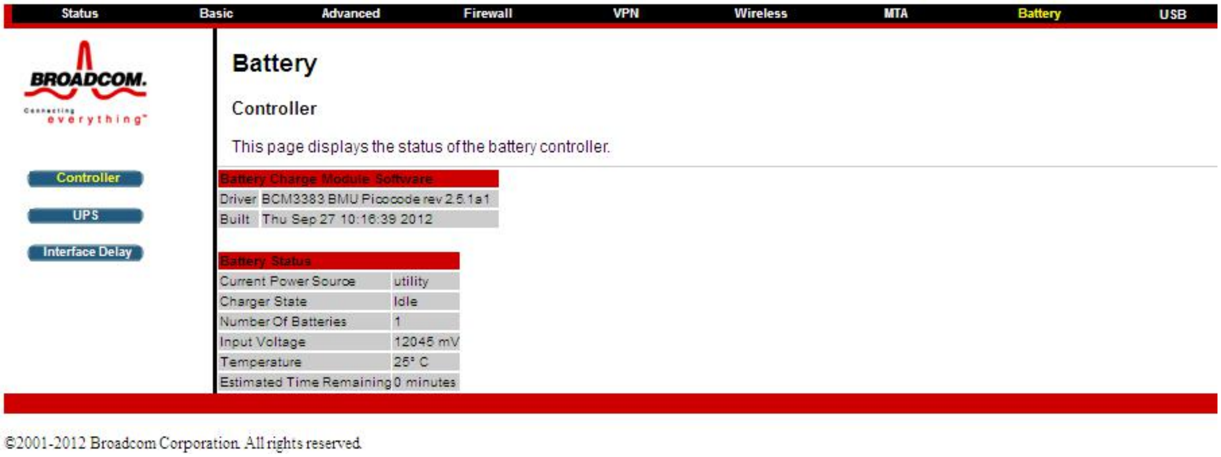
This page display MTA events.

5.8 Battery

Choose **Battery** and the submenus of **Battery** are shown as below:

5.8.1 Controller

Choose **Battery > Controller** to display the following page.



Battery

Controller

This page displays the status of the battery controller.

Battery Charge Module Software	
Driver	BCM3383 BMU Picocode rev 2.5.1a1
Built	Thu Sep 27 10:16:39 2012

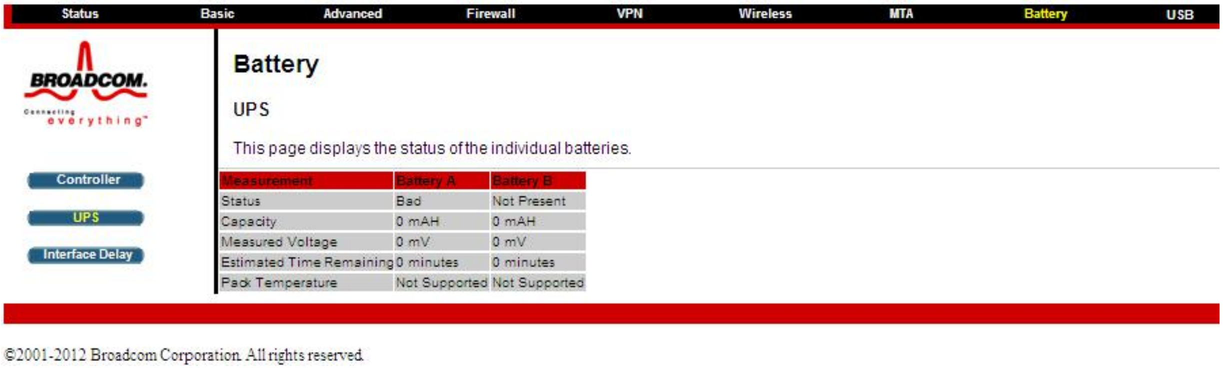
Battery Status	
Current Power Source	utility
Charger State	Idle
Number Of Batteries	1
Input Voltage	12045 mV
Temperature	25° C
Estimated Time Remaining	0 minutes

©2001-2012 Broadcom Corporation. All rights reserved.

This page display general battery pack information and the Pico version (UPS driver).

5.8.2 UPS

Choose **Battery > UPS** to display the following page.



Battery

UPS

This page displays the status of the individual batteries.

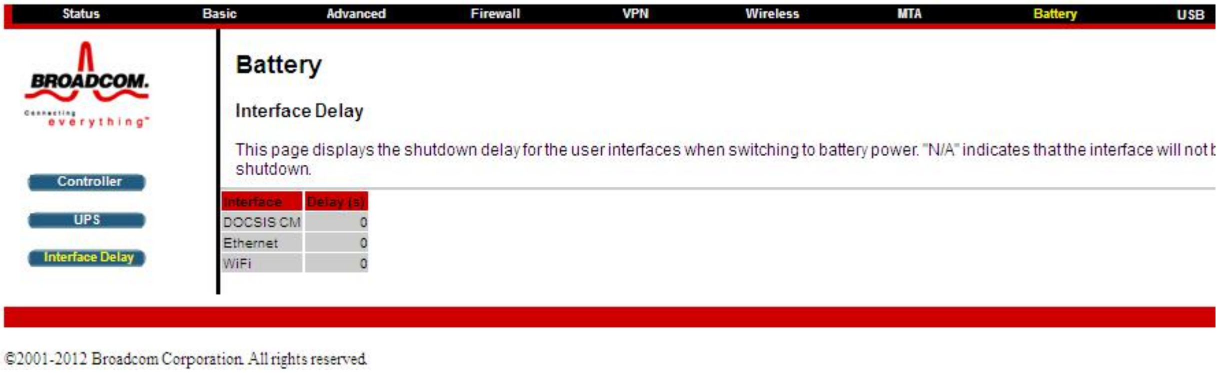
Measurement	Battery A	Battery B
Status	Bad	Not Present
Capacity	0 mAH	0 mAH
Measured Voltage	0 mV	0 mV
Estimated Time Remaining	0 minutes	0 minutes
Pack Temperature	Not Supported	Not Supported

©2001-2012 Broadcom Corporation. All rights reserved.

This page displays the status of the individual batteries.

5.8.3 Interface Delay

Choose **Battery > Interface Delay** to display the following page.



Battery

Interface Delay

This page displays the shutdown delay for the user interfaces when switching to battery power. "N/A" indicates that the interface will not b shutdown.

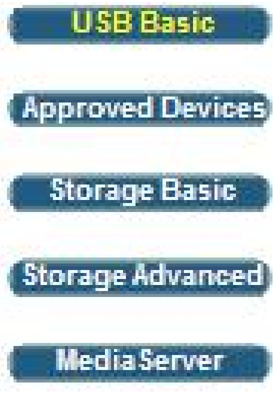
Interface	Delay (s)
DOCSIS CM	0
Ethernet	0
WiFi	0

©2001-2012 Broadcom Corporation. All rights reserved.

This page display the interface delay values. Each interface has the ability to support a different value for the shutdown delay that will be applied after switching to battery power.

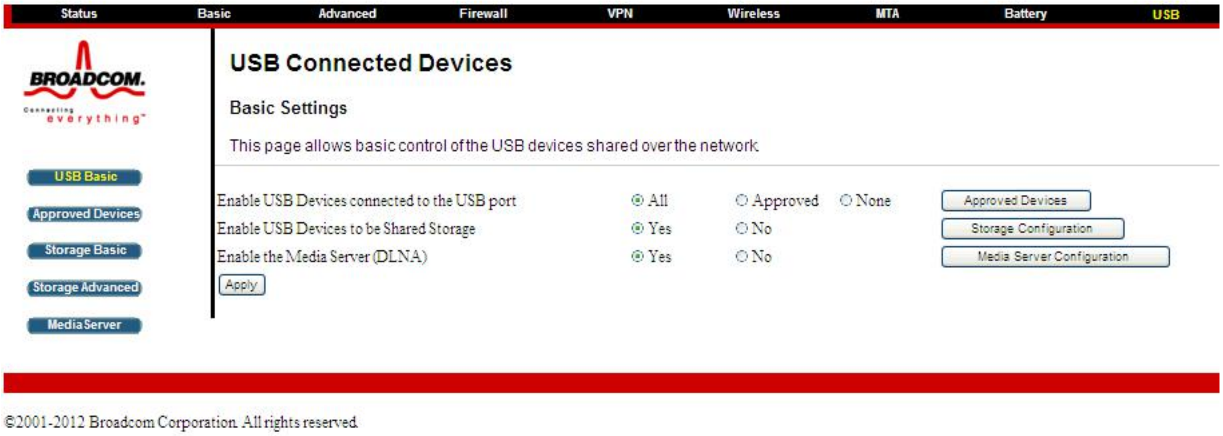
5.9 USB

Choose **USB** and the submenus of **USB** are shown as below:



5.9.1 USB Basic

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



USB Connected Devices

Basic Settings

This page allows basic control of the USB devices shared over the network.

Enable USB Devices connected to the USB port ● All ○ Approved ○ None

Enable USB Devices to be Shared Storage ● Yes ○ No

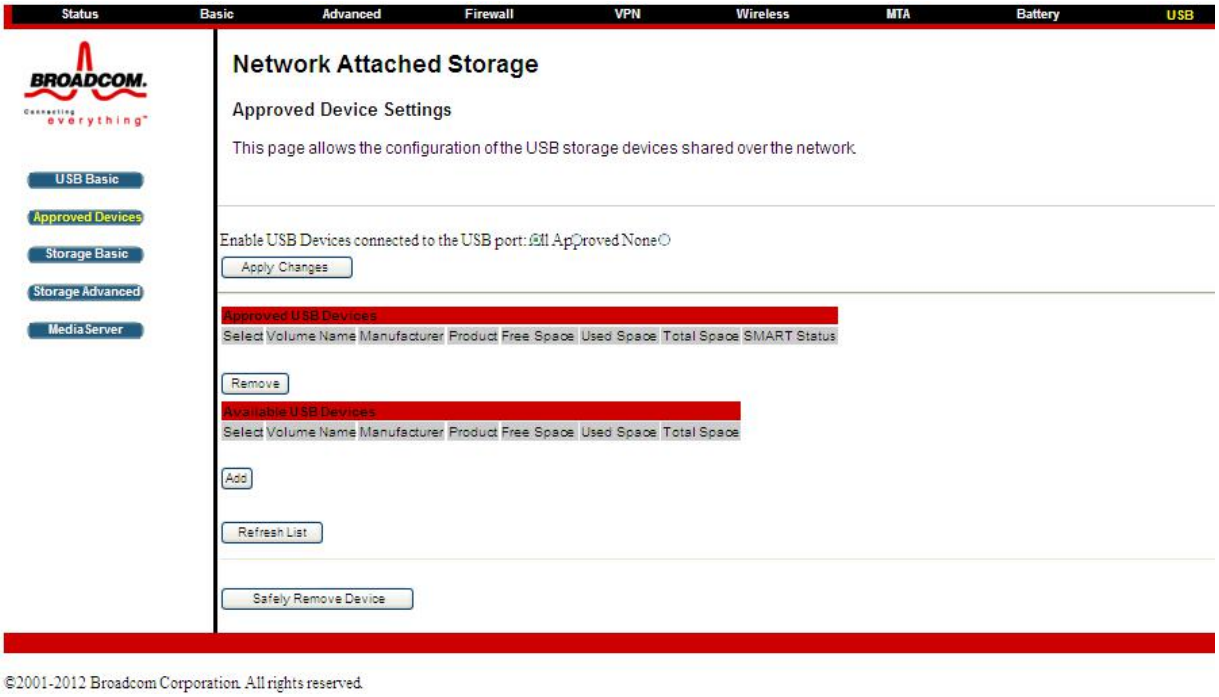
Enable the Media Server (DLNA) ● Yes ○ No

©2001-2012 Broadcom Corporation. All rights reserved.

This page allow you to config Linux based servers. The buttons on the right side of the page are short cuts to the buttons on the left side frame.

5.9.2 Approved Devices

Choose **USB > Approved Devices** to display the following page.



Network Attached Storage

Approved Device Settings

This page allows the configuration of the USB storage devices shared over the network.

Enable USB Devices connected to the USB port: ●All Ap○roved None○

Approved USB Devices

Select	Volume Name	Manufacturer	Product	Free Space	Used Space	Total Space	SMART Status

Available USB Devices

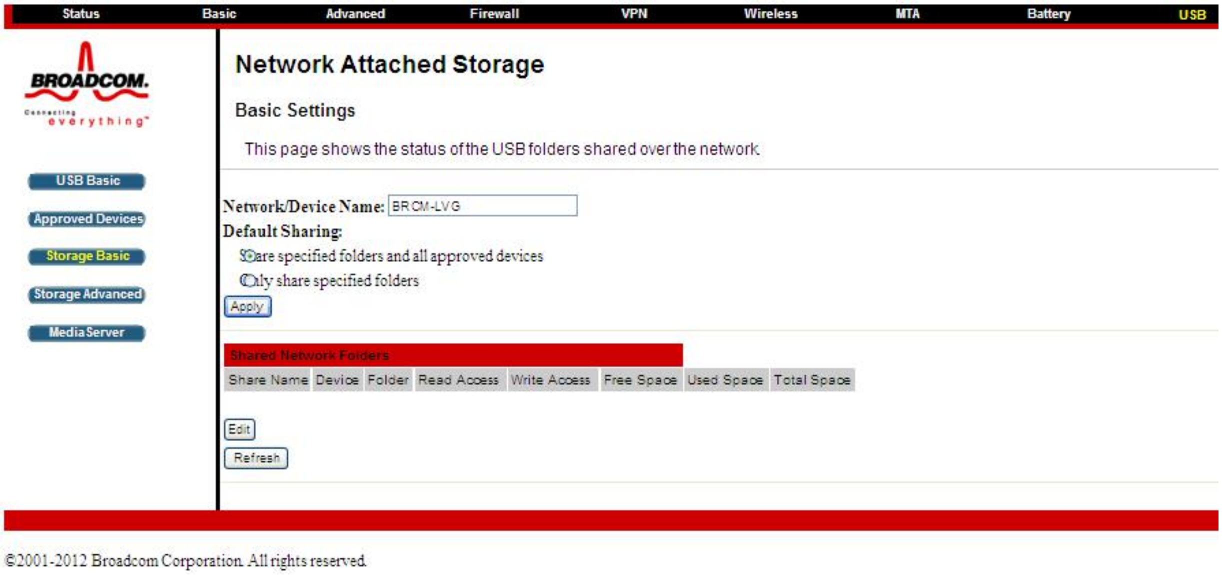
Select	Volume Name	Manufacturer	Product	Free Space	Used Space	Total Space

©2001-2012 Broadcom Corporation. All rights reserved.

This page allow to choose if any USB storage device plugged into the modem can be used or only approved devices. If approved device is selected then each device must be manually approved on this page. USB storage devices can be safely removed after selecting the Safely Remove Device button. The user will be asked which device they want to remove.

5.9.3 Storage Basic

Choose **USB > Storage Basic** to display the following page.



Network Attached Storage

Basic Settings

This page shows the status of the USB folders shared over the network.

Network/Device Name: BRCM-LVG

Default Sharing:

● Share specified folders and all approved devices

○ Only share specified folders

Apply

Shared Network Folders

Share Name	Device	Folder	Read Access	Write Access	Free Space	Used Space	Total Space

Edit

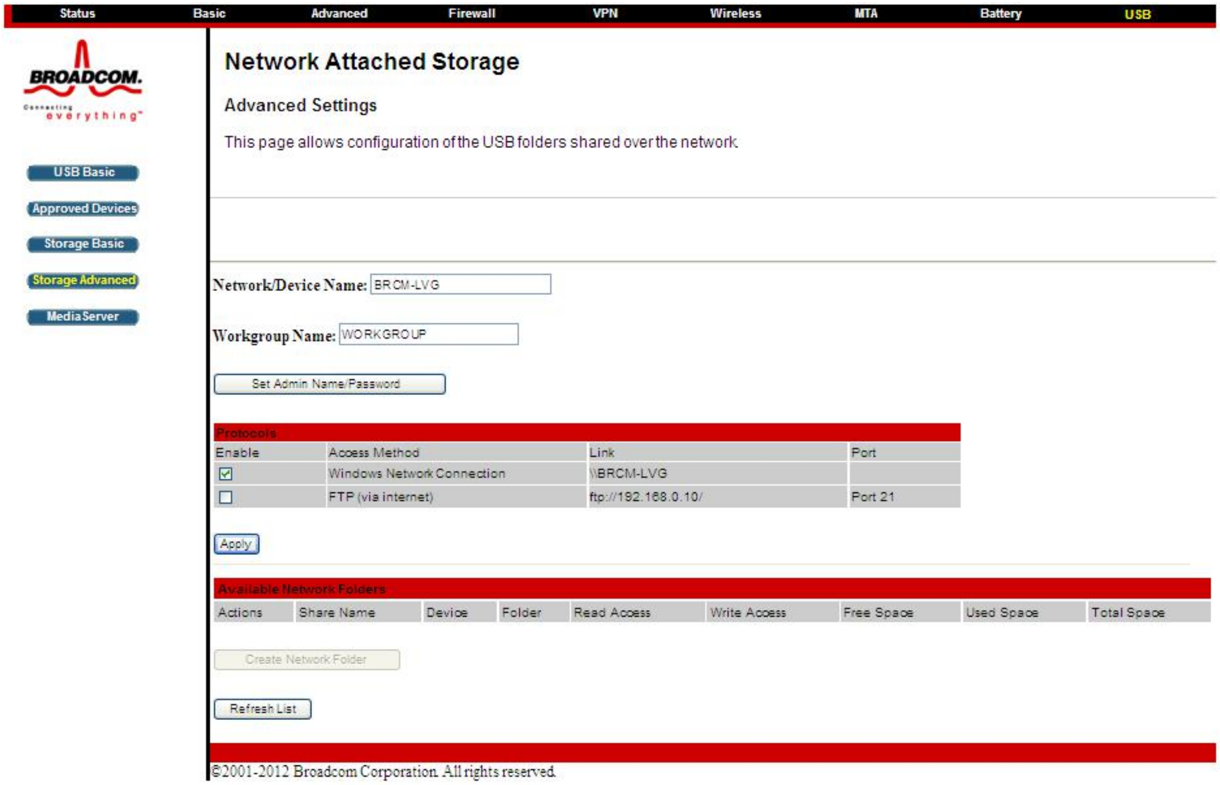
Refresh

©2001-2012 Broadcom Corporation. All rights reserved.

This page allows you to configure the device name and what folders should be shared.

5.9.4 Storage Advanced

Choose **USB > Storage Advanced** to display the following page.



Network Attached Storage

Advanced Settings

This page allows configuration of the USB folders shared over the network.

Network/Device Name: BRCM-LVG

Workgroup Name: WORKGROUP

Protocols

Enable	Access Method	Link	Port
☑	Windows Network Connection	\\BRCM-LVG	
□	FTP (via internet)	ftp://192.168.0.10/	Port 21

Available Network Folders

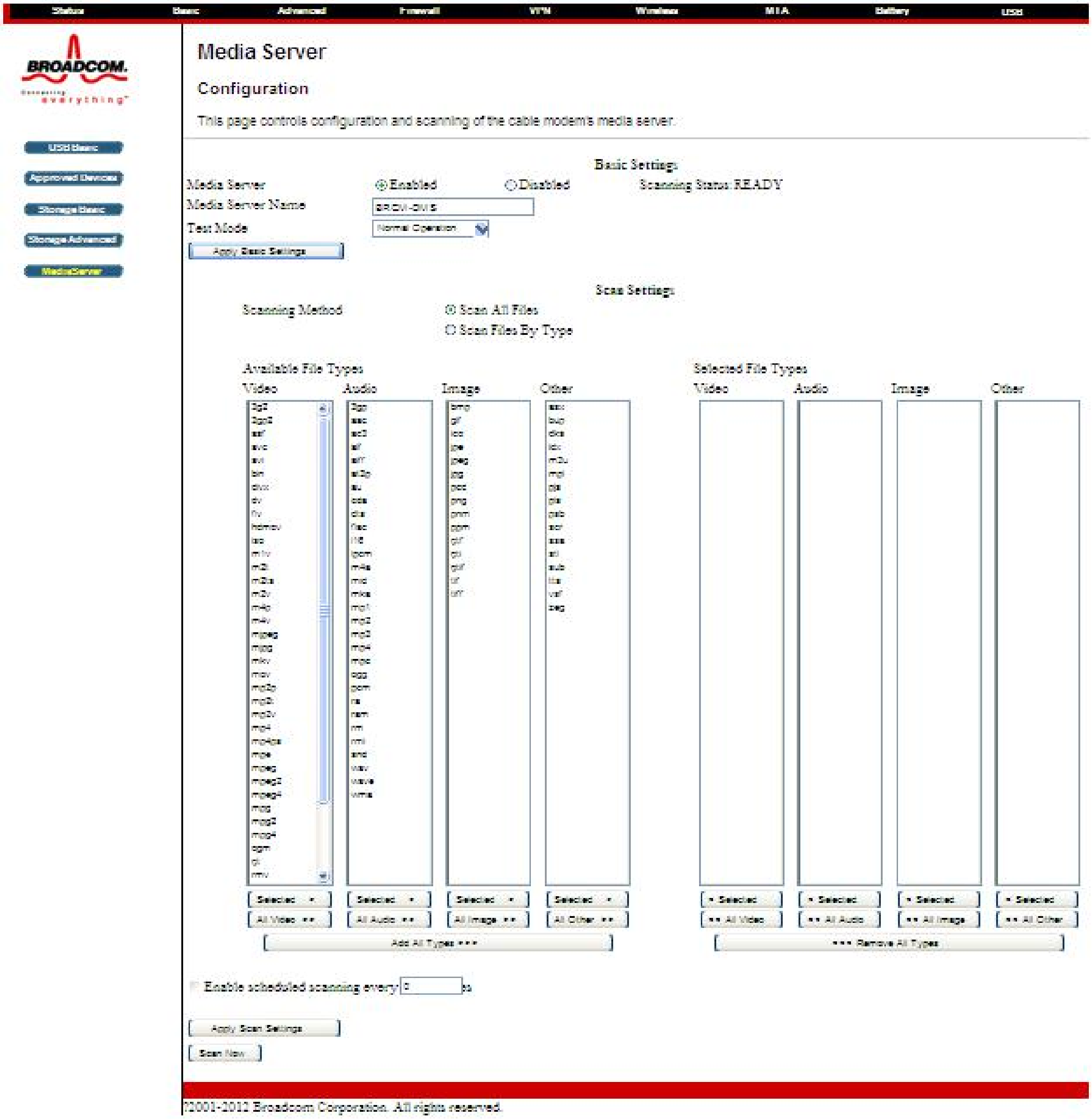
Actions	Share Name	Device	Folder	Read Access	Write Access	Free Space	Used Space	Total Space

©2001-2012 Broadcom Corporation. All rights reserved.

This page allows you to configure the device name. Additionally the workgroup name can is configured here. The Windows Network and FTP support can be enabled or disabled on this page. The IP address displayed in the link field is the Linux IP stack address that should be used for the FTP server address in the FTP clients.

5.9.5 MediaServer

Choose **USB > MediaServer** to display the following page.



Media Server

Configuration

This page controls configuration and scanning of the cable modem's media server.

Basic Settings

Media Server ● Enabled ○ Disabled

Scanning Status: READY

Media Server Name: BRCM-DMS

Test Mode: Normal Operation

Scan Settings

Scanning Method ● Scan All Files ○ Scan Files By Type

□ Enable scheduled scanning every 0 hs

?2001-2012 Broadcom Corporation. All rights reserved.

This page allow you to configure the DLNA media server. The media server name and the file names that will be scanned on the USB storage devices are configured using this page. If desired the media Server can scan the device periodically to check for new files.

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.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed an operated with a minimum distance of 20cm between the radiator and your body.

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

antenna or transmitter.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority
to operate the equipment.

Canada Statement

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numrique de la classe B est conforme Ã la norme NMB-003 du Canada.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
The device meets the exemption from the routine evaluation limits in section 2.5 of RSS 102 and compliance with RSS-102 RF exposure, users can obtain Canadian information on RF exposure and compliance.
Le dispositif rencontre l'exemption des limites courantes d'évaluation dans la section 2.5 de RSS 102 et la conformité à l'exposition de RSS-102 rf, utilisateurs peut obtenir l'information canadienne sur l'exposition et la conformité de rf.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
Cet émetteur ne doit pas être Co-placé ou ne fonctionnant en même temps qu'aucune autre antenne ou émetteur. Cet équipement devrait être installé et actionné avec une distance minimum de 20 centimètres entre le radiateur et votre corps.
This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (identifier le dispositif par son numéro de certification ou son numéro de modèle s'il fait partie du matériel de catégorie I) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

5GHz

5150-5250 MHz band is restricted to indoor operations only.